

Tutorial

Sistema Agenda de Contatos Pessoal

Este projeto modelo, denominado **Agenda de Contatos Pessoal**, foi desenhado especificamente para você aprender o passo a passo de como desenvolver um sistema web simples, utilizando PHP estruturado (procedural), MySQL e Bootstrap.

Ele aborda desde a segurança do login até o CRUD completo (Create, Read, Update, Delete) de contatos e usuários. Siga etapas para criar o sistema.

Parte I: Configuração do Ambiente e Estrutura

1. Preparação (VS Code e XAMPP)

- Instale e Inicie o XAMPP:**
 - Certifique-se de que o XAMPP está instalado em sua máquina.
 - Abra o **XAMPP Control Panel** e inicie os módulos **Apache** (servidor web) e **MySQL** (servidor de banco de dados).
- Crie a Pasta do Projeto:**
 - Navegue até o diretório de instalação do XAMPP (geralmente `C:\xampp`).
 - Dentro da pasta `htdocs`, crie uma nova pasta chamada `agenda_pessoal`.
- Abra no VS Code:**
 - Abra o Visual Studio Code.
 - Vá em **File > Open Folder** e selecione a pasta `C:\xampp\htdocs\agenda_pessoal`.

2. Estrutura de Pastas

Dentro da pasta `agenda_pessoal`, crie a seguinte estrutura (fundamental para organizar o código procedural):

None

`agenda_pessoal/`

```
├── assets/
│   ├── css/      (Estilos personalizados)
│   └── js/        (Scripts JavaScript/jQuery)
├── config/
│   └── database.php (Conexão e Sessão PHP)
├── includes/
│   ├── header.php  (Cabeçalho, nav e Bootstrap)
│   └── footer.php   (Rodapé e scripts JS)
├── db/
│   └── estrutura.sql (Script de criação do BD)
├── index.php        (Login ou Lista de Contatos)
├── contatos_cadastrar.php (Formulário C)
├── contatos_editar.php   (Formulário U)
├── usuarios.php          (Listagem/Exclusão de Usuários)
├── usuarios_cadastrar.php (Formulário C para Usuário)
└── processa.php          (Lógica CRUD e Login/Logout)
```

Parte II: Banco de Dados (MySQL)

3. Criando as Tabelas

1. Acesse seu navegador e digite `http://localhost/phpmyadmin`.
2. Crie um novo banco de dados chamado `agenda_db`.
3. Execute o script SQL abaixo para criar as tabelas `usuarios` e `contatos`.

SQL

```
-- Criação do banco de dados (se necessário, execute no phpMyAdmin)
CREATE DATABASE IF NOT EXISTS agenda_db;

USE agenda_db;

-- Tabela de Utilizadores (Para Login/Área Restrita)
CREATE TABLE usuarios (
    id INT AUTO_INCREMENT PRIMARY KEY,
    usuario VARCHAR(50) NOT NULL UNIQUE,
    email VARCHAR(100),
    senha VARCHAR(255) NOT NULL, -- Armazena a senha criptografada (hash)
    nivel ENUM('Admin', 'Comum') NOT NULL DEFAULT 'Comum'
);

-- Tabela de Contatos (CRUD Principal da Aplicação)
```

```

CREATE TABLE contatos (
    id INT AUTO_INCREMENT PRIMARY KEY,
    nome VARCHAR(100) NOT NULL,
    telefone VARCHAR(20),
    email VARCHAR(100),
    data_nascimento DATE,
    endereco TEXT,
    data_cadastro TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

-- Inserir um utilizador Administrador padrão: 'admin' com senha '123456'
-- O hash é gerado com password_hash('123456', PASSWORD_DEFAULT)
INSERT INTO usuarios (usuario, email, senha, nivel) VALUES
('admin', 'admin@agenda.com.br',
'$2y$10$YiBpez0RPaoPnQM6oH8hT0J/jeh0g7k4NFGMpABJj5Hto0lcHC9G.', 'Admin');

```

Parte III: Código PHP Base e Segurança

4. Configuração da Conexão e Sessão (config/database.php)

Este arquivo define a conexão MySQL e as funções de segurança.

```

PHP
<?php
// Define as configurações de conexão
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "agenda_db";

// Tenta estabelecer a conexão com o MySQL
$conn = mysqli_connect($servername, $username, $password, $dbname);

// Verifica a conexão
if (!$conn) {
    // Exibe erro fatal em caso de falha de conexão com o banco
    die("Falha na conexão com o banco de dados: " . mysqli_connect_error());
}

// Inicia a sessão PHP (essencial para login e persistência de dados do
utilizador)
session_start();

/**
 * Função de segurança: Verifica se o utilizador está logado.

