INSTITUTO UNIVERSITÁRIO DE LISBOA

Engenharia de Telecomunicações e Informática

**Segurança em Redes e Sistemas de Informação**

# Hospital de Lisboa


**Grupo 2**

João Rabuge | 98509

Bernardo Assunção | 98616

Hugo Costa | 93910

**Docente**:

Nuno Filipe Martins de Silveira Reis


**Ano curricular**: 4º

**Semestre**: 1º Semestre

**2023/2024**

## Índice

# Introdução

O objetivo deste relatório é realizar analisar o risco abrangente para uma organização fictícia - o **Hospital de Lisboa**.

Este é uma das principais **instituições de saúde do país** e composta por uma grande equipa de profissionais de saúde composta por médicos, enfermeiros, técnicos e administradores e consequentemente ter capacidade de atender mais de **300 pacientes** por dia.

Neste hospital, cada caso é um caso. E cada caso é partilhado e discutido por uma equipa **multidisciplinar**, numa concentração de **talento** e conhecimento em diferentes áreas de especialidade.

No Hospital de Lisboa, **ser recebido por um médico é ser tratado por vários**.

Ao longo deste relatório, iremos aprofundar o contexto **operacional** do Hospital de Lisboa, identificar e avaliar os seus **ativos**, enumerar potenciais **ameaças** a esses ativos, rever os **controlos** existentes, identificar **vulnerabilidades** e avaliar os **riscos** associados.

A análise de risco englobará **ameaças físicas**, **cibernéticas** e **operacionais**, oferecendo uma visão holística do cenário de **risco da organização**.

Este relatório tem como objetivo fornecer informações valiosas sobre estratégias e metodologias de **gestão do risco**, que podem ser aplicadas não só ao Hospital de Lisboa, mas também a organizações semelhantes que operam num sector em rápida evolução, competitivo e altamente regulamentado.

## Contexto

O **Hospital de Lisboa** é um hospital privado fundado com o apoio económico de várias multinacionais portuguesas. Fundado em 2017 o Hospital tem o seu edifício no Parque das Nações. Embora relativamente recente, o hospital já demonstrou um crescimento e inovação notáveis no atendimento ao utente e nas novas tecnologias ligadas à saúde apresentadas.

**Missão:** "Prestamos cuidados de saúde num ambiente que privilegia a modernidade, a funcionalidade e a segurança, mas sem esquecer o conforto e a privacidade dos doentes e das suas famílias, proporcionando-lhes uma experiência personalizada e um ambiente de confiança."

**Contexto Operacional:** O Hospital de Lisboa opera no setor de saúde privada, que é altamente dinâmico e inovador. Este setor é caracterizado por avanços tecnológicos rápidos, alta concorrência, complexidades regulatórias e necessidades evolutivas dos pacientes. O hospital opera num mercado global, com seus serviços relevantes tanto para clientes locais quanto internacionais.

A principal força desta instituição reside na sua abordagem inovadora, aproveitando a tecnologia de ponta e a pesquisa para desenvolver serviços de alta qualidade, eficientes e centrados no paciente. A sua equipa dedicada e qualificada de médicos e profissionais de saúde contribui significativamente nesta área, para seus esforços de pesquisa e desenvolvimento.

No entanto, existem Estes incluem manter-se atualizado com os avanços tecnológicos, manter uma força de trabalho qualificada e gerir riscos operacionais e cibernéticos, que serão discutidos em detalhe nas seções subsequentes deste relatório.

# Identificação e Valor Estimado dos Ativos mais Relevantes da Organização

Os ativos do Hospital de Lisboa podem ser categorizados em três grupos principais: **ativos fixos tangíveis**, **ativos intangíveis** e **ativos de dados**. Cada um desses ativos desempenha um papel crítico nas operações do hospital, e a sua perda ou degradação poderia ter consequências significativas.

## Ativos Fixos Tangíveis:

Estes são recursos **tangíveis** que o Hospital de Lisboa detém para executar as suas operações. Eles incluem as **instalações** do hospital localizadas no Parque das Nações em Lisboa, **equipamentos médicos** e de diagnóstico, e **IT**. Esses ativos são vitais para o diagnóstico do paciente e respetivo tratamento e funções administrativas. O valor total desses ativos físicos é estimado em cerca de **30 milhões de euros**.

## Ativos Intangíveis:

Os ativos intangíveis do Hospital de Lisboa são:

- **Reputação da Marca**: O Hospital de Lisboa construiu uma forte reputação desde 2017 devido à sua inovação e qualidade no setor de saúde. Esta reputação atrai pacientes, parceiros e talentosos profissionais de saúde para a organização.

- **Recursos Humanos**: A equipa deste hospital, composta por médicos experientes, investigadores e profissionais de saúde, impulsiona a sua inovação e sucesso. As habilidades coletivas, conhecimento e experiência da sua força de trabalho são ativos inestimáveis. Custam cerca de **1 milhão de euros** à empresa.

