Política Global de Privacidade e Proteção de Dados Pessoais LojaHub (pt-BR)

1. Definições

LOJAHUB LTDA, pessoa jurídica de direito privado, inscrita no CNPJ sob n. 27.984.556/0001-16, localizada em Rua Cabo Antônio Pinton, nº 31, CEP 02186-000, São Paulo-SP, Brasil, desenvolvedora e mantenedora dos sistemas **LojaHub**, versa neste documento sobre a definição da Política Global de Privacidade e Proteção de Dados Pessoais (ou simplesmente "PGPPDP").

Compartilham desta definição de Política Global de Privacidade e Proteção de Dados Pessoais, todos os sistemas desenvolvidos pela **LojaHub LTDA**, sendo eles neste momento:

- LojaHub → Hub e ERP para e-commerce
(https://lojahub.com.br)

- LojaHub Analytics → Análise de Mercado
(https://analytics.lojahub.com.br)

- LojaHub Financeiro → Conciliação de Vendas
(https://financeiro.lojahub.com.br)

- Total Connect → Integrador de Mercado Livre
(https://totalconnect.com.br)

2. Objetivo

A **LojaHub LTDA** tem o compromisso de proteger a privacidade dos dados pessoais de seus funcionários, clientes, parceiros de negócios e outras pessoas identificáveis. Desta forma, a **LojaHub LTDA** implementou um programa global de privacidade e proteção de dados para estabelecer e manter padrões elevados para coletar, usar, divulgar, armazenar, proteger, acessar, transferir ou processar dados pessoais. Esta política global de privacidade e proteção de dados pessoais é a base do programa de privacidade e proteção de dados e descreve a abordagem adotada pela **LojaHub LTDA** ao processar dados pessoais em qualquer lugar do mundo.

3. Escopo

Todos os funcionários, prestadores de serviços, consultores, colaboradores temporários e outros empregados na **LojaHub LTDA** e em suas subsidiárias devem cumprir tal política, inclusive toda a equipe afiliada a terceiros que podem ter acesso a qualquer recurso aplicável da **LojaHub LTDA**, inclusive serviços que consumam nosso webservice e/ou API's. Esta política global de privacidade e proteção de dados pessoais aplica-se internacionalmente ao processamento de dados pessoais da **LojaHub LTDA**, seja por meios eletrônicos ou manuais (isto é, em cópia impressa, papel ou formato analógico). Todas as entidades da **LojaHub LTDA** e respectivos funcionários devem cumprir a política global de privacidade e proteção de dados pessoais. A política aplica-se a quaisquer dados pessoais que são criados, coletados, processados, usados, compartilhados ou destruídos para ou pela **LojaHub LTDA**.

4. Informações Coletadas

Nós do **LojaHub LTDA**, coletamos diversas informações pessoais de indivíduos que interagem conosco, sejam eles clientes, visitantes do nosso site, usuários dos nossos produtos ou serviços, parceiros comerciais ou funcionários. As informações coletadas podem incluir, mas não se limitam a:

- **Informações de Identificação Pessoal**: Isso pode incluir nomes, sobrenomes, endereços residenciais, endereços de e-mail, números de telefone, número de identificação como CPF, e outras informações semelhantes.

- **Informações de Identificação Jurídica**: Isso pode incluir nomes, sobrenomes, endereços residenciais, endereços de e-mail, números de telefone, número de identificação como CNPJ e IE(Inscrição Estadual), e outras informações semelhantes.

- **Informações de Conta e Cadastro**: Ao criar uma conta conosco ou se registrar para usar nossos serviços, podemos coletar informações de conta, como nomes de usuário, senhas, preferências de comunicação, histórico de compras e outras informações relacionadas à sua conta.

- **Informações de Pagamento**: Para processar transações financeiras, podemos coletar informações de pagamento, como números de cartão de crédito ou débito, informações de contas bancárias, pix, detalhes de faturamento e outras informações relacionadas ao pagamento.

