# AVALIAÇÃO HOOBOX QUANTO À LGPD

## Introdução

Um dos grandes diferenciais das soluções da HOOBOX, além da qualidade internacional da tecnologia, é o preparo e amparo envolvido para proteção de dados e privacidade dos seus clientes, fornecedores e usuários. A HOOBOX nasceu como uma healthtech e como tal, e já teve suas soluções homologadas e aprovadas por times de TI, Segurança da Informação e Jurídicos de diversas instituições, especialmente as mais rígidas, como a do setor de saúde.

Com a nossa experiência nos processos de homologação, principalmente em instituições de saúde, onde privacidade e segurança do usuário é prioridade, construímos este documento que compila as principais perguntas e respostas sobre as soluções.

## Objetivo deste documento

Este documento tem por objetivo a apresentação prévia de requisitos de Segurança da Informação de solução HOOBOX, que geralmente são necessários no processo de Avaliação de fornecedores, homologação de segurança da informação ou acompanhamento jurídico no âmbito das instituições clientes da HOOBOX.

## Solução

Plataforma de visão computacional (PVC)

## ANEXOS

Respostas a seguir podem referenciar as políticas da empresa que se encontram no link abaixo:
https://github.com/hooboxrobotics/policies

- Contato DPO
- Comitê de Privacidade
- Plano de Continuidade de Negócio
- Política de Privacidade (Exemplo: Neonpass)
- Política de Descarte Seguro
- Política de Educação Continuada sobre LGPD
- Política de Governança
- Política de Prevenção de Vazamentos
- Política de Respostas a Incidentes
- Termo Geral de Uso (Exemplo: Neonpass)
- Termo de Notificação de Incidentes

**HOOBOX - Tabela Checklist LGPD - Evidências - HOOBOX**

| Nome da Empresa: HOOBOX Robotics | | | Políticas: https://github.com/hooboxrobotics/policies |
|---|---|---|---|
| **ID** | **Requisito** | **Resposta** | **Evidências** |
| 1 | Há DPO na empresa? | Sim | HOOBOX_CONTATO_DPO.pdf |
| 2 | Há um canal de contato com os titulares de dados pessoais? | Sim | HOOBOX_CONTATO_DPO.pdf & Empresa mantém contatos para titulares entrarem em contato via e-mail e telefone |
| 3 | Há Comitê de Privacidade? | Sim | HOOBOX_COMITE_PRIVACIDADE.pdf |
| 4 | Houve conscientização sobre LGPD? | Sim | Política_Educacao_LGPD_POL_EDU_LGPD.pdf |
| 5 | A empresa está adequada à LGPD? | Sim | Adequada |
| 6 | Há Política de Privacidade? (Neonpass exemplo) | Sim | Politica_Privacidade_Neonpass_POL_PRIV.docx.pdf |
| 7 | Há Política de Segurança da Informação? | Sim | Política_Prevencao_Vazamento_POL_VAZ_HBX_V2.pdf |
| 8 | Há Política de Retenção e Descarte de Dados Pessoais? | Sim | Política_Descarte_Seguro_POL_DESC_HBX_V2.pdf |
| 9 | Há compartilhamento de dados pessoais ou dados pessoais sensíveis? | Não | Não, exceto dados compartilhados com a permissão do usuário através do aceite da política de privacidade, termo de uso e termo de consentimento. |
| 11 | Há transferência internacional de dados pessoais e/ou dados pessoais sensíveis? | Não | |
| 12 | A empresa revisou seus contratos com base na LGPD? | Sim | Sim. Caso seja necessário apresentação de contrato como evidência, pede-se assinatura de NDA |
| 13 | A empresa utiliza NDAs? | Sim | -- |
| 14 | No ato da contratação de funcionários e parceiros de serviços, a empresa considera as regras da LGPD? | Sim | Política_Educacao_LGPD.pdf & Política_Governanca_POL_GOV_HBX_V2.pdf |
| 16 | Foram aplicados treinamentos? Há evidências? | Sim | Política_Educacao_LGPD_POL_EDU_LGPD.pdf |
| 17 | A empresa consegue rastrear todos os processos que envolvem dados pessoais? | Sim | -- |
| 18 | Há Plano de Governança? | Sim | Política_Governanca_POL_GOV_HBX_V2.pdf |
| 19 | Há Plano de Resposta a Incidentes? | Sim | Política_Resposta_Incidentes_POL_RES_INC_HBX_V2.pdf |
| 20 | Em caso de incidentes com dados pessoais, há termos de notificação para a ANPD e para os titulares de dados pessoais? | Sim | Termo_Notificacao_Incidente_TER_NOT.docx.pdf |

## Avaliação HOOBOX - Seção 01 – Projeto PVC

**1) Qual objetivo de uma solução HOOBOX de Plataforma de Visão Computacional (PVC)?**

Processos de atendimento, fabricação ou gestão de ativos, por exemplo, muitas vezes geram dados importantes, mas que, sem monitoramento automatizado e escalável são desconhecidos, fazendo com que a empresa precise operar em margens maiores para garantir o fluxo produtivo.

