

---

# Book Keeper

---

Raquel Paradinha 102491  
Miguel Matos 103341

---



---

# Conteúdos

**01**

**Visão do  
Sistema**

**02**

**Atores**

**03**

**Dados**

**04**

**Segurança e  
Privacidade**



---

**01**

# **Visão do Sistema**

---

---

# Serviços e Funcionalidades



## Livros

Requisitar e reservar livros

## Webpage

Dados e informação acessíveis



## Recomendações

Recomendações de livros baseadas em atividade anterior

## Tendências

Estatísticas gerais, estudo de modas e preferências



## Newsletter

Newsletter de novos livros e notícias da biblioteca

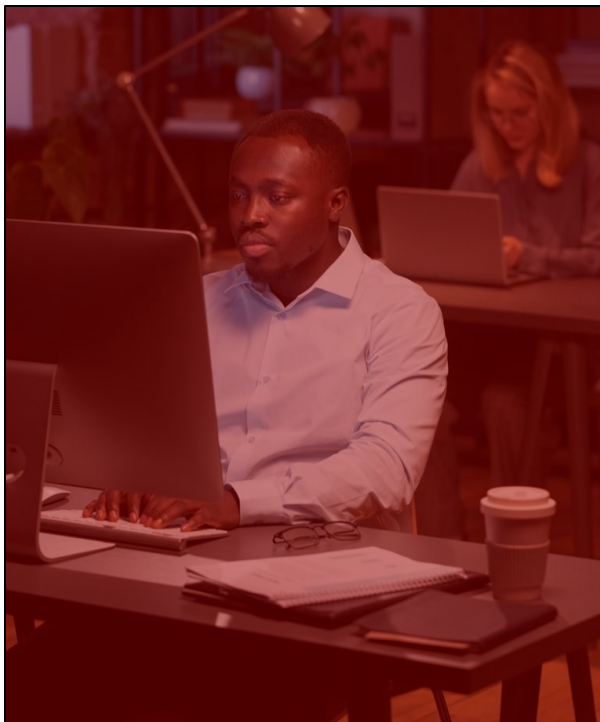
## Gestão interna

Gestão dos funcionários da biblioteca



A nossa biblioteca/sistema para bibliotecas oferece estes principais serviços e funcionalidades:

- Obviamente, requisitar e reservar livros, levá-los para casa emprestados
- Webpage que permite aos leitores acederem tanto aos dados públicos dos livros que estão na biblioteca, como acesso aos seus dados pessoais do sistema, para transparência
- Recomendações de livros para os leitores (opcionais, claro), baseadas na sua atividade anterior, com recurso a algoritmos estricados que adivinham tudo
- Análise estatística da biblioteca/leitores como um todo, e extrapolação de tendências e preferências para fins de investimento



---

**02**

# **Atores**

---

---

# Atores

## Leitor

Utilizadores da biblioteca que requisitam e lêem livros



## Bibliotecário

Profissionais que gerem a coleção da biblioteca e a circulação dos itens

## Desenvolvedor

Responsável pelo desenvolvimento e manutenção do sistema



## Administrador

Responsáveis por supervisionar o uso do sistema e garantir que funciona corretamente

### LEITORES

Leitores são os utilizadores da biblioteca, e podem navegar pelo catálogo da biblioteca, reservar livros, e ver o seu histórico de empréstimos e multas.

### BIBLIOTECÁRIOS

Têm um acesso mais extenso ao sistema. São responsáveis por registar empréstimos e devoluções de livros, gerir reservas e ver e editar informações dos leitores.

### DESENVOLVEDORES

Têm acesso ao sistema para o propósito de o desenvolver e atualizar.

### ADMINISTRADORES

Têm o acesso mais extenso ao sistema. Capazes de gerir contas de utilizadores e configurar definições do sistema.



---

**03**

# Dados

---

---

# Dados do Sistema

## Leitores

- Identificação de detentores de livros
- Reservas de livros
- Uso geral da biblioteca

## Financeiros

- Pagar multas
- Serviços de subscrição

## Funcionários

- Gestão do pessoal e do sistema

## Empréstimos

- Recomendações de livros
- Prever comportamentos
- Investir em novos livros/serviços de interesse
- Análise estatística

### DADOS DOS LEITORES

Nome, idade, contactos, morada, etc...