- **Informações de Uso e Navegação**: Quando você interage com nosso site, aplicativos ou serviços online, podemos coletar automaticamente informações sobre sua atividade, como endereços IP, dados de geolocalização, informações de cookies, registros de servidor, tipos de navegador, tempos de acesso e páginas visualizadas.

- **Informações de Dispositivos**: Podemos coletar informações sobre os dispositivos que você usa para acessar nossos serviços, incluindo informações sobre o dispositivo, como tipo de dispositivo, sistema operacional, identificadores exclusivos de dispositivos e configurações de hardware.

- **Informações de Comunicação**: Podemos coletar informações provenientes de suas interações conosco, incluindo registros de comunicações, como e-mails, mensagens de chat, correspondência, feedback, solicitações de suporte e outras formas de comunicação.

- **Informações de Recrutamento**: Para fins de recrutamento, podemos coletar informações pessoais de candidatos a emprego, como currículos, histórico de emprego, qualificações, referências e outras informações relacionadas ao processo de recrutamento.

Além das informações fornecidas diretamente pelos usuários, também podemos coletar informações de terceiros, como empresas ou pessoas físicas, mediante a sua autorização explícita. Isso pode incluir a integração de contas de terceiros com nossos sistemas, onde os dados são obtidos desses terceiros e incorporados ao nosso canal para permitir o funcionamento esperado de todas as funcionalidades ofertadas pelos sistemas da **LojaHub LTDA.**

As informações coletadas de terceiros podem variar dependendo das permissões concedidas pelo usuário e das políticas de privacidade dos terceiros envolvidos. Essas informações podem incluir, mas não estão limitadas a:

- **Dados de Vendas**: Informações disponíveis via integração com terceiros, onde pode ser obtido dados como cliente, endereço de entrega e valores transacionados. Assim sendo um cliente pode ter: CPF ou CNPJ, IE ou RG, nome completo, telefone, e-mail de contato, endereço residencial, endereço de entrega, produtos adquiridos, valores transacionados, e dados fiscais.

- **Atividades e Interesses do Terceiro**: Informações sobre as atividades, interações, interesses, preferências e outras informações relevantes associadas ao terceiro.

5. Finalidade do Processamento

Todo o dado processado pelos sistemas das **LojaHub LTDA** possuem uma ou mais de uma das seguintes finalidades:

- Permitir a gestão de usuários.

- Permitir a execução das funcionalidades previstas no sistema como gestão de estoque, controle de vendas, emissão fiscal, mediação e comunicação com clientes, entre outras funcionalidades de cunho do negócio.

- Permitir a otimização e recomendação do sistema baseado no uso e interação dos usuários.

- Permitir o aperfeiçoamento e evolução do sistema.

- Permitir a geração de cobranças e faturas ao usuário mediante o uso ou mediante assinatura contratada.

6. Objetivo

Ao utilizar nossos serviços ou interagir com nossas plataformas, você concorda expressamente com a coleta, uso, processamento e compartilhamento de suas informações pessoais, conforme descrito nesta Política de Privacidade e Proteção de Dados Pessoais.

- **Consentimento Voluntário**: Você tem o direito de decidir voluntariamente fornecer suas informações pessoais. Ao fornecer seus dados pessoais para nós e concordar com esta política, você nos dá seu consentimento para processar suas informações de acordo com os termos aqui descritos.

- **Consentimento para Fins Específicos**: Em determinadas circunstâncias, podemos solicitar seu consentimento específico para coletar, processar ou compartilhar suas informações pessoais para fins além daqueles estabelecidos nesta política. Nessas situações, solicitaremos seu consentimento explícito antes de prosseguir com a atividade em questão.

- **Retirada do Consentimento**: Você tem o direito de retirar seu consentimento a qualquer momento, sem afetar a legalidade do processamento com base no consentimento antes da sua retirada. Você pode retirar seu consentimento entrando em contato conosco conforme descrito na seção "**Contato**" desta política.

