# **Segurança em Sistemas de Informação**

## Requisitos Plataforma K+Home

### **Autenticação e autorização de usuário**

A K+Home deve oferecer métodos de autenticação que validem se o usuário é quem diz ser, promovendo segurança ao e-commerce evitando fraudes e golpes, e também assegurando ao usuário confiabilidade e responsabilidade no uso de seus dados pessoais, como CPF, endereço, dados bancários e assim por diante.

#### 

#### **Login:**

**Usuário e senha** - Esse é o método mais básico para a autenticação de um usuário, sendo necessário que o mesmo tome os devidos cuidados para proteger seus dados. Não obstante, a plataforma deverá armazenar os dados de login de forma a evitar qualquer tipo de incidente de segurança, como vazamentos ou roubo de senhas.

* **Padrão de senha:**

Para o cadastro na plataforma, o usuário deverá criar uma senha com os seguintes requisitos:

* Mínimo de 8 caracteres.
* Caracteres alfanuméricos, considerando maiúsculas, minúsculas e símbolos (&#$).
* Evitar sequências de caracteres, como 123456.
* Não utilizar nomes, datas importantes, ou qualquer informação que possa ser facilmente identificável.
* **Hashing de senha:**

Funções de criptográficas hash são algoritmos matemáticos que recebem uma entrada de qualquer tamanho e produzem um valor hash que são impossíveis de serem revertidos novamente para o valor original. Como a mesma entrada sempre resultará no mesmo valor de hash, este método pode ser utilizado para para validação de usuário sem necessariamente estar armazenando as senhas em si.

Função que pode ser utilizada: [bcrypt](https://en.wikipedia.org/wiki/Bcrypt)

**Autenticação em dois fatores (2FA)** - Na autenticação em dois fatores, para o acesso do usuário, além do username e senha, é realizada mais uma etapa para se concluir o acesso, utilizando de outro meio de comunicação com o usuário para realizar a autenticação em dois fatores. Os canais a serem utilizados podem ser por: email, sms ou aplicações específicas para 2FA, como Authy, Microsoft Authenticator e outros.

Nesse tipo de autenticação, são gerados códigos/tokens aleatórios, normalmente constituídos por números, que são enviados ao usuário pelo canal secundário definido pela própria pessoa, e o mesmo deve utilizá-lo na plataforma para a conclusão da segunda etapa. Uma características importante do 2FA, é a existência de um tempo máximo para que a segunda etapa seja concluída, se caso não houver essa conclusão dentro do tempo determinado o código é invalidado e o usuário terá que refazer todo o processo novamente.

Uma outra característica é que 2FA não é obrigatório, sendo de escolha da pessoa ter ou não essa opção de segurança.

**Autenticação por token -** Esse é mais um método de segurança que parte da validação já existente de um usuário e senha. Após a confirmação de usuário e senha, o cliente (browser) receberá como resposta do servidor um token, que permitirá ao usuário o acesso a aplicação.

O JWT, JSON Web Token, é o formato padrão mais utilizado no momento para a comunicação entre pares de forma segura. Os tokens, sendo assinados digitalmente, vão permitir a verificação pela parte interessada e a autorização ao usuário daquilo que for permitido dentro do seu escopo.

#### **Reset de senha:**

#### Para caso o usuário esqueça a senha ou precise trocar a senha atual, o fluxo básico será: - O usuário precisará inserir o email utilizado na plataforma. - Caso o email exista na base de dados, um token será criado e enviado ao usuário por email, e a partir dele a pessoa poderá realizar o reset de senha. - Caso o email não exista na base de dados, o usuário receberá o feedback e não poderá continuar com fluxo normal.

### **LGPD**

A plataforma K+Home se compromete em oferecer seus serviços em compliance com a Lei Geral de Proteção de Dados, zelando tanto pela qualidade do serviço, quanto pela segurança do usuário.