## Ativos de Dados:

Os ativos de dados do Hospital de Lisboa são:

- **Dados do Paciente**: Informações sobre as necessidades, preferências e comportamentos dos pacientes ajudam o hospital a personalizar os seus serviços, alcançando a satisfação e lealdade do paciente.

- **Dados Financeiros**: Registos detalhados das transações financeiras do hospital, orçamentos e previsões são cruciais para o planeamento estratégico e tomada de decisão.

Em seguida, é possível verificar algumas das **despesas** do Hospital de Lisboa:

| | **Preço (Milhões €)** |
|---|---|
| **Registos Médicos dos Pacientes** | 1 |
| **Equipamento Médico** | 10 |
| **Trabalhadores do Hospital** | 1 |
| **Infraestrutura de IT** | 4 |
| **Infraestrutura do Hospital** | 15 |
| **Total** | 31 |

## Identificação das ameaças aos ativos

Nesta secção irão ser exploradas as **potenciais ameaças** ao Hospital de Lisboa, e como este se **protege** dessas mesmas.

Na sua operação diária, o Hospital de Lisboa enfrenta várias ameaças que podem prejudicar os seus ativos, incluindo **ameaças físicas**, **cibernéticas** e **operacionais**.

**Ameaças Físicas**: Estas ameaças dizem respeito a potenciais danos aos ativos fixos tangíveis do hospital. Podem incluir:

- **Desastres Naturais**: Marmotos, incêndios ou terramotos que podem danificar as instalações e/ou equipamentos do hospital.
- **Roubo ou Vandalismo**: Equipamentos e/ou outros ativos fixos tangíveis podem ser roubados ou vandalizados.
- **Acidentes**: Acidentes no local de trabalho, que resulta em estragos das máquinas e/ou outros equipamentos.

**Ameaças Cibernéticas**: Dado o seu investimento tecnológico, o Hospital de Lisboa, possui um elevado risco a nível cibernético. Essas ameaças podem incluir:

- **Exposição de Dados Sensíveis**: O acesso não autorizado aos dados do hospital pode levar à exposição de informações sensíveis, como os registos médicos dos pacientes.
- **Ciberataques**: Ataques como malware, phishing, ou ataques DDoS podem interromper as operações digitais do hospital e levar à perda de dados.
- **Ameaças Internas**: Ações maliciosas de funcionários ou contratados podem levar à exposição ou perda de dados.

**Ameaças Operacionais**: Estas ameaças estão relacionadas com as operações diárias do hospital e podem incluir:

- **Falhas técnicas**: O uso contínuo dos equipamentos médicos pode levar ao desgaste ou falhas.

- **Contaminação de medicamentos ou materiais hospitalares**: Medicamentos ou instrumentos podem ser contaminados, afetando os tratamentos.

## Controlo das ameaças

Em seguida, apresentaremos as medidas de **controlo** que o Hospital de Lisboa tem em vigor para mitigar essas **ameaças**.

Para proteger os ativos e mitigar as possíveis ameaças identificadas na secção anterior, o Hospital de Lisboa implementou vários controlos.

**Medidas de Segurança Física**: O hospital garante a proteção de seus ativos fixos tangíveis através de:

- **Sistemas de Vigilância**: Câmaras de CCTV são instaladas em áreas-chave das instalações do hospital para monitorar possíveis atividades suspeitas.
- **Controlos de Acesso**: Áreas restritas são protegidas com controlos de acesso como **biometria** e sistemas de cartão-chave, onde apenas pessoas autorizadas conseguem entrar.

**Medidas de segurança cibernética**: O Hospital de Lisboa adota várias medidas de segurança cibernética para proteger seus ativos fixos tangíveis:

- **Firewalls**: São usados para bloquear o acesso não autorizado à rede do hospital, monitorizando o tráfego da rede.
- **Criptografia**: Os dados sensíveis são criptografados (AES).
- **Backups**: São realizados backups com uma frequência de 8 em 8 horas de modo a mitigar as perdas no caso de um ataque bem-sucedido.

- **Sistemas de Refrigeração:** Sistemas de refrigeração de última geração para reduzir o risco de sobreaquecimento dos servidores.

- **Autenticação de Dois Fatores**: Os funcionários do hospital são obrigados a usar a autenticação de dois fatores ao aceder a dados sensíveis ou sistemas. Foi utilizada a aplicação DUO para tal fim.

**Medidas de Segurança Operacionais**: Estas são medidas que garantem o bom funcionamento das operações e mitigam o impacto de ameaças operacionais ao máximo possível:

- **Fornecedores de Reserva**: O hospital tem acordos com fornecedores de reserva para garantir a continuidade de medicamentos no caso de interrupções na cadeia de fornecimento primário.
- **Planeamento de Sucessão**: O hospital tem sempre em vigor um plano de sucessão dos funcionários, para garantir transições suaves quando estes se ausentam.