- **Consequências da Não Fornecimento de Consentimento**: Em alguns casos, a falta de consentimento para o processamento de suas informações pessoais pode impactar nossa capacidade de fornecer determinados serviços ou funcionalidades. Se isso ocorrer, informaremos claramente as consequências de não fornecer o consentimento necessário.

- **Consentimento de Menores**: Se você for menor de idade em sua jurisdição de residência, você só deve fornecer informações pessoais com o consentimento de um dos pais ou responsável legal. Se tomarmos conhecimento de que coletamos informações de um menor de idade sem o consentimento dos pais ou responsável legal, tomaremos medidas para excluir essas informações o mais rápido possível.

7. Segurança dos Dados

A segurança dos seus dados pessoais é uma prioridade para nós. Implementamos medidas técnicas, administrativas e organizacionais para proteger suas informações contra acesso não autorizado, uso indevido, divulgação, alteração e destruição não autorizados. Abaixo estão algumas das práticas de segurança que empregamos:

- **Acesso Restrito**: Limitamos o acesso às suas informações pessoais apenas a funcionários autorizados e que precisam delas para cumprir suas responsabilidades de trabalho. Esses funcionários estão sujeitos a obrigações de confidencialidade e acesso restrito às suas informações, tendo o sigilo dos dados regido por contrato pré afirmado. Ver tópico "**Identificação e Autorização de Acesso às Informações Restritas**" para mais detalhes.

- **Criptografia**: Utilizamos tecnologias de criptografia para proteger suas informações durante a transmissão e armazenamento. Isso inclui o uso de protocolos seguros de comunicação (por exemplo, HTTPS) para proteger a transmissão de dados pela internet. Além disso, para determinados dados pessoais é empregado criptografia "**AES-256-CBC**" de 256 bits garantido assim maior segurança aos dados armazenados.

- **Controles de Acesso**: Implementamos controles de acesso para garantir que apenas indivíduos autorizados tenham acesso às suas informações pessoais. Isso inclui a autenticação de usuários, senhas seguras e a aplicação de políticas de acesso baseadas em função. Ver tópico "**Controles Técnicos para Prevenir o Download de 'PII' em Dispositivos Pessoais**" para mais detalhes.

- **Monitoramento e Auditoria**: Monitoramos continuamente nossos sistemas para detectar e responder a quaisquer ameaças à segurança dos dados. Realizamos auditorias regulares para avaliar a eficácia de nossos controles de segurança e fazer melhorias conforme necessário.

- **Proteção contra Malware e Ataques**: Utilizamos software atualizado de proteção contra *malware* e *firewalls* para proteger nossos sistemas contra ataques cibernéticos, como vírus, *ransomware* e *phishing*. Esporadicamente podemos colocar nossos sistemas a prova, através da contração de serviços de *bug bounty* ou consultorias de segurança da informação.

- **Armazenamento em Repouso**: A depender do uso do dado e de sua importância para a entrega das soluções oferecidas pelos sistemas da **LojaHub LTDA**, pode ser aplicado o armazenamento em repouso, o que de fato está sujeito a aplicação de criptografia ou compressão de dados. Dentro os motivos para armazenamento de repouso está obrigatoriedades legais de armazenamento de dados fiscais, entre outros cenários em que a **LojaHub LTDA** possa ver como necessário ou oportuno este tipo de armazenamento. Além disso, as regras para armazenamento podem ser aprimoradas por requisitos e *compliance* com sistemas integrados, aplicando sob os mesmos as políticas necessárias de modo a jamais reduzir as capacidades de segurança já

estipuladas e aplicadas pela **LojaHub LTDA**.

- **Backup e Recuperação de Dados**: Implementamos procedimentos de backup e recuperação de dados para garantir a disponibilidade e integridade das suas informações em caso de falha de sistema, desastres naturais ou outras emergências.