Utilizados para utilização geral da biblioteca por parte dos leitores.

### DADOS FINANCEIROS

Dados de pagamentos e cartões

Utilizados para processamento de pagamentos referentes a multas, ou serviços de subscrições, como newsletters.

### DADOS DOS FUNCIONÁRIOS

Nome, idade, contactos, morada, salário, horário, etc...

Utilizados para gestão de pessoal e sistema.

### DADOS DE EMPRÉSTIMOS

Registos de empréstimos e reservas

Utilizados para fins estatísticos, como análises de tendências e preferências e geração de recomendações de livros dada a atividade de um leitor.

### ARMAZENAMENTO

Todos os dados são guardados na cloud pelos benefícios que oferece, nomeadamente:

- Escalabilidade: caso o sistema venha a integrar mais do que uma biblioteca, o que nos leva à...
- Acessibilidade: que permite um acesso mais rápido e fácil aos dados a partir



- de diferentes localizações
- Segurança: os sistemas de cloud estão equipados com medidas de segurança e são mais robustos face a fatores como erro humano ou fenómenos climatéricos



---

**04**

# **Segurança e Privacidade**

---

---

# Segurança e Privacidade



## Segurança

Proteger dados e informação de acessos não autorizados, modificações ou destruição.

Encriptação, firewalls, controlos de acesso



## Privacidade

Proteger dados pessoais e controlar como são adquiridos, usados e partilhados.

Consentimento informado, minimização de dados, políticas de proteção de dados



## SEGURANÇA

Segurança é referente a todas as medidas implementadas para proteger dados pessoais de acessos não autorizados, roubo e mau uso. Inclui medidas como encriptação, firewalls, controlos de acesso e backups dos dados.

## PRIVACIDADE

Privacidade refere-se ao direito de um indivíduo de controlar o uso e divulgação dos seus próprios dados. Inclui o direito de escolher qual informação partilhar, com quem, e como esta deve ser usada.

## REGULAÇÕES

Existem regulações para salvaguardar estes aspectos. Uma delas é o Regulamento Geral de Proteção de Dados, ou RGPD, que é um regulamento da União Europeia que governa a proteção de dados pessoais.

Em Portugal existe a Lei de Proteção de Dados Pessoais, que é uma lei nacional que regula para além do RGPD, adicionando leis e regras extra.

Alguns dos artigos mais relevantes de cada regulamento são:

### RGPD

#### 1. Artigo 5

Descreve os princípios do tratamento de dados. Requer que os dados pessoais sejam tratados de forma legal, justa e transparente.

#### 1. Artigo 6

Descreve as bases legais do tratamento de dados, incluindo a necessidade de

consentimento por parte do titular.

1. Artigo 16

Define o direito de retificação dos dados.

1. Artigo 17

Define o direito à eliminação dos dados.

1. Artigo 21

Define o direito à objeção ao processamento dos dados.

1. Artigo 24

Estabelece a obrigação para os responsáveis pelo tratamento de dados de implementarem medidas técnicas e organizacionais apropriadas para garantir a segurança dos dados.

1. Artigo 25

Define o princípio da proteção de dados desde a conceção e por defeito.

1. Artigo 33

Estabelece a obrigação dos responsáveis pelo tratamento de dados de informarem as autoridades reguladoras competentes em caso de violações de dados.

1. Artigo 35

Estabelece a exigência da realização de avaliações de impacto sobre a proteção de dados.

1. Artigo 37

Estabelece a necessidade de nomear um Encarregado de Proteção de Dados (EPD).

## **LPDP**

1. Capítulo 3

Define o que é um EPD, os seus deveres e as suas funções

1. Capítulo 6

Define algumas situações específicas para o tratamento de dados que caem fora do RGPD.

a. Artigo 31

Define como os dados podem ser utilizados para fins estatísticos.

---

## Medidas Gerais

### Consentimento

Obter o consentimento explícito, claro e informado do titular dos dados antes de qualquer processamento.



### Rigor

Dados corretos, atualizados e relevantes para o propósito de recolha.