```

```

    * Se não estiver, redireciona para a página de login (index.php) com erro.
    */
function verificar_login() {
    if (!isset($_SESSION['usuario_logado'])) {
        // Redireciona corretamente para a raiz do projeto (index.php)
        $caminho_base = (basename(getcwd()) == 'agenda_pessoal') ? '' :
        '../';
        header("Location: " . $caminho_base . "index.php?erro=Acesso negado!
        Faça login para continuar.");
        exit();
    }
}

/**
 * Função de segurança: Verifica se o utilizador logado é Administrador.
 */
function verificar_admin() {
    verificar_login(); // Garante que está logado primeiro
    if (!isset($_SESSION['usuario_nivel']) || $_SESSION['usuario_nivel'] !=
    'Admin') {
        // Redireciona com erro de permissão
        $caminho_base = (basename(getcwd()) == 'agenda_pessoal') ? '' :
        '../';
        header("Location: " . $caminho_base . "index.php?erro=Acesso
        restrito a Administradores.");
        exit();
    }
}
}
?>

```

5. Componentes Visuais Reutilizáveis (includes/)

O `header.php` carrega o Bootstrap e o `footer.php` carrega os scripts.

header.php

```

PHP
<?php
// Define o caminho base para que os links funcionem corretamente,
independente da pasta
$caminho = (basename(getcwd()) == 'agenda_pessoal') ? '' : '../';
?>
<!DOCTYPE html>
<html lang="pt-br">
<head>
    <meta charset="UTF-8">

```

```

<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Agenda de Contatos Pessoal | PHP Procedural</title>
<!-- Incluindo Bootstrap CSS via CDN para estilização e responsividade
-->
<link
href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.cs
s" rel="stylesheet">
<style>
    body { background-color: #f0f2f5; }
    .card-login { max-width: 450px; margin-top: 50px; }
</style>
</head>
<body>
    <nav class="navbar navbar-expand-lg navbar-dark bg-primary shadow-sm">
        <div class="container">
            <a class="navbar-brand" href="<?php echo $caminho;
?>index.php">🐼 Agenda Pessoal</a>
            <button class="navbar-toggler" type="button"
data-bs-toggle="collapse" data-bs-target="#navbarNav"
aria-controls="navbarNav" aria-expanded="false" aria-label="Toggle
navigation">
                <span class="navbar-toggler-icon"></span>
            </button>
            <div class="collapse navbar-collapse" id="navbarNav">
                <ul class="navbar-nav me-auto">
                    <!-- Links visíveis apenas se o utilizador estiver
logado -->
                    <?php if (isset($_SESSION['usuario_logado'])): ?>
                        <li class="nav-item">
                            <a class="nav-link" href="<?php echo $caminho;
?>contatos_cadastrar.php">Cadastrar Contato</a>
                        </li>
                        <!-- Link visível apenas para Administradores -->
                        <?php if (isset($_SESSION['usuario_nivel']) &&
$_SESSION['usuario_nivel'] == 'Admin'): ?>
                            <li class="nav-item">
                                <a class="nav-link text-warning" href="<?php
echo $caminho; ?>usuarios.php">Gerenciar Utilizadores</a>
                            </li>
                        <?php endif; ?>
                    <?php endif; ?>
                </ul>
                <ul class="navbar-nav">
                    <!-- Informações e botão de Sair -->
                    <?php if (isset($_SESSION['usuario_logado'])): ?>
                        <li class="nav-item me-3">
                            <span class="nav-link text-light">

```

```

                Olá, **<?php echo
htmlspecialchars($_SESSION['usuario_logado']); ?>**
            </span>
        </li>
        <li class="nav-item">
            <a href="<?php echo $caminho;
?>processa.php?acao=logout" class="btn btn-sm btn-danger">Sair</a>
        </li>
    <?php endif; ?>
</ul>
</div>
</div>
</nav>
<div class="container mt-4">

