Política de Uso Aceitável LojaHub (pt-BR)

1. Este documento define a Política de Uso Aceitável (ou simplesmente "PUA") do sistema LojaHub. Seu objetivo é orientar a utilização adequada e responsável da LojaHub.

2. Violações de sistemas ou de segurança de quaisquer redes são práticas proibidas e resultam na responsabilização cível e criminal de seu infrator. A LojaHub irá investigar quaisquer incidentes envolvendo tais violações e irá cooperar com as autoridades cíveis e criminais responsáveis nos casos de suspeita de violações.

3. O uso aceitável dos serviços da LojaHub é sempre ético, honesto, e respeita os direitos individuais, inclusive os direitos à privacidade, personalidade e inviolabilidade.

4. Constituem restrições à utilização dos serviços da LojaHub, as quais deverão ser seguidas por todos os Clientes e Usuários dos serviços da LojaHub, as abaixo listadas, devendo, ainda, serem observadas outras políticas de utilização aceitáveis, de Clientes LojaHub, de Plataformas de Serviços Digitais, de Marketplaces, de Loja Virtuais, ou de qualquer outra rede de dados ou integração com parceiros LojasHub, desde que não conflitantes com o presente documento:

4.1. É proibido o envio de mensagens não solicitadas, incluindo, mas não se limitando a, quantidade significativas de mensagens com publicidade comercial ("spam") ou anúncios informativos que possam vir a prejudicar os serviços providos pela LojaHub ou, ainda, mensagens que gerem reclamações dos receptores de tais e-mails não solicitados;

4.2. É proibida a prática ou tentativa de burlar e/ou violação de qualquer protocolo utilizado para a transmissão de informações na rede de comunicação de dados com a LojaHub;

4.3. Nenhum serviço, sistema ou integração da LojaHub pode ser utilizado para finalidades ilegais e/ou não éticas que violem quaisquer leis locais, estaduais, nacionais ou acordos internacionais;

4.4. É vedado o uso do sistema LojaHub para obtenção de acesso não autorizado a dados, sistemas ou redes, incluindo, mas não se limitando a qualquer tentativa de investigação, exames ou testes de vulnerabilidade;

Parágrafo único – O uso indevido do sistema LojaHub constitui crime podendo o usuário ser responsabilizado penalmente pela prática de seus atos.

5. Quaisquer reclamações referentes a (i) incidentes de segurança, como uso ilegal do sistema por pessoas não autorizadas, infringindo quaisquer mecanismos de segurança ou ferindo direitos individuais, deverão ser enviadas ao endereço eletrônico **suporte@lojahub.com.br** e (ii) referentes a abuso no envio de mensagens eletrônicas ("e-mail") e spam deverão ser enviadas ao endereço eletrônico **suporte@lojahub.com.br**;

6. A LojaHub reserva-se ao direito de modificar esta PUA, a qualquer momento e sem aviso prévio, sendo que será válido o documento que estiver disponível no seguinte endereço eletrônico: **http://www.lojahub.com.br/pua**. As provisões contidas nesta PUA não encerram as restrições de uso do sistema LojaHub.

Plano de Resposta a Incidentes

A equipe de desenvolvimento do Lojahub atua fortemente na contenção de problemas e incidentes de segurança, adotando o seguinte protocolo prevenção e ações:

1. Prevenção

1.1. Para prevenção e realização de testes quantitativos e de versionamento, possuímos ambientes de desenvolvimento, homologação e produção. Todos os desenvolvedores do Lojahub possuem acesso e permissão para utilizar tanto nosso ambiente de desenvolvimento como o de homologação. Entretanto, nosso ambiente de produção é restrito apenas aos responsáveis por realizar o deploy em produção, que são justamente os profissionais qualificados e treinados para este processo.

1.2. Utilização de containers Docker com imagens idênticas nos ambientes de homologação e produção.

1.3. O plano de Reposta a Incidentes deve ser revisado a cada 6 meses.

2. Preparação

2.1. Todos os desenvolvedores e equipe de suporte do Lojahub são orientados desde os seus primeiros dias de empresa a sempre que diagnosticarem falhas ou erros de processamentos do sistema repassar rapidamente à equipe de testes, para estar dar segmento e analisar mais a fundo a falha.