A fim de otimizar processos nas instituições a HOOBOX desenvolve versões de Plataforma de Visão Computacional (PVC), treinando algoritmos de I.A. para detectar, monitorar e ajudar no processo decisório. Uma PVC tem por natureza a qualidade de apresentar um dos maiores ROI da empresa, muitas vezes pagando o custo de desenvolvimento e licença nos primeiros meses de operação.

Uma PVC pode ser completa e contar com infraestrutura isolada em nuvem, Dashboard, sistema de login e cadastro, ou iniciar em FASE 1 apenas com o módulo de tecnologia para conta também com Dashboard com indicadores de todas as informações relevantes para mensurar a saúde do ambiente, ocupação, relatórios sobre os acessos, envio de convites para usuários VIP, cancelamento de convites etc.

**2) A solução irá coletar dados pessoais e sensíveis?**

Quando sim, seguindo a política de privacidade, termo de uso, ambos orientados pela LGPD.

**3) Como é feito esse armazenamento?**

O armazenamento é realizado em nuvem (AWS), seguindo as regras de segurança. Alguns dos itens de segurança são: backups diários armazenados por sete dias com criptografia de repouso com chave simétrica.

**4) O desenvolvimento é interno ou externo?**

O desenvolvimento é 100% da empresa.

**5) O produto apresenta Política de Privacidade, Termo Geral de Uso e Termo de Consentimento?**

Quando de acesso ao público, um exemplo é o produto Neonpass:
Podem ser acessados no link: https://github.com/hooboxrobotics/policies

## Avaliação HOOBOX- Seção 02 - Plano de continuidade de negócio

**6) A empresa possui um plano de continuidade de negócio?**

Sim.
Pode ser acessado para mais detalhes em "Plano de Continuidade de Negócio"
(https://github.com/hooboxrobotics/policies)

a. Em caso de desastres naturais, como funciona?
   De acordo com o PCN, desastre natural tem importância 4, de impacto direto e valor alto, sendo prontamente acionada a Defesa Civil. A preocupação é primeiramente com as pessoas, em seguida, com o salvamento de bens materiais. Em termos de salvamento de materiais, hoje existe condição

técnica e de infraestrutura em nuvem, onde um desastre natural impactando 100% de materiais, não impactaria na continuidade dos negócios, podendo ser a HOOBOX estabelecida prontamente em outra localização.

b. Em caso de pandemia, como funciona?
De acordo com o PCN, até que a situação se estabeleça, a empresa aplica três protocolos básicos e imediatos: avaliação para ampliação do regime home-office a fim de estabelecer a proteção dos colaboradores e garantir a continuidade das operações sem breakdowns; viabilizar padrões de segurança para o regime presencial com distanciamento, circulação de ar, limpeza e uso de equipamentos de proteção, orientar sobre a procura de ajuda médica em caso de sintomas e por fim, garantir acesso a ferramentas para suportar a contínua expansão da empresa.

c. Em caso de ataques cibernéticos, como funciona?
Na ocorrência de incidentes relevantes ou reconhecimento de novas vulnerabilidades ou modalidades de ataques, é realizada a análise de i)probabilidade, ii)impacto e iii) risco, tendo cada ataque, um procedimento associado. Em caso de acontecimento, tais procedimentos são prontamente executados. Tais procedimentos estão listados no documento acima.

d. Com qual frequência são realizados os testes do plano de continuidade de negócio.?
1 vez ao ano, ou após-ocorrência de evento como descrito no documento mencionado acima.

**7) Qual frequência do Backup?**

a. Qual período de retenção e ou Guarda?
    i. 7 dias de retenção para os bancos de dados

b. Onde são armazenados os Backups?
    i. Em São Paulo, através do serviço de AWS-RDS da amazon com criptografia de repouso com chaves simétricas.

c. Qual a frequência de testes de restore/recuperação?
    i. Protocolo em desenvolvimento. Pretendemos executar um procedimento mensal de restore de banco.

**8) O ambiente está em alta disponibilidade?**

a. O ambiente é Cloud? Se sim qual é a Cloud?

Sim, utilizamos o AWS Auto Scaling para monitorar os aplicativos e ajustar automaticamente a capacidade horizontal do parque de servidores para manter um desempenho constante e previsível. Usamos em conjunto com o Elastic Load Balancing para distribuir automaticamente o tráfego de entrada de aplicações entre as novas instâncias geradas pelo Auto Scaling.

b. Se forem servidores físicos, como funciona a alta disponibilidade?
Não utilizamos servidores físicos.

c. Banco de dados e aplicação, como funciona a alta disponibilidade?

Monitoramos constantemente o consumo de memória e processamento da aplicação para que sejam gatilhos automatizados de criação de novas instâncias para atender a demanda de requisições.

O front-end é disponibilizado em diferentes servidores de CDN através do serviço do AWS-Cloudfront.