- **Treinamento de Funcionários**: Fornecemos treinamento regular aos nossos funcionários sobre práticas de segurança de dados, incluindo a conscientização sobre ameaças cibernéticas, procedimentos de segurança e responsabilidades individuais na proteção das informações dos nossos usuários.

8. Identificação e Autorização de Acesso às Informações Restritas

Nossa organização reconhece a importância de identificar e autorizar adequadamente os funcionários que têm acesso às informações restritas de usuários e terceiros integrados ao **LojaHub LTDA**. Para garantir a segurança e a proteção dos dados pessoais de todos, implementamos os seguintes procedimentos:

- **Autenticação de Identidade:** Todos os funcionários que necessitam acessar informações restritas passam por um processo de autenticação de identidade rigoroso. Isso pode incluir, mas não se limita a, autenticação multifatorial, uso de credenciais exclusivas e verificações de segurança adicionais.

- **Autorização de Acesso:** Além da autenticação de identidade, implementamos um sistema de autorização de acesso granular. Cada funcionário recebe acesso apenas às informações necessárias para cumprir suas responsabilidades de trabalho específicas. Esse acesso é revisado e atualizado regularmente de acordo com as mudanças nas funções e responsabilidades dos funcionários.

- **Controle de Acesso Baseado em Funções (RBAC):** Utilizamos um modelo de controle de acesso baseado em funções para garantir que os funcionários tenham acesso apenas às informações relevantes para suas funções específicas na organização. Isso limita o risco de acesso não autorizado ou uso indevido de dados.

- **Registro de Acesso e Auditoria:** Implementamos registros detalhados de todas as atividades de acesso às informações, ajustados conforme o grau de sigilo dos dados. Para garantir a flexibilidade necessária, a aplicação de auditoria pode variar, sendo considerada de acordo com a sensibilidade das informações envolvidas. Esses registros incluem informações sobre os indivíduos que acessaram os dados, horários de acesso e as ações realizadas. No entanto, é importante ressaltar que a extensão da auditoria pode ser adaptada de acordo com a política interna da empresa e a natureza das informações manipuladas. Esses registros são revisados regularmente para garantir total conformidade com nossas políticas internas de segurança de dados, bem

como com os regulamentos de privacidade aplicáveis.

É importante ressaltar que a segurança e a proteção dos dados pessoais dos usuários são prioridades fundamentais para nossa organização. Estamos comprometidos em manter práticas de segurança modernas, robustas e em garantir que todos os funcionários sigam rigorosamente nossas políticas e procedimentos de segurança de dados.

9. Controles Técnicos para Prevenir o Download de “PII” em Dispositivos Pessoais

Nossa organização reconhece a importância de implementar controles técnicos robustos para prevenir o download não autorizado de informações pessoalmente identificáveis (PII) nos dispositivos pessoais dos funcionários. Para garantir a segurança e a proteção dos dados, adotamos as seguintes medidas:

- **Política de Restrição de Download:** Implementamos uma política clara que proíbe explicitamente o download de PII em dispositivos pessoais dos funcionários, a menos que seja estritamente necessário para o desempenho das suas funções de trabalho e de acordo com os procedimentos estabelecidos.

- **Controles de Acesso e Autenticação:** Utilizamos sistemas de gerenciamento de acesso e autenticação para garantir que apenas funcionários autorizados tenham permissão para acessar e baixar informações sensíveis. Isso inclui autenticação multifatorial e restrições de acesso baseadas em funções.

- **Procedimentos de Alerta e Resposta:** Além dos controles técnicos, estabelecemos procedimentos claros para alertar e responder a tentativas de download não autorizado de informações pessoalmente identificáveis (PII) nos dispositivos pessoais dos funcionários:

    - **Alertas Automatizados:** Aplicamos sistemas de alerta automatizados que detectam e notificam imediatamente nossa equipe de segurança da informação sobre qualquer tentativa de download de PII nos dispositivos pessoais dos funcionários.