2.2. A equipe de testes também é responsável por monitorar e acompanhar erros produzidos pelo sistema durante sua execução, analisando para isso os logs gerados pelo próprio sistema assim como também analisar as métricas de erros e sucessos nas apis e sistemas integrados que disponibilizarem tais dados.

2.3. Mensalmente serão realizadas reuniões com membros de toda a equipe Lojahub para transmissão de novidades do sistema, pontos de atenção e orientação sobre o tratamento de situações adversas.

2.4. Toda vez que um deploy é feito para produção, toda a equipe de desenvolvimento, suporte e testes é orientada sobre a atualização e como proceder caso seja diagnosticado possíveis incidentes.

2.5. Sempre que houver atualizações de riscos ou de impacto estruturais, será emitido notificações a todos os usuários do sistema, manifestando nossa nota de atualização e orientando o usuário quando necessário sobre possíveis falhas que podem aparecer, assim como também o orientando também a como agir caso se depare com algum problema.

3. Análise

3.1. Toda falha relatada ou submetida a equipe responsável por testes deverá gerar um breve relatório sobre o resultado da análise. Neste ponto é que falhas ou incidentes podem ser descaracterizados e terem suas relevâncias reduzidas ou até mesmo serem descartados.

3.2. Neste processo também ocorre a categorização de prioridade do incidente, onde através deste processo é dado a devida atenção e prioridade para resolução do problema.

3.3. Os incidentes serão categorizados pelo nível de suas falhas, de forma que possibilite a realização de suas correções conforme as necessidade e prioridades presentes no sistema sendo estas em ordem de menor impacto para de maior impacto:

3.3.1. Mínimo, no qual a falha tem muito baixo nível de impacto do sistema e não interfere o funcionamento das atividades do sistema.

3.3.2. Baixo, no qual a falha começa a interferir esporadicamente ou sobre situações restritas no funcionamento da atividade do sistema.

3.3.3. Médio, no qual a falha começa contempla a todos os usuários do sistema e se restringe a poucos fluxos de atividades.

3.3.4. Alto, no qual a falha interfere fluxos do sistema, a ponto de tornar-se inutilizáveis funções ou até mesmo o sistema como um todo. Entram também nesta classificação, falhas de integração ou comunicação com outras API's de sistemas integrados ao Lojahub.

3.3.5. Extrema, falhas de segurança, violações de privacidades, servidores e containers, protocolos de segurança vencidos e falhas demais incidentes que impeçam ou afetem mais de 5% dos usuários ao mesmo tempo.

3.3.4. Assim, tendo diagnosticado e classificado o incidente, temos por concluído a etapa de análise.

4. Contensão

4.1. Neste processo é tomado a devida providência imediata para resolução do problema, sendo divido em dois tipos de providências, as quais classificamos por:

- Contenção curta, neste tipo de providência, realizamos em instantes a melhor solução prevista por nossa equipe de responsáveis técnicos para parar o incidente. Este tipo de contenção comumente mais utilizado em caso em que não se tem o diagnóstico completo do problema ou não se tem uma ação plausível para solucionar em definitivo o problema. Neste contesto de providencias fazem parte também a reinicialização do sistema, de containers ou alocação de serviços em nova instancia. Em resumo, adotando este tipo de providência, se busca sempre impedir que a ameaça se espalhe e que os danos sejam maiores.

- Contenção longa, já neste caso, visa-se aplicar uma solução de reversão do sistema para um ponto anterior e estável perante o incidente, neste ponto pode ser necessário até mesmo a reversão de backups.

5. Erradicação

5.1. Ao chegar nessa etapa, será com cautela e muita análise, será produzida uma solução em ambiente de homologação, a qual será submetida a diversos testes. Somente então após a estabilização e confirmação da insistência de incidentes nessa versão é que será publicada em produção.

5.2. É importante também que instantes antes da aplicação e liberação da atualização em ambiente de produção, que seja realizados todos os backups necessários, para facilitar assim em caso de emergência uma rápida restauração do sistema.