### Acesso

Os titulares dos dados têm direito ao acesso, retificação e objeção do processamento dos mesmos.



### EPD/DPO

Indicação de um Encarregado de Proteção de Dados.

## CONSENTIMENTO

É necessário para garantir que os leitores percebem como é que os seus dados pessoais serão utilizados e para que fins, e dá-lhes controlo sobre se querem dar consentimento ou não.

No nosso contexto, é pedido, por exemplo, ao criar uma nova conta/cartão, ou no antes da análise dos registos de empréstimos do utilizador para recomendações de livros relevantes.

## RIGOR

Assegurar que os dados armazenados se mantêm corretos, atualizados, e relevantes para o propósito de recolha. Por exemplo, se dados foram recolhidos para criar um cartão da biblioteca que o utilizador pretende cancelar, não vale a pena mantê-los armazenados.

## ACESSO

Garantir que os titulares dos dados têm acesso aos mesmos, possibilidade de os retificar e de se opôr ao seu processamento - fomentando transparência entre a biblioteca e os leitores.

Por exemplo, através do portal online do sistema, é possível ao utilizador aceder aos seus dados pessoais, retificá-los, e até mesmo revogar o consentimento dado anteriormente.

## ENCARREGADO DE PROTEÇÃO DE DADOS

Por conformidade ao RGPD e LPDP, é necessário indicar um encarregado de

proteção de dados, que pode monitorar e aconselhar sobre questões de conformidade com regulamentações, e servir como ponto de contacto para titulares de dados e autoridades regulatórias.

# Medidas Técnicas



## Encriptação

Dados são encriptados antes de armazenados.

## Controlo de acesso

Acesso aos dados deve ser mantido no mínimo necessário



## Minimização

Anonimização e pseudonimização dos dados adequados

## Firewalls

Prevenção de acessos não autorizados a redes e computadores



## Backups

Backups regulares e distintos

## Manutenção

Updates de software e manutenção do hardware



## ENCRIPTAÇÃO

Encriptação é uma medida técnica que ajuda a proteger dados pessoais de acessos não autorizados, roubo, ou mau uso. Consiste em converter a informação para um formato não legível, protegendo contra maus acessos e salvaguardando a privacidade.

Antes de armazenados, todos os dados pessoais são encriptados, de forma a fomentar a sua segurança.

## CONTROLO DE ACESSO

Consiste em limitar quem tem acesso a que dados. Ao reduzir o acesso a dados ao estritamente necessário, podemos evitar acessos não autorizados e fugas de dados. No nosso caso, temos diferentes tipos de utilizadores, cada um com permissões de acesso diferentes:

- Os leitores têm acesso apenas aos seus dados pessoais
- Os bibliotecários têm acesso apenas aos dados necessários para realizar o seu trabalho
- Os desenvolvedores não têm acesso a qualquer tipo de dados pessoais, exceto para casos de teste e debugging, quando estritamente necessário
- Os administradores teriam o acesso mais extensivo ao sistema

Além disso, são mantidos também registos de auditoria, que deixam registado quem acedeu a que dados, e quando.

## ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

A anonimização é o processo de irreversivelmente transformar dados pessoais de

forma a que não possam mais ser atribuídos a um indivíduo específico - deixando, portanto, de ser considerados dados pessoais, e saindo do escopo de regulamentos de proteção de dados pessoais.

Por outro lado, a pseudonimização dos dados torna mais difícil atribuí-los a um indivíduo, mas não quebra completamente a ligação entre dados e indivíduo.

Consiste em substituir informação identificadora por pseudónimos ou identificadores artificiais. Não torna os dados anónimos - continuam a ser dados pessoais.

## **FIREWALLS**

Usadas para prevenir acessos não autorizados a um computador ou rede. Ao bloquear tráfego não desejado, podemos proteger melhor a privacidade dos titulares dos dados subjacentes ao sistema.

## **BACKUPS**

Backups servem para garantir a recuperação dos dados em caso de desastre; ao criar cópias redundantes dos dados, podemos garantir a disponibilidade dos dados em caso de perda.

## **MANUTENÇÃO**

Updates de software e manutenção do hardware são essenciais para o bom funcionamento do sistema, logo, são também essenciais para a segurança e proteção da privacidade dos dados pessoais.