O banco de dados é constantemente monitorado para dimensionarmos a capacidade vertical do servidor de escrita. Nossa estratégia para o aumento de requisições de leitura é aumentar a capacidade horizontal através de réplicas de servidores de leitura através do próprio serviço da AWS RDS.

## HOOBOX - Seção 03 – Proteção de Dados

**9) O Sistema utiliza alguma tecnologia de Criptografia?**

a. Usamos SSL para trafegar as informações pelas aplicações web
b. Utilizamos chaves simétricas de criptografia de repouso para os dados armazenados.

**10) O sistema utiliza alguma tecnologia para anonimizar/ou mascaramento dados?**

A HOOBOX utiliza técnicas de anonimização e mascaramento de dados como tokenização, ofuscamento, generalização, perturbação, mascaramento e a própria criptografia. Para imagens de biometria, por exemplo, não são armazenadas as mesmas, mas suas representações em hash. No entanto, para esse sistema em específico, os dados relacionados aos usuários são tão importantes quanto às suas propriedades, sendo as técnicas de anonimização e mascaramento de dados restritas à criptografia.

**11) A empresa possui um processo para gerenciamento dos riscos de privacidade e segurança da informação?**

Sim.
"Política de Prevenção de Vazamento de dados" (https://github.com/hooboxrobotics/policies)

**12) A empresa possui uma política de segurança da informação e privacidade de dados?**

Sim.
"Política de Prevenção de Vazamento de dados" (https://github.com/hooboxrobotics/policies)

**13) A empresa possui processos, procedimentos, políticas de controle de acesso?**

Sim.
Mais detalhes sobre os processos e protocolos da empresa, na Seção 4 (Proteção do Ambiente da Hoobox) da "Política de Prevenção de Vazamento de dados" (https://github.com/hooboxrobotics/policies)

Detalhando o sistema padrão de acesso da empresa: Todos os desenvolvedores e funcionários da contratada não possuem acesso aos dados de login e senha do usuário. Quanto ao acesso ao banco de dados, apenas o grupo de administradores têm acesso aos servidores de dados e produção, porém eles não têm acesso de alteração ou identificação dos dados de login dos usuários. Apesar dos mesmos possuírem acesso aos dados sensíveis dos usuários do cliente, o computador dos administradores possui software de controle de acesso às informações, que pode ser rastreado e identificado com dados de IP, login e logs de acesso.

**14) A empresa possui um SOC? (Security Operation Center)**

A empresa implementou uma hierarquia de funções com processos bem estruturados para centralizar e permitir que a empresa recupere ou bloqueie qualquer vazão de dados, DDoS ou outros incidentes o mais rapidamente possível para evitar danos ao negócio. O SOC da HOOBOX é composto por membros-chave do time da TI com experiência em

infraestrutura, com o suporte do Comitê de Privacidade que deve contar com pelo menos um tomador de decisão de nível executivo.

**15) A empresa treina seus colaboradores e fornecedores com relação às melhores práticas de Segurança da informação e privacidade de dados?**

Sim. A empresa possui uma Política de Educação, onde realiza o treinamento em três momentos distintos. Contratação, outra anualmente, e dependendo da equipe, a cada contratação de novo cliente.
Mais detalhes em "Diretrizes de Educação quanto à LGPD" (https://github.com/hooboxrobotics/policies)

**16) A empresa realiza avaliação de riscos para empresas parceiras e fornecedores?**

Sim. De acordo com a seção de Due Diligence da "Política de Governança" (https://github.com/hooboxrobotics/policies)

**17) Quais soluções de segurança da informação são utilizadas para proteger o ambiente?**

Para os servidores existe o processo de blindagem de acordo com as boas práticas de firewall, logs de acesso (IP) e acesso individualizado. Quanto às estações de trabalho, todos os desenvolvedores são administradores de suas próprias estações de trabalho, porém qualquer alteração de código fonte das aplicações da Hoobox é controlada por acessos individualizados, restritos e com aplicação de autenticação 2FA. Os desenvolvedores não possuem acesso ao banco de dados e/ou servidores. Para os computadores que acessam os servidores e banco de dados são utilizados acessos individuais através de softwares de controle de acesso às informações. Todo o trabalho da Hoobox de desenvolvimento é realizado dentro de rede devidamente protegida e controlada com todos os níveis de segurança para qualquer vazamento e/ou invasão externa, portanto trabalham de acordo com seus protocolos e leis de acesso. Além disso, todos os projetos em produção estão em container, o que dificulta o acesso.

Mais detalhes: Seção 4 "Proteção do Ambiente da Hoobox", Documento "Política de Prevenção de Vazamento de dados" (https://github.com/hooboxrobotics/policies)

**18) A empresa possui uma equipe de respostas a incidentes de privacidade e segurança da informação?**

Sim.
Equipe formada pela TI, com suporte do Comitê de Privacidade e Jurídico.
"Política de Resposta a Incidentes" (https://github.com/hooboxrobotics/policies)