    - **Avaliação e Resposta:** Uma vez alertados, nossa equipe de segurança da informação conduz uma avaliação detalhada do incidente para determinar a extensão do acesso não autorizado e tomar medidas corretivas imediatas. Isso pode incluir a remoção remota dos dados comprometidos e a aplicação de medidas disciplinares conforme necessário.

Estamos comprometidos em garantir a integridade e a confidencialidade dos dados pessoais dos nossos usuários e em tomar todas as medidas necessárias para protegê-los contra acesso não autorizado e uso indevido.

10. Transferência Internacional de Dados

Como uma organização global, podemos transferir suas informações pessoais para fora do seu país de residência, incluindo para países que podem ter padrões de proteção de dados diferentes dos do seu país. Essas transferências podem ser necessárias para cumprir nossas obrigações contratuais com você, fornecer serviços ou produtos solicitados por você, ou para outros fins legítimos descritos nesta Política de Privacidade.

Ao fornecer suas informações pessoais para nós e concordar com esta Política de Privacidade, você concorda com a transferência de suas informações para fora do seu país de residência. Tomaremos medidas para garantir que suas informações continuem a ser protegidas de acordo com os padrões de segurança descritos nesta política, independentemente do local para onde são transferidas.

Quando transferimos suas informações pessoais para países que não oferecem o mesmo nível de proteção de dados que o seu país de residência, implementaremos medidas apropriadas para garantir a proteção adequada de suas informações. Isso pode incluir a celebração de contratos de transferência de dados com destinatários das informações ou a adesão a esquemas de certificação de proteção de privacidade reconhecidos internacionalmente.

Se desejar obter mais informações sobre as medidas específicas que implementamos para proteger suas informações durante a transferência internacional de dados, entre em contato conosco conforme descrito na seção "**Contato**" desta política.

11. Retenção de Dados

Mantemos suas informações pessoais apenas pelo tempo necessário para os fins para os quais foram coletadas e em conformidade com as leis e regulamentos aplicáveis. O período de retenção de dados pode variar dependendo do tipo de informação e dos fins para os quais é processada. Abaixo estão algumas das considerações que levamos em conta ao determinar o período de retenção de dados:

- **Finalidade do Processamento**: Retemos suas informações pessoais pelo tempo necessário para cumprir as finalidades para as quais foram coletadas. Por exemplo, podemos reter suas informações enquanto você mantiver uma conta ativa conosco, enquanto o usuário estiver inadimplente ou enquanto for necessário para fornecer os serviços ou produtos solicitados por você.

- **Obrigações Contratuais**: Se você for um cliente ou usuário dos nossos

serviços, podemos reter suas informações pelo tempo necessário para cumprir nossas obrigações contratuais com você, resolver disputas, fazer cumprir nossos termos e condições ou proteger nossos interesses legítimos.

- **Requisitos Legais**: Em alguns casos, podemos ser obrigados por lei a reter suas informações pessoais por um período mais longo do que o necessário para as finalidades originais de processamento. Nesses casos, seguiremos os requisitos legais de retenção de dados aplicáveis.

- **Consentimento do Titular dos Dados**: Se coletarmos suas informações com base no seu consentimento, reteremos essas informações pelo tempo necessário para cumprir as finalidades para as quais você deu seu consentimento, a menos que você retire seu consentimento mais cedo.

- **Interesses Legítimos**: Em certas circunstâncias, podemos reter suas informações pessoais por um período mais longo se for necessário para proteger nossos interesses legítimos, como prevenir fraudes, garantir a segurança dos nossos sistemas ou cumprir obrigações regulatórias.

Após o término do período de retenção aplicável, suas informações pessoais serão excluídas, anonimizadas ou de outra forma tornadas irreversivelmente não identificáveis, a menos que haja uma razão legítima para retê-las por mais tempo, como exigido por lei ou para o exercício ou defesa de reivindicações legais.