```

footer.php

```

PHP
</div><!-- Fim do container do Bootstrap -->

<footer class="text-center text-white bg-dark py-3 mt-5">
    <div class="container">
        <p class="mb-0">Projeto Agenda de Contatos Pessoal &copy; <?php
echo date("Y"); ?></p>
    </div>
</footer>

<!-- Incluindo jQuery e Bootstrap JS (Bundle com Popper) -->
<script
src="[https://code.jquery.com/jquery-3.7.1.min.js](https://code.jquery.com/j
query-3.7.1.min.js)"></script>
<script
src="[https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.
min.js](https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundl
e.min.js)"></script>
</body>
</html>

```

Parte IV: Lógica Central e Funcionalidades (CRUD)

6. Motor do Sistema (processa.php)

Este arquivo é o único que interage diretamente com o banco de dados para criar, editar, excluir e autenticar.

```

PHP
<?php
// Inclui a configuração do BD e as funções de segurança
require_once 'config/database.php';

// Recebe a ação a ser executada (geralmente via GET na URL)
$acao = isset($_REQUEST['acao']) ? $_REQUEST['acao'] : '';

switch ($acao) {
    // =====
    // AÇÕES DE AUTENTICAÇÃO (LOGIN / LOGOUT)
    // =====
    case 'login':
        // Filtra e limpa as entradas para segurança
        $usuario = filter_input(INPUT_POST, 'usuario',
FILTER_SANITIZE_STRING);
        $senha = filter_input(INPUT_POST, 'senha', FILTER_SANITIZE_STRING);

        // Prepara a consulta para buscar o utilizador
        $stmt = mysqli_prepare($conn, "SELECT id, usuario, senha, nivel FROM
usuarios WHERE usuario = ?");
        mysqli_stmt_bind_param($stmt, "s", $usuario);
        mysqli_stmt_execute($stmt);
        $resultado = mysqli_stmt_get_result($stmt);

        if (mysqli_num_rows($resultado) == 1) {
            $linha = mysqli_fetch_assoc($resultado);

            // Verifica a senha fornecida contra o hash salvo (ESSENCIAL!)
            if (password_verify($senha, $linha['senha'])) {
                // Login bem-sucedido: Armazena dados essenciais na sessão
                $_SESSION['usuario_logado'] = $linha['usuario'];
                $_SESSION['usuario_nivel'] = $linha['nivel'];
                $_SESSION['usuario_id'] = $linha['id'];

                header("Location: index.php?msg=Bem-vindo(a), " .
$linha['usuario'] . "! Login realizado com sucesso.");
                exit();
            }
        }

        // Falha no login
        header("Location: index.php?erro=Credenciais inválidas. Verifique
utilizador e senha.");
        mysqli_stmt_close($stmt);
        break;

    case 'logout':
        session_unset(); // Limpa todas as variáveis de sessão

```

```

        session_destroy(); // Destrói a sessão
        header("Location: index.php?msg=Você foi desconectado(a) do
sistema.");
        break;

// =====
// CRUD DE CONTATOS
// =====
case 'cadastrar_contato':
    verificar_login();

    $nome = filter_input(INPUT_POST, 'nome', FILTER_SANITIZE_STRING);
    $telefone = filter_input(INPUT_POST, 'telefone',
FILTER_SANITIZE_STRING);
    $email = filter_input(INPUT_POST, 'email', FILTER_SANITIZE_EMAIL);
    $data_nascimento = filter_input(INPUT_POST, 'data_nascimento',
FILTER_SANITIZE_STRING);
    $endereco = filter_input(INPUT_POST, 'endereco',
FILTER_SANITIZE_STRING);

    // Prepared Statement para INSERT (Proteção contra SQL Injection)
    $stmt = mysqli_prepare($conn, "INSERT INTO contatos (nome, telefone,
email, data_nascimento, endereco) VALUES (?, ?, ?, ?, ?)");
    mysqli_stmt_bind_param($stmt, "sssss", $nome, $telefone, $email,
$data_nascimento, $endereco);

    if (mysqli_stmt_execute($stmt)) {
        header("Location: index.php?msg=Contato '$nome' cadastrado com
sucesso!");
    } else {
        header("Location: contatos_cadastrar.php?erro=Erro ao cadastrar:
" . mysqli_error($conn));
    }
    mysqli_stmt_close($stmt);
    break;

case 'editar_contato':
    verificar_login();

    $id = filter_input(INPUT_POST, 'id', FILTER_VALIDATE_INT);
    $nome = filter_input(INPUT_POST, 'nome', FILTER_SANITIZE_STRING);
    $telefone = filter_input(INPUT_POST, 'telefone',
FILTER_SANITIZE_STRING);
    $email = filter_input(INPUT_POST, 'email', FILTER_SANITIZE_EMAIL);
    $data_nascimento = filter_input(INPUT_POST, 'data_nascimento',
FILTER_SANITIZE_STRING);
    $endereco = filter_input(INPUT_POST, 'endereco',
FILTER_SANITIZE_STRING);