5.3. Está atualização final pode ainda ser fragmenta em partes(features) menores, a ponto de ir submetendo parte a parte toda a atualização de correção e estabilização do sistema, com intervalos de ao menos 2 dias, afim de se validar a ocorrência de incidentes.

6. Recuperação

6.1. Como rotina de recuperação a falhas e garantia de acessibilidade a informações durante incidentes, o sistema Lojahub adota as seguintes estratégias para tratar e guardar informações relevantes ao sistema e aos usuários.

6.1.1 Ao menos uma vez na semana ou sempre à anteceder atualizações estruturais será realizado backup em nuvem dos bancos de dados do sistema Lojahub.

6.1.2. O Lojahub possui ainda repositório de versionamento privado, que garante o armazenamento seguro e confiável de todas as instancias serverless do sistema. Garantindo assim uma gestão e armazenamento seguro do código fonte.

6.1.3. Arquivos de usuário como imagens, vídeos, arquivos zip, pdfs, estarão sempre armazenados e sendo assegurados por uma instancia de armazenamento isolada do tipo CDN (Content Delivery Network). Cuja qual, possuí seus próprios métodos e rotinas de backup e higienização.

6.1.4. Das imagens do Sistema Operacional e execução de softwares e dependências de ambiente, a plataforma Lojahub adota técnicas de container Docker e Docker Swarm, salvos em repositórios seguros de versionamento e estáveis. Dessa forma, utilizando o conceito de auto escalonamento, o sistema consegue sobreviver a falhas operacionais e se replicar conforme a demanda.

6.5. Dispostos as rotinas de segurança adotadas para manutenção e backup do sistema, o Lojahub ao seguilas fielmente se torna capaz capaz de se recuperar a todos os tipos incidentes, restaurando se necessário imagens em novos containers, restauração de imagem do banco de dados, ou mesmo subir novas máquinas utilizando o próprio sistema Lojahub e suas imagens e dados salvos. E também, garantir a segurança de dados salvos no sistema, seja pelo nosso CDN, seja pelos backups de banco de dados.

7. Balanço

6.1. A partir do momento que temos o sistema de volta aos trilhos, operando normalmente e recuperado do incidente, reunimos toda a equipe envolvida para participar de uma reunião a ser relatada em ata. Na qual debatemos todo o problema e dificuldades enfrentadas, analisamos e discutimos as causas do incidente, e concluímos com o que podemos fazer para que isso não volte a ocorrer, de forma a aplicar novas rotinas ou passas para serem aplicados na gestão de processo, de equipe e de deploy.

6.2. Durante o balanço é também avaliado os danos resultantes do incidente, comparado taxas de usuários antes e após o incidente, bem como métricas de fluxo de dados entre os servidores e demanda.

6.3. É verificado a possibilidade de recorrência desse incidente. Se diagnosticado que este incidente vem se repetindo com certa regularidade, medidas mais severas deverão ser tomadas. Dentre as ações: alteração na gestão da equipe, alterações de estrutura, migração de servidores, refatoramento de códigos, alteração nos membros da equipe, contratação de mão de obra ou consultoria com especialistas neste tipo de incidente, entre outras.

O que posso fazer para me proteger?

1. Algumas dicas para bom uso da internet para usuários residenciais:

1.1. Tenha um bom antivírus instalado e atualizado;

1.2. Não abra e-mails enviados por desconhecidos;

1.3. Não execute arquivos de fontes não confiáveis;

1.4. Se o seu computador está se comportando estranhamente e você desconfia que ele pode ter se tornado um “zumbi”, procure um técnico;

2. Se você é administrador de um servidor ou rede, seguem algumas dicas:

2.1. Procure a documentação dos softwares usados em seu servidor, a fim de que eles não estejam configurados de um jeito que permita a exploração por pessoas maliciosas e/ou criminosas;

2.2. Proteja sua rede contra ataques externos.

Acceptable Use Policy LojaHub (en-US)

1. This document defines an Acceptable Use Policy (PUA) of the LojaHub system. Its purpose is to be oriented towards a proper and responsible use of LojaHub.