12. Direitos dos Titulares dos Dados

Você tem direitos em relação às suas informações pessoais que coletamos e processamos. Abaixo estão resumidos os principais direitos que você possui:

- **Direito de Acesso**: Você tem o direito de solicitar detalhes sobre as informações pessoais que mantemos sobre você, incluindo o propósito do processamento, as categorias de informações pessoais envolvidas e os destinatários aos quais as informações foram ou serão divulgadas.

- **Direito de Retificação**: Se suas informações pessoais estiverem imprecisas ou incompletas, você tem o direito de solicitar a correção ou complementação dessas informações.

- **Direito de Exclusão**: Você pode solicitar a exclusão das suas informações pessoais em determinadas circunstâncias, como quando as informações não são mais necessárias para os fins para os quais foram coletadas ou quando você retira seu consentimento para o processamento.

- **Direito de Restrição de Processamento**: Em certas situações, você pode solicitar a restrição do processamento das suas informações pessoais, por exemplo, quando você contesta a precisão das informações ou quando o processamento é ilegal,

mas você se opõe à exclusão.

- **Direito à Portabilidade de Dados**: Se processarmos suas informações pessoais com base no seu consentimento ou para executar um contrato, você pode solicitar uma cópia das suas informações em um formato estruturado “CSV”, comumente usado e legível por máquina, ou pode solicitar que as informações sejam transmitidas diretamente para outro controlador de dados, quando tecnicamente viável, integrado ao sistema e disponível, para maiores detalhes entre em contato conosco conforme descrito na seção “**Contato**”.

- **Direito de Oposição ao Processamento**: Você tem o direito de se opor ao processamento das suas informações pessoais em certas circunstâncias, como quando processamos suas informações para fins de marketing direto ou quando o processamento é baseado em interesses legítimos.

- **Direito de Retirar o Consentimento**: Se processarmos suas informações com base no seu consentimento, você tem o direito de retirar esse consentimento a qualquer momento. A retirada do consentimento não afetará a legalidade do processamento com base no consentimento antes da retirada.

Para exercer esses direitos ou fazer uma solicitação relacionada à privacidade de dados, entre em contato conosco conforme descrito na seção "**Contato**" desta política. Responderemos às suas solicitações dentro dos prazos e de acordo com os requisitos legais aplicáveis.

Por favor, esteja ciente de que podemos solicitar informações adicionais para confirmar sua identidade antes de processar sua solicitação.

13. Responsabilidades dos Funcionários

Nossos funcionários desempenham um papel crucial na proteção da privacidade e segurança dos dados pessoais dos nossos usuários, clientes e parceiros integrados. Todos os funcionários são orientados e instruídos a seguir estas diretrizes para garantir a conformidade com as leis de privacidade de dados e as políticas internas da organização:

Treinamento e Conscientização: Todos os funcionários recebem treinamento regular sobre as políticas e práticas de privacidade de dados da organização. Eles são informados sobre a importância da proteção dos dados pessoais e os procedimentos a serem seguidos para garantir a conformidade com as leis de privacidade aplicáveis.

Princípio da Necessidade: Os funcionários são orientados a coletar, acessar e usar apenas as informações pessoais necessárias para cumprir suas responsabilidades de trabalho. Eles devem garantir que não haja acesso não autorizado ou uso indevido das informações pessoais dos usuários.

Confidencialidade: Os funcionários são obrigados a manter a confidencialidade das informações pessoais dos usuários e clientes, tanto durante o emprego quanto após o término do emprego. Eles devem proteger as informações pessoais contra acesso não autorizado, divulgação ou uso indevido.

Segurança dos Dados: É responsabilidade de cada funcionário seguir as práticas de segurança de dados estabelecidas pela organização para proteger as informações pessoais dos usuários contra acesso não autorizado, perda, destruição, roubo ou comprometimento.

