Plano de Resposta à Incidentes
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 02.186-000, São Paulo-SP, Brasil, desenvolvedora e mantenedora de sistemas, versa neste documento sobre a definição do Plano de Resposta à Incidentes dos sistemas desenvolvidos e/ou geridos pela **LojaHub LTDA**. Tendo como objetivo a definição de estratégias de contenção de problemas e incidentes de segurança, adotando este protocolo prevenção e ações a serem realizadas mediante qualquer tipo de incidente.

No momento que foi redigido este documento são sistemas de propriedade da **LojaHub LTDA**, os seguintes:

- LojaHub Hub & ERP – https://lojahub.com.br
- LojaHub Analytics – https://analytics.lojahub.com.br
- LojaHub Financeiro – em fase de pré lançamento
- Total Connect – https://totalconnect.com.br

Parágrafo Único: Este documento é válido para todos os sistemas desenvolvidos e comercializados pela empresa **LojaHub LTDA**.

2. Prevenção

2.1. Para prevenção e realização de testes quantitativos e de versionamento, possuímos ambientes de desenvolvimento, homologação e produção. Todos os desenvolvedores do **LojaHub LTDA** 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.

2.2. Utilização de conceito de “conteinerização” com imagens idênticas nos ambientes de homologação e produção, estando estas constantemente atualizadas.

2.3. Atualização frequente de *frameworks*, dependências e pacotes de terceiros, bem como acompanhamento constante de vulnerabilidade de cada um.

2.4. O plano de Reposta a Incidentes será revisado a cada 6 meses.

3. Preparação

3.1. Todos os desenvolvedores e equipe de suporte do **LojaHub LTDA** 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 esta dar segmento e analisar mais a fundo a falha.

3.2. 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 *API's* e sistemas integrados que disponibilizarem tais dados.

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

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

3.5. 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 sobre como agir caso se depare com algum problema relacionado.

3.6. Manutenções programadas que possam resultar em indisponibilidade do sistema também serão comunicadas com antecedências aos usuários.

4. Análise

4.1. 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.

4.2. 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.

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

4.3.1. Mínimo, no qual a falha tem muito baixo nível de impacto do sistema e não interfere o funcionamento das atividades do sistema, e se quer representa uma ameaça de segurança.

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

4.3.3. Médio, no qual a falha começa a contemplar a todos os usuários do sistema direta ou indiretamente, e ainda se restringe a poucos fluxos de atividades.

4.3.4. 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 LTDA** e pequenas brechas de segurança.

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

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

Parágrafo Único: em caso de incidentes críticos ou com suspeita de vazamento de dados, um comitê de crise será criado para acompanhamento e realização de ações pelo bem-estar da empresa e de seus usuários, bem como comunicação com meios e entidades responsáveis.

5. Contensão

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

5.1. Contenção curta, neste tipo de providência, realizamos em instantes a melhor solução prevista por nossa equipe de responsáveis técnicos para conter 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 providências fazem parte

também a reinicialização do sistema, interrupção abrupta de serviço, indisponibilidade de recursos, reinicialização de máquinas virtuais ou alocação de serviços em nova instância. Em resumo, adotando este tipo de providência, se busca sempre impedir que a ameaça se espalhe e que os danos sejam maiores.

5.2. 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*.

Parágrafo Único: em conformidade com a Lei Geral de Proteção de Dados, lei brasileira 13.709/2018, também chamada de LGPD, é que o **LojaHub LTDA** se reserva, em caso de vazamento de dados, à imediatamente comunicar o órgão competente, o informando sobre a ocorrência e sobre as medidas que estão sendo adotadas bem como ao conteúdo dos dados que foram ou possam ter sido vazados. Além disso o LojaHub LTDA se reserva a notificar os meios integrados dispostos no tópico "**Notificação a terceiros**" desde documento.

6. Erradicação

Ao chegar nessa etapa, após 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 inexistência de incidentes nessa versão é que será publicada em produção.

É importante também que instantes antes da aplicação e liberação da atualização em ambiente de produção, que sejam realizados todos os *backups* necessários, para facilitar assim em caso de emergência uma rápida restauração do sistema. 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, a fim de se acompanhar a recorrência de incidentes ou novas falhas.

7. Recuperação

7.1. Como rotina de recuperação a falhas e garantia de acessibilidade a informações durante incidentes, o **LojaHub LTDA** adota as seguintes estratégias para

tratar e guardar informações relevantes ao sistema e aos usuários.