```



```

        if (!$id) {
            header("Location: index.php?erro=ID de contato inválido.");
            exit();
        }

        // Prepared Statement para UPDATE
        $stmt = mysqli_prepare($conn, "UPDATE contatos SET nome = ?,
telefone = ?, email = ?, data_nascimento = ?, endereco = ? WHERE id = ?");
        mysqli_stmt_bind_param($stmt, "sssssi", $nome, $telefone, $email,
$data_nascimento, $endereco, $id);

        if (mysqli_stmt_execute($stmt)) {
            header("Location: index.php?msg=Contato ID:$id atualizado com
sucesso!");
        } else {
            header("Location: contatos_editar.php?id=$id&erro=Erro ao
atualizar: " . mysqli_error($conn));
        }
        mysqli_stmt_close($stmt);
        break;

    case 'excluir_contato':
        verificar_login();

        $id = filter_input(INPUT_GET, 'id', FILTER_VALIDATE_INT);
        if (!$id) {
            header("Location: index.php?erro=ID de contato inválido.");
            exit();
        }

        // Prepared Statement para DELETE
        $stmt = mysqli_prepare($conn, "DELETE FROM contatos WHERE id = ?");
        mysqli_stmt_bind_param($stmt, "i", $id);

        if (mysqli_stmt_execute($stmt)) {
            header("Location: index.php?msg=Contato excluído com sucesso!");
        } else {
            header("Location: index.php?erro=Erro ao excluir: " .
mysqli_error($conn));
        }
        mysqli_stmt_close($stmt);
        break;

    // =====
    // CRUD DE UTILIZADORES (Apenas para Administradores)
    // =====
    case 'cadastrar_usuario':

```

```

        verificar_admin();

        $usuario = filter_input(INPUT_POST, 'usuario',
FILTER_SANITIZE_STRING);
        $email = filter_input(INPUT_POST, 'email', FILTER_SANITIZE_EMAIL);
        $senha_original = filter_input(INPUT_POST, 'senha',
FILTER_SANITIZE_STRING);
        $nivel = filter_input(INPUT_POST, 'nivel', FILTER_SANITIZE_STRING);

        // Criptografa a senha antes de salvar (MANDATÓRIO)
        $senha_hash = password_hash($senha_original, PASSWORD_DEFAULT);

        // Prepared Statement para INSERT
        $stmt = mysqli_prepare($conn, "INSERT INTO usuarios (usuario, email,
senha, nivel) VALUES (?, ?, ?, ?)");
        mysqli_stmt_bind_param($stmt, "ssss", $usuario, $email, $senha_hash,
$nivel);

        if (mysqli_stmt_execute($stmt)) {
            header("Location: usuarios.php?msg=Utilizador '$usuario'
cadastrado com sucesso!");
        } else {
            // Trata erro de duplicidade de utilizador (código 1062 no
MySQL)
            $erro_msg = (mysqli_errno($conn) == 1062) ? "Utilizador já
existe no banco de dados." : mysqli_error($conn);
            header("Location: usuarios_cadastrar.php?erro=Erro ao cadastrar:
" . $erro_msg);
        }
        mysqli_stmt_close($stmt);
        break;

    case 'excluir_usuario':
        verificar_admin();

        $id = filter_input(INPUT_GET, 'id', FILTER_VALIDATE_INT);

        // Não permite excluir o próprio utilizador logado
        if ($id === $_SESSION['usuario_id']) {
            header("Location: usuarios.php?erro=Você não pode excluir o seu
próprio utilizador enquanto logado.");
            exit();
        }
        if (!$id) {
            header("Location: usuarios.php?erro=ID de utilizador
inválido.");
            exit();
        }