## Vulnerabilidades Existentes

Nesta secção, identificaremos as **vulnerabilidades existentes** que podem expôr o Hospital de Lisboa a todos os riscos mencionados nas secções anteriores.

Apesar dos vários controlos implementados, o Hospital de Lisboa ainda possui certas vulnerabilidades. A identificação das mesmas é crucial para melhorar a estratégia de gestão dos riscos do hospital.

- **Base de Clientes Pequena**: Como um hospital relativamente novo no setor da saúde, e devido ao facto de ser privado e não público, o Hospital de Lisboa atualmente atende a uma base de clientes ainda relativamente pequena, embora em crescimento. Ou seja, a perda abrupta de alguns pacientes poderia impactar significativamente a receita do hospital.

- **Formações de Funcionários**: Os funcionários do departamento de IT do hospital, podem não estar cientes das últimas ameaças cibernéticas e melhores práticas para a segurança dos dados, o que pode levar a violações inadvertidas.
- **Conformidade Regulamentária**: Como o Hospital de Lisboa opera numa indústria altamente regulada, como é o caso da saúde, manter-se atualizado com as frequentes mudanças regulamentárias pode ser desafiador. O hospital pode ter dificuldades para se adaptar rapidamente de modo a cumprir os novos regulamentos, tornando-o assim suscetível a questões legais.
- **Proteção de Propriedade Intelectual**: Embora o hospital tenha patentes para algumas de suas tecnologias, pode ser desafiador proteger todas as suas inovações, deixando-o vulnerável ao roubo de propriedade intelectual.

## Avaliação de Risco

Nesta seção, **avaliaremos esses riscos com base na sua probabilidade** e potencial **impacto**.

Com base nas **vulnerabilidades anteriormente identificadas**, a avaliação de risco para o Hospital de Lisboa é a seguinte: (Todos os níveis de risco colocados são após as medidas de controlo, pois primariamente sem estas, todos eram de nível de alta prioridade)

- **Base de Clientes Pequena**: A probabilidade deste risco é **média**, no entanto, o impacto na receita e na reputação do hospital seria alto se este risco de facto acontecesse. Portanto, este risco é categorizado como de **média prioridade**.
- **Formações de Funcionários**: A probabilidade deste risco é **média**, mas o impacto potencial na segurança dos dados do paciente e na reputação do hospital é alto. Este risco é, portanto, categorizado como de **média prioridade**.
- **Conformidade Regulamentária**: A probabilidade deste risco é **alta**, dada a natureza altamente regulamentado da indústria da saúde. O impacto potencial de penalidades legais e danos à reputação também é **alto**. Portanto, este risco é categorizado como de **alta prioridade**.
- **Proteção de Propriedade Intelectual**: A probabilidade deste risco é **baixa**, devido às patentes existentes e ao conhecimento específico necessário para replicar as tecnologias do hospital. No entanto, o impacto seria significativo se ocorresse, levando à perda de vantagem competitiva. Este risco é, portanto, categorizado como de **baixa prioridade**.

Cada um desses riscos, embora **aceites** e **diagnosticados**, requer **contínua atenção** e **gestão** adequada para minimizar o seu potencial impacto no Hospital de Lisboa.

.

# Bibliografia


- Johnson, M. E. (2011). Managing information risk and the economics of security. Springer Science & Business Media.
- Anderson, J. M. (2003). Why we need a new definition of information security. Computers & Security, 22(4), 308-313.
- CNCS (2022). Guia para Gestão dos Riscos em matérias da Segurança da Informação e Cibersegurança

## Conclusão

A identificação e análise de risco realizadas para o Hospital de Lisboa revelaram várias **ameaças** e **potenciais vulnerabilidades**. Embora o Hospital de Lisboa possua excelentes **controlos**, existem áreas onde ainda se pode aprimorar mais as suas estratégias de **gestão de riscos.**

O risco de **alta prioridade** identificado, a **conformidade regulamentária**, requer atenção imediata. É recomendável ainda que o hospital se mantenha atualizado em relação às frequentes mudanças regulamentares.

O Hospital de Lisboa também deveria considerar expandir a sua **base de clientes** para reduzir a dependência de um número reduzido de pacientes através de várias medidas. Em termos de **proteção da propriedade intelectual**, é recomendável que o hospital continue a garantir patentes para as suas inovações e implemente controlos rigorosos de acesso a dados.

A **gestão de riscos** será sempre um **processo contínuo** que deve ser integrado no planeamento estratégico do hospital. Ao identificar, avaliar e abordar regularmente os riscos, o Hospital de Lisboa pode garantir a **proteção dos seus ativos**, o **normal funcionamento** das suas operações e, em última análise, proporcionar cuidados de saúde de **qualidade a todos os utentes**.

Este trabalho, forneceu uma **análise de risco** abrangente para o fictício hospital privado, **Hospital de Lisboa**. No entanto, a natureza dinâmica do ambiente de saúde requer uma **revisão** e **atualização contínua das práticas de gestão de riscos do hospital**.