**Medidas a serem tomadas:**

* O usuário será solicitado a fornecer seu consentimento para acesso e uso de seus dados pessoais.
* Fornecer ao usuário explicações detalhadas sobre a necessidade, a finalidade e quais são os dados a serem utilizados na plataforma, deixando claro quais são dados essenciais para o oferecimento do serviço e quais são opcionais e ficam como escolha do usuário, em todo o caso, o usuario terá que consentir explicitamente.
* Os dados coletados estarão restritos àqueles necessários para o funcionamento e realização das finalidades.
* Os usuários também poderão solicitar informações sobre o uso dos dados, e até a exclusão dos mesmos.
* Reservar uma seção específica da plataforma para que os usuários tenham acesso facilitado às “Políticas de privacidade”, “Termos e condições de uso” e qualquer outro tipo de informações que são referentes à segurança da informação e afins.
* Oferecer um suporte preparado em caso de dúvidas de cliente referente ao tópico.
* Buscar consultoria jurídica para validação das medidas tomadas pela K+Home.

**Finalidades mapeadas e dados necessários:**

* Cadastro de usuário, para possibilitar o login na plataforma.
  + Nome
  + Email
  + Senha
  + Telefone para contato (opcional, caso o usuário queira validar a conta e adicionar mais uma forma de autenticação)
* Cadastro de informações de pagamento e envio, somente no caso em que o usuário realize uma compra.
  + CPF
  + Cartão de crédito (caso seja a forma de pagamento escolhida)
  + Endereço residencial
  + Telefone para contato
* Cookies essenciais para o funcionamento do site.
* Newsletter ou email marketing
  + email

### **Sistema de pagamentos e antifraude**

Para o sistema de pagamentos do e-commerce sugere-se a plataforma [Pagar me](https://pagar.me/pronto-para-usar).

Funcionalidades oferecidas, para a gestão de negócio:

* **Dashboard;**
* **Formas de pagamento variadas:** Crédito, Débito, Boleto, Pix;
* **Página de checkout do Pagar.me;**
* **Multimeios de pagamentos:** os clientes podem realizar pagamentos combinando meio diferentes de pagamento;
* **Multicompradores:** Permite dividir o pagamento por mais de uma pessoa;
* **VerifyCard;**
* **Webhooks;**

Segurança e antifraude:

* **Chargeback;**
* **Konduto** (Antifraude): análise de transações e mapeamento do comportamento de compra dos consumidores;
* **ClearSale** (Antifraude): gestão e análise de fraude para o segmento de ecommerce;
* **Alerta de Transações Suspeitas:** monitoramento interno do Pagar.me que detecta um comportamento suspeito nas transações do site;
* **Alerta da Bandeira:** Notificação da bandeira do cartão, sobre uma ou mais transações da loja;

### **Certificados**

**PCI DSS – Payment Card Industry Data Security Standard**

Certificado internacional de segurança atribuído às empresas que estão em conformidade com suas regras para manuseio de dados sensíveis de cartão de crédito, tais como: número, validade, nome do portador e CVV do mesmo.

**Certificado SSL**

O **SSL** (Secure Socket Layer) permite a comunicação segura entre o servidor e o navegador, garantindo que todas as informações estejam seguras e sigilosas. Vantagens:

* Melhor posicionamento nos buscadores (SEO);
* Criptografia avançada;
* Cadeado verde no site;
* Mais confiança para os consumidores;

**SiteLock**

SiteLock protege o e-commerce ao automaticamente encontrar e resolver ameaças. Vantagens:

* Proteção;
* Confiança e Credibilidade:;
* PageRank;
* Preço;

### **Norton Seal**

O Norton Secured possui tecnologia Symantec. Uma das vantagens deste selo é o reconhecimento internacional. 

### **Outros requisitos gerais**

### Backups diários e espelhamento de servidores

Recomenda-se utilizar um sistema de backup em nuvem, garantindo que não se perca os dados armazenados. Além disso, o backup dos dados, idealmente, deve ser feito de modo automático e frequente. Esse cuidado será importante para reduzir as possibilidades de perda de dados entre as cópias de segurança.

**Espelhamento de servidores** é, basicamente, a criação automática de réplicas entre servidores paralelos, permitindo que, caso um deles apresente algum problema, o outro seja acionado imediatamente, diminuindo os impactos

### reCaptchas

O CAPTCHA é um serviço provido pelo Google, e ele protege contra spam e descriptografia de senhas com um teste simples que prova que você é um ser humano, não um computador tentando invadir uma conta protegida por senha.

Pode ser usado no e-commerce em logins, finalização de compras e etc.