```

```

        // Prepared Statement para DELETE
        $stmt = mysqli_prepare($conn, "DELETE FROM usuarios WHERE id = ?");
        mysqli_stmt_bind_param($stmt, "i", $id);

        if (mysqli_stmt_execute($stmt)) {
            header("Location: usuarios.php?msg=Utilizador excluído com
sucesso!");
        } else {
            header("Location: usuarios.php?erro=Erro ao excluir: " .
mysqli_error($conn));
        }
        mysqli_stmt_close($stmt);
        break;

    default:
        // Ação desconhecida
        header("Location: index.php?erro=Ação inválida ou não
especificada.");
        break;
}

mysqli_close($conn);
exit();
?>

```

Parte V: Páginas da Aplicação

7. Página Principal (index.php)

Gerencia o login e a visualização da agenda.

```

PHP
<?php
// Inclui a configuração do banco e a sessão
require_once 'config/database.php';
// Inclui o cabeçalho (início do HTML, navbar)
include 'includes/header.php';

// Variáveis para mensagens (sucesso ou erro)
$msgmensagem_sucesso = isset($_GET['msg']) ? htmlspecialchars($_GET['msg']) :
'';
$msgmensagem_erro = isset($_GET['erro']) ? htmlspecialchars($_GET['erro']) :
'';

```

```
// 1. EXIBIÇÃO DE MENSAGENS (Feedback do sistema)
if (!empty($mensagem_sucesso)):
?>
    <div class="alert alert-success alert-dismissible fade show"
role="alert">
        <strong>Sucesso!</strong> <?php echo $mensagem_sucesso; ?>
        <button type="button" class="btn-close" data-bs-dismiss="alert"
aria-label="Close"></button>
    </div>
<?php
endif;

if (!empty($mensagem_erro)):
?>
    <div class="alert alert-danger alert-dismissible fade show"
role="alert">
        <strong>Erro!</strong> <?php echo $mensagem_erro; ?>
        <button type="button" class="btn-close" data-bs-dismiss="alert"
aria-label="Close"></button>
    </div>
<?php
endif;

// 2. LÓGICA CONDICIONAL: SE LOGADO OU NÃO
if (isset($_SESSION['usuario_logado'])):
    // =====
    // ÁREA RESTRITA: UTILIZADOR LOGADO - EXIBIR AGENDA (READ)
    // =====

    // Consulta SQL para buscar todos os contatos
    $sql = "SELECT id, nome, telefone, email, data_nascimento FROM contatos
ORDER BY nome ASC";
    $resultado = mysqli_query($conn, $sql);
?>

<h1 class="mb-4">Lista Completa de Contatos </h1>

<div class="d-flex justify-content-between mb-3">
    <p class="h5 text-muted">Total de contatos: **<?php echo
mysqli_num_rows($resultado); ?>**</p>
    <a href="contatos_cadastrar.php" class="btn btn-success">+
Cadastrar Novo Contato</a>
</div>

<?php if (mysqli_num_rows($resultado) > 0): ?>
    <div class="table-responsive">
        <table class="table table-striped table-hover shadow-sm">
            <thead class="table-dark">
                <tr>
```

```

        <th>Nome</th>
        <th>Telefone</th>
        <th>Email</th>
        <th>Nascimento</th>
        <th>Ações</th>
    </tr>
</thead>
<tbody>
    <?php while ($contato = mysqli_fetch_assoc($resultado)):
?>
        <tr>
            <td><?php echo
htmlspecialchars($contato['nome']); ?></td>
            <td><?php echo
htmlspecialchars($contato['telefone']); ?></td>
            <td><?php echo
htmlspecialchars($contato['email']); ?></td>
            <td><?php echo date('d/m/Y',
strtotime($contato['data_nascimento'])); ?></td>
            <td>
                <!-- Link para editar -->
                <a href="contatos_editar.php?id=<?php echo
$contato['id']; ?>" class="btn btn-sm btn-warning me-2">Editar</a>
                <!-- Link para excluir, com confirmação via
JS -->
                <a
href="processa.php?acao=excluir_contato&id=<?php echo $contato['id']; ?>"
class="btn btn-sm btn-danger"
onclick="return confirm('Tem certeza que
deseja EXCLUIR o contato: <?php echo htmlspecialchars($contato['nome']);
?>?');">
                    Excluir
                </a>
            </td>
        </tr>
    <?php endwhile; ?>
</tbody>
</table>
</div>
<?php else: ?>
    <div class="alert alert-info">
        Sua agenda está vazia. Comece cadastrando seu primeiro contato!
    </div>
<?php endif; ?>

<?php else: ?>
    <!-- =====
    ÁREA PÚBLICA: UTILIZADOR DESLOGADO - EXIBIR FORMULÁRIO DE LOGIN

