SecurePortal – Aplicação Web Interna

1) CONTEXTO DO PROJETO

O **SecurePortal** é uma aplicação web interna usada pelos colaboradores da organização para aceder a documentos, informações internas e políticas. O objetivo do projeto é realizar uma análise de risco baseada no **ISSO 27005**, identificando ativos, ameaças, vulnerabilidades e propondo controles de mitigação alinhados com **NIST CSF**, **CIS Controls** e **ISSO 27001**.

2) INVENTÁRIO DE ATIVOS

Ativo	Tipo	Valor	Justificação
SecurePortal (Aplicação Web)	Aplicação	Alto	Contém informação sensível interna
BD interna	Informação	Alto	Armazena credenciais e documentos
Contas de Utilizador	Identidade	Médio	Permitem acesso à aplicação
Servidor Linux	Infraestrutura	Médio	Hospeda a aplicação e a base de dados

3) RISK ASSESSMENT (ISO 27005)

1. **Risco 1 — SQL Injection:**

- **Ativo**: Base de Dados
- **Ameaça**: Acesso não autorizado através de SQL Injection
- **Vulnerabilidade**: Validação de input fraca
- **Impacto**: Alto
- **Probabilidade**: Média
- **Risco**: Alto
- **Mitigação**: input validation, prepared statements, WAF, testes SAST/DAST

2. **Risco 2 — Acesso não autorizado (autenticação fraca)**

- **Ativo**: Contas de Utilizador
- **Ameaça**: Credential stuffing / brute force
- **Vulnerabilidade**: Falta de MFA e password policy fraca
- **Impacto**: Alto
- **Probabilidade**: Média
- **Risco**: Alto
- **Mitigação**: MFA, rate limiting, password policy, monitorização e alertas

3. **Risco 3 — Falha de backups**

- **Ativo**: Base de Dados
- **Ameaça**: Perda ou corrupção de dados
- **Vulnerabilidade**: Backups irregulares sem testes
- **Impacto**: Alto
- **Probabilidade**: Baixa
- **Risco**: Médio
- **Mitigação**: backups diários, testes mensais, backups isolados

4) MATRIZ DE RISCO

Probabilidade x Impacto

	Baixa (1)	Média (2)	Alta (3)
Alta (3)	R3 (Backup Failure)	R1 + R2 (SQLi + Unauthorized)	— (Crítico)
Média (2)	— (Baixo)	— (Médio)	— (Alto)
Baixa (1)	— (Baixo)	— (Baixo)	— (Médio)

5) PLANO DE MITIGAÇÃO

Risco	Mitigação	Prioridade	Deadline
SQL Injection	Validação de inputs, WAF	Alta	30 dias
Acesso não autorizado	MFA, rate limiting	Alta	15 dias
Falha de backups	Revisão da política de backups	Média	45 dias

6) MINI ROADMAP

Sprint 1:

- Implementar MFA;

- Criar novas políticas de password;

- Rever política de backups;

Sprint 2:

- Implementar validação e higienização de inputs;

- Configurar WAF;

- Testar restauração de backup;

Sprint 3:

- Criar dashboard simples do estado dos riscos;

- Fechar documentação e reporting;