7.1.1 Ao menos uma vez na semana ou sempre de modo a se precaver sobre grandes atualizações estruturais é que será realizado backup em nuvem dos bancos de dados e estado da aplicação.

7.1.2. O **LojaHub LTDA** possui ainda repositório de versionamento privado, que garante o armazenamento seguro e confiável de todas as instâncias do sistema. Garantindo assim uma gestão e armazenamento seguro do código fonte.

7.1.3. Arquivos de usuário como imagens, vídeos, arquivos zip, pdfs, estarão sempre armazenados e sendo assegurados por uma instância de armazenamento isolada na modalidade de CDN (*Content Delivery Network*). Cuja qual, possuí seus próprios métodos e rotinas de *backups* e higienização.

7.1.4. Das imagens do Sistema Operacional e execução de softwares e dependências de ambiente, os sistemas do **LojaHub LTDA** adotam técnicas de manutenção de *containers*, salvos em repositórios seguros de versionamento e estáveis. Dessa forma, utilizando o conceito de autoescalonamento, o sistema consegue sobreviver a falhas operacionais e se replicar conforme a demanda.

7.5. Dispostos as rotinas de segurança adotadas para manutenção e *backups* do sistema, os sistemas desenvolvidos pelo **LojaHub LTDA** ao segui-las fielmente se tornam 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 os códigos fontes dos repositórios ou os backups disponíveis e todo e qualquer dado salvo. Para garantir a segurança de dados salvos no sistema, seja pelo nosso CDN, seja pelos *backups* de banco de dados, testes são feitos com frequência para simulação de restaurações perante catástrofes.

7.6. O **LojaHub LTDA**, atualmente, utiliza infraestrutura *multicloud*, permitindo a substituição imediata de um provedor de hospedagem em caso de problemas críticos por qualquer outro disponível.

8. Balanço

8.1. 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 passos para serem aplicados na gestão de processo, de equipe e de *deploy*.

8.2. 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.

8.3. 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, refatoração de códigos, alteração nos membros da equipe, contratação de mão de obra ou consultoria com especialistas neste tipo de incidente, entre outras.

9. Notificação a terceiros

Versa neste tópico os sistemas de terceiros integrados diretamente ou indiretamente ao **LojaHub LTDA** e que deverão ser notificados em caso de incidente de segurança.

9.1 – Amazon Marketplace: deverá ser enviado um e-mail em idioma inglês para **3p-security@amazon.com** dentro de 24 horas após a contestação do incidente.

10. Glossário

10.1. **Deploy**: O ato de implementar ou lançar uma aplicação, sistema ou recurso em um ambiente operacional, geralmente após ter sido desenvolvido, testado e preparado para uso.

10.2. **Frameworks**: Conjuntos de ferramentas, bibliotecas e padrões que fornecem uma estrutura para o desenvolvimento de software. Eles simplificam e agilizam o processo de criação de aplicativos ao fornecer abstrações de alto nível para tarefas comuns.

10.3. **APIs (Interfaces de Programação de Aplicativos)**: Conjuntos de regras e definições que permitem que diferentes softwares se comuniquem entre si. Elas especificam como componentes de software devem interagir, permitindo a integração de sistemas e o compartilhamento de dados e funcionalidades.

10.4. **Logs**: Registros ou registros de eventos que ocorrem em um sistema ou aplicação. Eles podem incluir informações sobre erros, transações, atividades do usuário e outras métricas relevantes para monitoramento, diagnóstico e análise.

10.5. **Features (Recursos)**: Funcionalidades específicas de um produto de software que oferecem benefícios aos usuários. Eles podem incluir ferramentas, capacidades ou características distintivas que agregam valor ao produto.

10.6. **Containers**: Ambientes isolados que executam aplicativos e seus respectivos ambientes de tempo de execução de forma independente. Eles permitem a implantação consistente e escalável de aplicativos, facilitando a portabilidade e a distribuição.

10.7. **Multicloud**: A prática de distribuir cargas de trabalho e recursos de TI em mais de um provedor de serviços de nuvem. Isso proporciona redundância, flexibilidade e mitigação de riscos ao evitar a dependência exclusiva de um único provedor de nuvem.

10.8. **Backups (Cópias de Segurança)**: Cópias de dados armazenadas para proteger contra perdas de dados, corrupção ou falhas de sistema. Os backups são essenciais para a recuperação de dados em caso de falhas de hardware, erros humanos, ataques de malware ou desastres naturais.