```

```

===== -->
<div class="row justify-content-center">
  <div class="col-md-7">
    <div class="card card-login shadow-lg">
      <div class="card-header bg-primary text-white text-center">
        <h2 class="mb-0">🔒 Acesso à Agenda Pessoal</h2>
      </div>
      <div class="card-body">
        <p class="text-center text-muted">Credencial de teste:
**admin** / **123456**</p>
        <form action="processa.php?acao=login" method="POST">
          <div class="mb-3">
            <label for="usuario"
class="form-label">Utilizador:</label>
            <input type="text" class="form-control"
id="usuario" name="usuario" required>
          </div>
          <div class="mb-3">
            <label for="senha"
class="form-label">Senha:</label>
            <input type="password" class="form-control"
id="senha" name="senha" required>
          </div>
          <div class="d-grid mt-4">
            <button type="submit" class="btn btn-success
btn-lg">Entrar</button>
          </div>
        </form>
      </div>
    </div>
  </div>
</div>

<?php endif;

// Inclui o rodapé
include 'includes/footer.php';
// Fecha a conexão com o banco
mysqli_close($conn);
?>

```

8. Formulário de Cadastro de Contato (contatos_cadastrar.php)

Formulario de Cadastro de Contato

PHP

```
<?php
require_once 'config/database.php';
verificar_login(); // Protege a página: só acessa se estiver logado

include 'includes/header.php';
?>

<h1 class="mb-4">✚ Cadastrar Novo Contato</h1>

<div class="card shadow">
  <div class="card-body">
    <form action="processa.php" method="POST">
      <!-- Ação para o processa.php -->
      <input type="hidden" name="acao" value="cadastrar_contato">

      <div class="row">
        <div class="col-md-6 mb-3">
          <label for="nome" class="form-label">Nome
Completo:</label>
          <input type="text" class="form-control" id="nome"
name="nome" required maxlength="100">
        </div>
        <div class="col-md-3 mb-3">
          <label for="telefone"
class="form-label">Telefone:</label>
          <input type="text" class="form-control" id="telefone"
name="telefone" maxlength="20">
        </div>
        <div class="col-md-3 mb-3">
          <label for="data_nascimento" class="form-label">Data de
Nasc.:</label>
          <input type="date" class="form-control"
id="data_nascimento" name="data_nascimento">
        </div>
      </div>

      <div class="mb-3">
        <label for="email" class="form-label">Email:</label>
        <input type="email" class="form-control" id="email"
name="email" maxlength="100">
      </div>

      <div class="mb-3">
        <label for="endereco" class="form-label">Morada
(Opcional):</label>
        <textarea class="form-control" id="endereco" name="endereco"
rows="3"></textarea>
      </div>
    </form>
  </div>
</div>
```

```

        <div class="mt-4">
            <button type="submit" class="btn btn-success btn-lg">💾
Salvar Contato</button>
            <a href="index.php" class="btn btn-secondary
btn-lg">Voltar</a>
        </div>
    </form>
</div>
</div>

<?php
include 'includes/footer.php';
?>

