UNIVERSIDADE
LUSÓFONA

# Cibersegurança associada aos RPAs

## Trabalho Final de curso

Relatório Intercalar 1º Semestre

Nome do Aluno: Rafael Lourenço da Silva

Nome do Aluno: Henrique Manuel Pinheiro da Gama Franco

Nome do Orientador: José Cascais Brás

Trabalho Final de Curso | LEI | 23/11/2024

www.ulusofona.pt

## Direitos de cópia

# Resumo

Com o aumento da complexidade e o aumento de ataques informáticos as empresas procuram métodos mais eficazes de se defender, pois os seus métodos tradicionais estão cada vez mais frágeis e suscetíveis a ataques às suas infraestruturas de rede, o que pode causar estragos significativos nas suas empresas.

Neste trabalho final de curso examinamos a complexidade dos crescentes ataques informáticos e a inadequação dos métodos utilizados nas defesas das infraestruturas de rede, propondo uma abordagem inovadora através de um Processo de Automação Inteligente (IPA) e a utilização da ferramenta Selenium.

Reconhecendo a relevância da cibersegurança e da automação, destacando o IPA como uma ferramenta promissora para identificar e mitigar vulnerabilidades críticas. Neste projeto exploramos a integração dos IPAs com a ferramenta de automação Selenium para aprimorarmos a precisão e a velocidade de resposta a incidentes, garantindo uma proteção robusta dos sistemas contra novas vulnerabilidades.

Após uma análise das soluções existentes, com destaque a solução da IBM, comparando os custos e a eficiência da solução proposta chegamos a conclusão de que o projeto considera a viabilidade da implementação, abordando custos de desenvolvimento e estratégias para a gestão dos riscos e da proteção de dados. É apresentada uma análise teórica das redes e do papel do IPA na segurança, evidenciando o valor desta abordagem na identificação de ameaças complexas.

Além disso, o projeto entra em detalhe sobre o processo de automação utilizando a tecnologia Selenium para obtenção das vulnerabilidades no website oficial da NVD. Este é um sistema que fornece vários alertas e informações sobre novas vulnerabilidades.

A metodologia adotada inclui uma abordagem interdisciplinar, com o objetivo de desenvolver um sistema dinâmico que permita uma defesa proativa e eficiente para estas novas vulnerabilidades, contribuindo assim para a integridade e segurança dos sistemas organizacionais.

# Abstract

With the increasing complexity and growing number of cyberattacks, companies are seeking more effective methods to defend themselves, as their traditional methods are becoming increasingly fragile and susceptible to attacks on their network infrastructures, potentially causing significant damage to their operations.

In this final course project, we examine the complexity of the rising cyberattacks and the inadequacy of the methods used to defend network infrastructures, proposing an innovative approach through Intelligent Process Automation (IPA) and the use of the Selenium tool.

Recognizing the relevance of cybersecurity and automation, we highlight IPA as a promising tool for identifying and mitigating critical vulnerabilities. This project explores the integration of IPAs with the Selenium automation tool to enhance accuracy and response speed to incidents, ensuring robust system protection against new vulnerabilities.

After analyzing existing solutions, particularly IBM's approach, and comparing the costs and efficiency of the proposed solution, we concluded that the project considers the feasibility of implementation, addressing development costs and strategies for risk management and data protection. A theoretical analysis of networks and the role of IPA in security is presented, emphasizing the value of this approach in identifying complex threats.

Furthermore, the project delves into the automation process using Selenium technology to retrieve vulnerabilities from the official NVD website. This system provides various alerts and information about new vulnerabilities.

The adopted methodology includes an interdisciplinary approach, aiming to develop a dynamic system that enables proactive and efficient defense against these new vulnerabilities, thus contributing to the integrity and security of organizational systems.

# Índice

# Lista de Figuras

# Lista de Tabelas

# 1 Introdução

No mundo atual, onde a evolução tecnológica evolui de forma muito rápida, o mesmo acontece para as ameaças a estas tecnologias. As organizações enfrentam desafios cada vez mais complexos para defender as suas infraestruturas digitais.

Este trabalho final de curso aborda a juncão de cibersegurança e uma automação inteligente com foco na tecnologia de Automação Inteligente de Processos (IPA) e ferramentas como o Selenium para enfrentar problemas reais relacionados a deteção de novas vulnerabilidades.