Notificação de Violações de Dados: Os funcionários são incentivados a relatar prontamente qualquer suspeita de violação de dados ou falha de segurança à equipe responsável pela proteção de dados da organização. Eles devem seguir os procedimentos estabelecidos para relatar incidentes de segurança e cooperar nas investigações relacionadas.

Atualização e Conformidade: Os funcionários devem manter-se atualizados sobre as mudanças nas leis de privacidade de dados e nas políticas internas da organização. Eles são responsáveis por garantir sua conformidade contínua com as políticas e procedimentos de privacidade de dados da organização.

O não cumprimento das responsabilidades de privacidade de dados pode resultar em medidas disciplinares, incluindo advertências, suspensões ou rescisões do contrato de trabalho, conforme a gravidade da violação e as políticas internas da organização.

14. Desenvolvimento de Código Seguro

Este tópico abrange todos os procedimentos adotados e orientações fornecidas às equipes de desenvolvimento da **LojaHub LTDA** para garantir a entrega de um código seguro, empregando os melhores princípios de qualidade e segurança no desenvolvimento de software. Estes princípios incluem:

- **Security by Design**: Durante todo o processo de desenvolvimento, desde o planejamento inicial, aplicamos os princípios estabelecidos no padrão de Segurança pelo Design (Security by Design). Isso significa que a segurança dos dados é considerada desde a concepção do software ou de novas funcionalidades.

- **Planejamento de Segurança**: Etapa fundamental deste processo, onde se identifica todos os requisitos de segurança que serão aplicados ao projeto. Isso inclui aspectos relacionados à proteção de dados, criptografia, gerenciamento de chaves, *tokens*, entre outros. Todos os requisitos de segurança devem ser documentados e validados.

- **Padronização**: A padronização e a criação de protótipos de código facilitam a

validação de segurança, tornando os processos mais eficientes. A padronização ajuda na detecção e correção mais rápida de erros ou problemas de segurança.

- **Requisitos de Segurança**: Este tópico fornece sugestões de ferramentas, bibliotecas e boas práticas que garantem que os códigos desenvolvidos sejam seguros e que mitiguem possíveis ameaças. É essencial lembrar que todos os sistemas estão sujeitos a problemas de segurança e que podem sofrer incidentes. Portanto, é crucial estar sempre atento a *logs*, atualizações e falhas reportadas, aplicando correções e atualizações o mais rápido possível.

- **Boas Práticas de Codificação Segura**:

    - **Não Hardcode de Credenciais Sensíveis**: Desenvolvedores devem evitar a inclusão de credenciais sensíveis no código, como chaves de criptografia, chaves de acesso secretas ou senhas. Estas informações devem ser armazenadas de forma segura, fora do código-fonte.

    - **Gestão de Repositórios**: Credenciais sensíveis não devem ser expostas em repositórios de código público. Repositórios privados e sistemas de gerenciamento de segredos devem ser utilizados prioritariamente.

    - **Ambientes Separados**: É extremamente importante manter ambientes de desenvolvimento, teste e produção separados para garantir a segurança das aplicações e dos dados. Dados de produção não devem ser utilizados em ambientes de desenvolvimento ou teste.

    - **Revisão e Auditoria de Código**: Implementar processos regulares de revisão e auditoria de código para identificar e corrigir vulnerabilidades de segurança.

    - **Atualização e Manutenção**: Manter todas as bibliotecas, *frameworks* e dependências atualizadas para proteger contra vulnerabilidades conhecidas.

15. Procedimentos de Resposta a Incidentes

Nosso compromisso com a proteção dos dados pessoais dos nossos usuários e clientes inclui a implementação de procedimentos de resposta a incidentes para lidar prontamente com qualquer violação de dados que possa ocorrer. Abaixo estão os passos que seguimos em caso de incidentes de segurança de dados:

Identificação do Incidente: Nossa equipe de segurança da informação monitora continuamente nossos sistemas em busca de atividades suspeitas que possam indicar uma possível violação de dados. Se um incidente de segurança for detectado ou suspeitado, ele será imediatamente investigado para determinar a natureza e a extensão do incidente.