```

9. Formulário de Edição de Contato (contatos_editar.php)

```

PHP
<?php
require_once 'config/database.php';
verificar_login(); // Protege a página

// 1. Validação e obtenção do ID
$id = filter_input(INPUT_GET, 'id', FILTER_VALIDATE_INT);
if (!$id) {
    header("Location: index.php?erro=ID de contato inválido para edição.");
    exit();
}

// 2. Busca dos dados do contato usando Prepared Statement
$stmt = mysqli_prepare($conn, "SELECT nome, telefone, email,
data_nascimento, endereco FROM contatos WHERE id = ?");
mysqli_stmt_bind_param($stmt, "i", $id);
mysqli_stmt_execute($stmt);
$resultado = mysqli_stmt_get_result($stmt);

if (mysqli_num_rows($resultado) == 0) {
    header("Location: index.php?erro=Contato não encontrado.");
    exit();
}

$contato = mysqli_fetch_assoc($resultado);
mysqli_stmt_close($stmt);

include 'includes/header.php';

```


?>

```
<h1 class="mb-4">✎ Editar Contato: <?php echo  
htmlspecialchars($contato['nome']); ?></h1>
```

```
<div class="card shadow">  
  <div class="card-body">  
    <form action="processa.php" method="POST">  
      <!-- Campos ocultos para a lógica do processa.php -->  
      <input type="hidden" name="acao" value="editar_contato">  
      <input type="hidden" name="id" value="<?php echo $id; ?>">  
  
      <div class="row">  
        <div class="col-md-6 mb-3">  
          <label for="nome" class="form-label">Nome  
Completo:</label>  
          <input type="text" class="form-control" id="nome"  
name="nome" value="<?php echo htmlspecialchars($contato['nome']); ?>"  
required maxlength="100">  
        </div>  
        <div class="col-md-3 mb-3">  
          <label for="telefone" class="form-label">Telefone:</label>  
          <input type="text" class="form-control" id="telefone"  
name="telefone" value="<?php echo htmlspecialchars($contato['telefone']);  
?>" maxlength="20">  
        </div>  
        <div class="col-md-3 mb-3">  
          <label for="data_nascimento" class="form-label">Data de  
Nasc.:</label>  
          <!-- Garante que a data está no formato YYYY-MM-DD para  
o input type="date" -->  
          <input type="date" class="form-control"  
id="data_nascimento" name="data_nascimento" value="<?php echo  
htmlspecialchars($contato['data_nascimento']); ?>">  
        </div>  
      </div>  
  
      <div class="mb-3">  
        <label for="email" class="form-label">Email:</label>  
        <input type="email" class="form-control" id="email"  
name="email" value="<?php echo htmlspecialchars($contato['email']); ?>"  
maxlength="100">  
      </div>  
  
      <div class="mb-3">  
        <label for="endereco" class="form-label">Morada  
(Opcional):</label>
```

```

        <textarea class="form-control" id="endereco" name="endereco"
rows="3"><?php echo htmlspecialchars($contato['endereco']); ?></textarea>
    </div>

    <div class="mt-4">
        <button type="submit" class="btn btn-warning btn-lg"><img alt="Atualizar Contato" data-bbox="775 195 795 210"/>
Atualizar Contato</button>
        <a href="index.php" class="btn btn-secondary
btn-lg">Cancelar</a>
    </div>
</form>
</div>
</div>

<?php
include 'includes/footer.php';
mysqli_close($conn);
?>

```

10. Gerenciamento de Usuários (usuarios.php e usuarios_cadastrar.php)

Estas páginas só são acessíveis se o usuário logado tiver o nível Admin.

usuarios.php

```

PHP
<?php
require_once 'config/database.php';
verificar_admin(); // APENAS ADMIN PODE ACESSAR ESTA PÁGINA

include 'includes/header.php';

// Variáveis para mensagens (sucesso ou erro)
$mensagem_sucesso = isset($_GET['msg']) ? htmlspecialchars($_GET['msg']) :
'';
$mensagem_erro = isset($_GET['erro']) ? htmlspecialchars($_GET['erro']) :
'';

// 1. EXIBIÇÃO DE MENSAGENS
if (!empty($mensagem_sucesso)):
?>
    <div class="alert alert-success alert-dismissible fade show"
role="alert">
        <strong>Sucesso!</strong> <?php echo $mensagem_sucesso; ?>
        <button type="button" class="btn-close" data-bs-dismiss="alert"
aria-label="Close"></button>