2. Violations of security or data protection systems are prohibited and result in civil and criminal liability of your violator. LojaHub will investigate the incidences of such violence and will cooperate as civil and criminal authorities in cases of suspected violations.

3. The use of the services of the LojaHub is seminar, law, and individual rights, including the rights to privacy, personality and inviolability.

4. To constitute restrictions on the use of LojaHub services, such as the following ones, and other acceptable usage policies of LojaHub Customers, Digital Services Platforms, Marketplaces, Virtual Store, any other exchange of data or integration with LojasHub, provided they do not conflict with this document:

4.1. Unauthorized text messaging is prohibited, including but not limited to the communication of commercial messages (spam) or information that may be impaired in the services provided by LojaHub, or messages that generate complaints from recipients of such messages. unsolicited emails;

4.2. The practice of attempting to circumvent and / or violate any type of information used for the transmission of information in the communication network with LojaHub is prohibited;

4.3. A Store service, system, or integration may be used for unlawful and / or unethical purposes that violate local, state, national, or international agreements;

4.4. The use of the LojaHub system for access to unauthorized data, systems or networks, including, but not limited to, any attempt to investigate, test or test for vulnerability is prohibited;

Sole Paragraph - The improper use of the LojaHub system, the user is criminally liable for the practice of his acts.

5. Any complaints regarding (i) security incidents, such as the use of the system by unauthorized persons, in violation of the same security principles or individual rights, must be registered at the e-mail address **suporte@lojahub.com.br** and (ii) Bibliographic references in electronic mail ("e-mail") and spam should be sent to the e-mail address **suporte@lojahub.com.br**;

6. LojaHub reserves the right to change this AUP at any time and without prior notice, and the document will be available at the following electronic address: **https://www.lojahub.com.br/pua**. The provisions contained in this AUP can not be terminated as a restriction on the use of the LojaHub system.

Incident Response Plan

The Lojahub development team acts strongly in containing security problems and incidents, adopting the following prevention protocol and actions:

1. Prevention

1.1. To prevent and carry out quantitative and versioning tests, we have development, approval and production environments. All Lojahub developers have access and permission to use both our development and homologation environments. However, our production environment is restricted only to those responsible for deploying to production, who are precisely the qualified and trained professionals for this process.

1.2. Use of Docker containers with identical images in the approval and production environments.

1.3. The Incident Response plan must be reviewed every 6 months.

2. Preparation

2.1. All Lojahub developers and support staff are guided from their first days at the company whenever they diagnose system processing errors or errors, quickly pass it on to the testing team, to be able to segment and analyze the failure further.

2.2. The test team is also responsible for monitoring and tracking errors produced by the system during its execution, analyzing the logs generated by the system itself as well as analyzing the metrics of errors and successes in the apis and integrated systems that make such data available.

2.3. Monthly meetings will be held with members of the entire Lojahub team to transmit system news, points of attention and guidance on the treatment of adverse situations.

2.4. Every time a deployment is made for production, the entire development, support and testing team is guided on the update and how to proceed if possible incidents are diagnosed.

2.5. Whenever there are risks or structural impact updates, notifications will be issued to all users of the system, expressing our update note and guiding the user when necessary about possible failures that may appear, as well as also advising on how to act if encounter a problem.

3. Analysis

3.1. Any failure reported or submitted to the testing team must generate a brief report on the analysis result. It is at this point that failures or incidents can be uncharacterized and have their relevance reduced or even be discarded.

3.2. In this process there is also the categorization of priority of the incident, where through this process due attention and priority is given to solving the problem.

3.3. The incidents will be categorized by the level of their failures, in a way that makes it possible to carry out their corrections according to the needs and priorities present in the system, these being in order of less impact to greater impact:

3.3.1. Minimum, in which the fault has a very low level of system impact and does not interfere with the operation of the system activities.

3.3.2. Low, in which the fault begins to interfere sporadically or on restricted situations in the functioning of the system's activity.