Contenção e Mitigação: Uma vez identificado um incidente de segurança,

tomamos medidas imediatas para conter e mitigar qualquer dano potencial. Isso pode incluir a interrupção do acesso não autorizado, a remoção de *malware*, a correção de vulnerabilidades de segurança e outras ações necessárias para impedir a continuação do incidente.

Avaliação de Risco: Realizamos uma avaliação detalhada do risco associado ao incidente de segurança, considerando fatores como a sensibilidade dos dados afetados, o número de indivíduos afetados, as consequências potenciais para os indivíduos afetados e outras considerações relevantes.

Plano de Resposta a Incidentes: Mantemos um "**Plano de Resposta a Incidentes"** documentado e atualizado, consultar tópico **"Referências"**, que descreve os procedimentos específicos a serem seguidos em caso de incidente de segurança. Este plano inclui atribuições de responsabilidades, procedimentos de comunicação, etapas de mitigação e outros detalhes importantes para garantir uma resposta eficaz e coordenada ao incidente.

Notificação às Autoridades Competentes: Se necessário, notificamos as autoridades reguladoras de proteção de dados competentes sobre a violação de dados de acordo com os requisitos legais aplicáveis. Nosso objetivo é cooperar plenamente com as autoridades reguladoras e fornecer todas as informações necessárias para investigar e resolver o incidente. Também podemos realizar comunicações de notificações sobre o incidente para parceiros ou terceiros, para isso mantemos atualizado no "**Plano de Resposta a Incidentes"** o tópico "**Notificação a terceiros**".

Comunicação aos Titulares dos Dados Afetados: Se determinarmos que a violação de dados pode resultar em um alto risco para os direitos e liberdades dos indivíduos afetados, notificaremos prontamente os titulares dos dados afetados sobre a violação de acordo com os requisitos legais aplicáveis. A notificação será clara, transparente e fornecerá informações sobre o incidente e as medidas que estão sendo tomadas para mitigar o impacto. Versa no "**Plano de Resposta a Incidentes"** no tópico "**Notificação a terceiros**" a lista e informações sobre os terceiros ao qual o **LojaHub LTDA** se compromete a notificar em caso de incidentes de segurança.

Melhoria Contínua: Após a resolução do incidente de segurança, realizamos uma revisão pós-incidente para identificar lições aprendidas e oportunidades de melhoria nos nossos processos de segurança de dados. Implementamos medidas corretivas para fortalecer nossas defesas e prevenir incidentes futuros.

16. Atualizações da Política

Nossa Política de Privacidade e Proteção de Dados Pessoais pode ser atualizada periodicamente para refletir mudanças nas leis de proteção de dados, práticas da

indústria e atualizações nos nossos serviços ou tecnologias. Recomendamos que você revise esta política regularmente para estar ciente de quaisquer alterações. Quando fizermos atualizações significativas nesta política, forneceremos um aviso destacado em nosso site ou aplicativo, e quando apropriado, solicitaremos seu consentimento para as alterações.

17. Contato para Questões de Privacidade

Se você tiver dúvidas, preocupações ou solicitações relacionadas à sua privacidade ou ao uso das suas informações pessoais, entre em contato conosco através dos seguintes meios:

E-mail: **contato@lojahub.com.br**

Correio: **Rua Cabo Antônio Pinton, 31 – Parque Novo Mundo, São Paulo - SP**.

Nós nos esforçamos para responder a todas as consultas sobre privacidade de forma oportuna e eficaz. Se você entrar em contato conosco por e-mail, faremos o possível para responder dentro de 2 dias úteis. Se preferir nos contatar por correio, responderemos à sua consulta no prazo de 30 dias úteis após recebermos sua correspondência.

18. Referencias

Plano de Resposta a Incidentes: Acessível em https://lojahub.com.br/docs/plano_de_respostas_a_incidentes