```

[illegible]

```

                                echo '<span class="badge
bg-danger">Admin</span>';
                                } else {
                                echo '<span class="badge
bg-secondary">Comum</span>';
                                }
                                ?>
                                </td>
                                <td>
                                <!-- Exclusão: Botão desabilitado se for o
utilizador logado para evitar auto-exclusão -->
                                <?php if ($usuario['id'] !=
$_SESSION['usuario_id']): ?>
                                <a
href="processa.php?acao=excluir_usuario&id=<?php echo $usuario['id']; ?>"
                                class="btn btn-sm btn-danger"
                                onclick="return confirm('ATENÇÃO: Deseja
realmente EXCLUIR o utilizador: <?php echo
htmlspecialchars($usuario['usuario']); ?>');">
                                Excluir
                                </a>
                                <?php else: ?>
                                <button class="btn btn-sm
btn-outline-secondary" disabled>Você está logado(a)</button>
                                <?php endif; ?>
                                </td>
                                </tr>
                                <?php endwhile; ?>
                                </tbody>
                                </table>
                                </div>
                                <?php else: ?>
                                <div class="alert alert-warning">
                                Nenhum utilizador cadastrado.
                                </div>
                                <?php endif; ?>

                                <?php
                                include 'includes/footer.php';
                                mysqli_close($conn);
                                ?>

```

usuarios_cadastrar.php

```

PHP
<?php

```

```

require_once 'config/database.php';
verificar_admin(); // APENAS ADMIN PODE ACESSAR ESTA PÁGINA

include 'includes/header.php';

// Variáveis para mensagens
$mensagem_erro = isset($_GET['erro']) ? htmlspecialchars($_GET['erro']) :
'';
?>

<h1 class="mb-4">✚ Cadastro de Novo Utilizador do Sistema</h1>

<?php if (!empty($mensagem_erro)): ?>
    <div class="alert alert-danger" role="alert">
        <strong>Erro!</strong> <?php echo $mensagem_erro; ?>
    </div>
<?php endif; ?>

<div class="card shadow">
    <div class="card-body">
        <form action="processa.php" method="POST">
            <input type="hidden" name="acao" value="cadastrar_usuario">

            <div class="mb-3">
                <label for="usuario" class="form-label">Nome de Utilizador
(Login):</label>
                <input type="text" class="form-control" id="usuario"
name="usuario" required maxlength="50">
            </div>

            <div class="mb-3">
                <label for="email" class="form-label">Email:</label>
                <input type="email" class="form-control" id="email"
name="email" required maxlength="100">
            </div>

            <div class="mb-3">
                <label for="senha" class="form-label">Senha:</label>
                <input type="password" class="form-control" id="senha"
name="senha" required minlength="6">
                <small class="form-text text-muted">A senha será
criptografada (hash) no banco de dados.</small>
            </div>

            <div class="mb-3">
                <label for="nivel" class="form-label">Nível de
Acesso:</label>

```

```

        <select class="form-select" id="nivel" name="nivel"
required>
            <option value="Comum">Comum (Apenas gerencia
contatos)</option>
            <option value="Admin">Admin (Gerencia contatos e
utilizadores)</option>
        </select>
    </div>

    <div class="mt-4">
        <button type="submit" class="btn btn-primary btn-lg">✔
Cadastrar Utilizador</button>
        <a href="usuarios.php" class="btn btn-secondary
btn-lg">Cancelar</a>
    </div>
</form>
</div>
</div>

<?php
include 'includes/footer.php';
?>

```

Parte VI: Testando a Aplicação

1. **Abra o seu navegador** e acesse a URL da sua aplicação (ex: http://localhost/agenda_pessoal/index.php ou similar).

A primeira tela que deve aparecer é o **formulário de Login**.

Tente fazer login com as credenciais de teste:

- **Utilizador:** `admin`
- **Senha:** `123456`

Se o login for bem-sucedido, você será redirecionado para a **Lista Completa de Contatos** (<index.php>), que é a área restrita do sistema.