3.3.3. Medium, in which the failure begins, covers all users of the system and is restricted to a few activity flows.

3.3.4. High, in which the failure interferes with system flows, to the point that functions or even the system as a whole become unusable. Also included in this classification are failures of integration or communication with other APIs of systems integrated with Lojahub.

3.3.5. Extreme security breaches, privacy violations, servers and containers, expired security protocols and other incidents that prevent or affect more than 5% of users at the same time.

3.3.4. Thus, having diagnosed and classified the incident, we have concluded the analysis stage.

4. Containment

4.1. In this process, immediate action is taken to resolve the problem, being divided into two types of measures, which we classify by:

- Short restraint, in this type of action, we carry out in an instant the best solution provided by our team of responsible technicians to stop the incident. This type of containment is most commonly used in cases where the problem has not been fully diagnosed or if there is no plausible action to definitively solve the problem. This challenge is also part of the system reset, of containers or allocation of services in a new instance. In short, by adopting this type of measure, the aim is always to prevent the threat from spreading and the damage from being greater.

- Long contention, in this case, the aim is to apply a solution to revert the system to a previous and stable point before the incident, at this point even the reversion of backups may be necessary.

5. Eradication

5.1. Upon reaching this stage, it will be with caution and much analysis, a solution will be produced in an approval environment, which will be subjected to various tests. Only then, after the stabilization and confirmation of the insistence of incidents in this version, will it be published in production.

5.2. It is also important that moments before the application and release of the update in the production environment, that all necessary backups are carried out, in order to facilitate, in case of emergency, a quick system restoration.

5.3. This final update can also be fragmented into smaller parts (features), to the point of submitting part of the entire system correction and stabilization update, with intervals of at least 2 days, in order to validate the occurrence of incidents.

6. Recovery

6.1. As a routine for recovering from failures and ensuring access to information during incidents, the Lojahub system adopts the following strategies to treat and store information relevant to the system and users.

6.1.1 At least once a week or always before structural updates will be backed up in the cloud to the databases of the Lojahub system.

6.1.2. Lojahub also has a private versioning repository, which guarantees safe and reliable storage of all serverless instances of the system. Thus guaranteeing safe management and storage of the source code.

6.1.3. User files such as images, videos, zip files, pdfs, will always be stored and secured by an isolated storage instance of the type CDN (Content Delivery Network). Whose, have their own methods and routines for backup and cleaning.

6.1.4. From the images of the Operating System and execution of software and environment dependencies, the Lojahub platform adopts Docker and Docker Swarm container techniques, saved in secure versioning and stable repositories. Thus, using the concept of self-scheduling, the system is able to survive operational failures and replicate according to demand.

6.5. Having arranged the security routines adopted for maintenance and backup of the system, Lojahub will follow you faithfully and be able to recover from all types of incidents, restoring images if necessary in new containers, restoring the database image, or even uploading new machines using the Lojahub system itself and its saved images and data. And also, to guarantee the security of data saved in the system, either through our CDN, or through database backups.

7. Balance sheet

6.1. From the moment we have the system back on track, operating normally and recovered from the incident, we gathered the entire team involved to participate in a meeting to be reported in the minutes. In which we discuss all the problems and difficulties faced, we analyze and discuss the causes of the incident, and we conclude with what we can do so that this does not happen again, in order to apply new routines or steps to be applied in the process management, team and deploy.

6.2. During the assessment, damage resulting from the incident is also assessed, comparing user rates before and after the incident, as well as data flow metrics between servers and demand.

6.3. The possibility of recurrence of this incident is verified. If diagnosed that this incident has been repeated with certain regularity, more severe measures should be taken. Among the actions: changes in team management, changes in structure, migration of servers, refactoring of codes, changes in team members, hiring of labor or consulting with specialists in this type of incident, among others.

What can I do to protect myself?

Some tips for good internet use for residential users:

• Have a good antivirus installed and updated;

• Do not open emails sent by strangers;

• Do not run files from untrusted sources;

• If your computer is behaving strangely and you suspect it may have become a "zombie", seek a technician;

If you are a server or network administrator, here are some tips:

• Look for documentation of the software used on your server so that it is not configured in a way that allows malicious and / or criminal exploitation;

• Protect your network from external attacks.