Partes mal-intencionadas procuram por falhas exploráveis constantemente. Ao garantir que o software está atualizado, estamos a proteger o sistema com as funcionalidades mais recentes e seguras.

Quanto ao hardware, é necessária uma manutenção regular. Equipamento físico está sujeito ao tempo e desgaste, que, quando ignorado, pode criar situações de falhas de sistema.



---

# Medidas Organizacionais



## Políticas e Procedimentos

Diretrizes que ditam como é que os dados devem ser tratados.



## Análises de Risco

Identificação de potenciais vulnerabilidades preventivamente.



## Treino dos Utilizadores

Treino e sensibilização de leitores e funcionários sobre as medidas de segurança e privacidade.

### POLÍTICAS E PROCEDIMENTOS

Devem ser postas em prática medidas organizacionais que descrevem como é que os dados pessoais devem ser adquiridos, processados, e armazenados. Com diretrizes claras, é mais fácil pôr em prática os mecanismos que permitem garantir a segurança dos dados e privacidade dos titulares.

### ANÁLISES DE RISCO

Análises de risco são essenciais para identificar vulnerabilidades potenciais antes que estas se tornem um problema. Ao procurar por falhas proativamente, podemos mitigar o seu impacto, ou até mesmo resolver a vulnerabilidade por completo, antes de qualquer desastre.

### TREINO DOS UTILIZADORES

O treino dos utilizadores é sempre essencial ao bom funcionamento de um sistema de dados que lide com dados pessoais.

É necessário que quem tenha acesso e processe os dados subjacentes ao sistema esteja sensibilizado para a importância da privacidade individual e dos riscos associados ao processamento de dados pessoais.

Este cobre aspectos como (mas não só) gestão de passwords, o reconhecimento de ameaças e resposta a incidentes.

# Acesso por entidades judiciais



## Verificação

É importante confirmar a legitimidade do pedido legal



## Comunicação

Os pedidos legais têm de ser feitos pelos meios apropriados



## Minimização

Fornecer apenas a informação pedida

## Prazos

Os pedidos legais geralmente têm um prazo de resposta associado



## Documentação

Guardar registos de todos pedidos de acesso a dados



## Notificação

Os utilizadores afetados pelo pedido serão notificados do acesso aos seus dados



## VERIFICAÇÃO

Antes de conceder acesso a qualquer dado do utilizador, é importante verificar a legitimidade do pedido legal. O pedido deve ser feito por escrito e incluir informações suficientes para identificar a pessoa ou entidade que faz o pedido, os dados específicos solicitados e a base legal para o pedido. Se o pedido não estiver claro ou for insuficiente, deve pedir-se esclarecimentos ao solicitante.

## COMUNICAÇÃO

Pedidos legais de dados do utilizador devem ser feitos pelos canais adequados, no caso de Portugal deve ser feito um requerimento ao órgão judicial competente.

## MINIMIZAÇÃO

Ao responder a pedidos legais de dados do utilizador, apenas fornecemos as informações solicitadas especificamente e nada mais. Isso ajuda a proteger a privacidade dos utilizadores e a evitar a divulgação não autorizada de informações sensíveis.

## PRAZOS

Pedidos legais de dados pessoais por norma têm um prazo para dar uma resposta. É importante responder dentro do prazo exigido, mas rever sempre cuidadosamente toda a informação e garantir que todas as leis e regulamentos aplicáveis são cumpridos.

## DOCUMENTAÇÃO

Mantemos registos detalhados de todos os pedidos legais de dados dos utilizadores, incluindo o pedido em si, qualquer correspondência com a entidade que solicita a informação e a resposta fornecida.

### **NOTIFICAÇÃO**

Notificamos sempre os nossos utilizadores quando recebemos um pedido para aceder aos seus dados.



---

# Obrigada!

Credits: This presentation template was created by **Slidesgo**, including icons by **Flaticon** and infographics & images by **Freepik**

---



---

“Proteger dados pessoais  
numa biblioteca é como  
devolver os teus livros a  
tempo. É senso comum,  
maltinha.”

---

— RILLON

---