A relevância do estudo reside no cenário crescente de ataques informáticos, onde métodos tradicionais de proteção mostram-se insuficientes diante da velocidade e sofisticação das ameaças. Neste contexto é importante que surjam novas soluções inovadoras que permitam dar uma resposta rápida e eficaz na deteção de potencias riscos de segurança.

Este trabalho é fundamentado por necessidades praticas identificadas em colaboração com a empresa CGI. O objetivo é integrar ferramentas de automação inteligente para monitorar continuamente novas vulnerabilidades e reportá-las de forma estruturada e eficiente, contribuindo para a segurança e integridade dos sistemas.

## 1.1 Enquadramento

A cibersegurança tem se tornado cada vez mais em uma área prioritária devido ao grande crescimento das organizações e infraestruturas organizacionais[9]. Este trabalho insere-se nesse contexto, focando-se na integração de uma automação inteligente de processos (IPA) que cada vez é mais procurado pelas empresas[4].

A automação inteligente surge como uma ferramenta estratégica com grande capacidade na deteção de vulnerabilidades críticas de forma mais rápida possível.

Este trabalho contribui para a evolução das práticas de cibersegurança, oferecendo uma abordagem pratica e adaptada as necessidades reais das organizações.

## 1.2 Motivação e Identificação do Problema

O aumento da complexidade dos ataques informáticos e das intrusões maliciosas nas infraestruturas de rede globais representa um desafio crescente para os modelos tradicionais de defesa. Abordagens convencionais de deteção de intrusões têm se mostrado insuficientes diante da diversidade e da velocidade com que novas ameaças surgem e evoluem. A deteção manual, por sua vez, exige uma quantidade significativa de tempo e recursos, destacando a necessidade urgente de soluções automatizadas que possam monitorar e identificar ameaças de forma eficiente e precisa. Esse cenário impulsionou a CGI a propor-nos a procura por uma abordagem inovadora, capaz de automatizar o processo de deteção, garantindo uma resposta mais rápida e eficaz a potenciais ataques (alguns requisitos). Dados recentes, conforme ilustrado na Figura 1, indicam um aumento significativo no interesse por temas relacionados à cibersegurança e automação, refletindo a prioridade crescente da automação inteligente na proteção das infraestruturas digitais.


**Figura 1- Interesse em cibersegurança desde 2004 [1]**

Os sistemas de Automação de Processos Robóticos (RPA) em conjunto com o IPA podem potencialmente detetar várias vulnerabilidades nos processos e sistemas de uma organização. Conforme é visível na Figura 2, interesse em procurar informação relacionada com RPA ganhou notoriedade desde 2015 e tem mantido o interesse desde então.

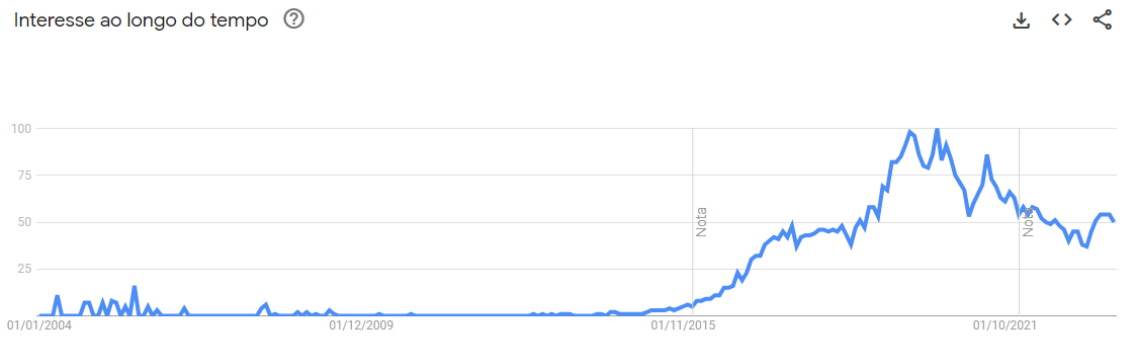


**Figura 2- Interesse em RPA desde 2004 [2]**

Algumas das vulnerabilidades que o IPA pode ajudar a identificar incluem:

Configurações de Segurança Incorretas:

Identificar instâncias em que sistemas, aplicações ou software foram configurados incorretamente, expondo potencialmente dados sensíveis ou tornando o sistema mais suscetível a ameaças informáticas.

Acesso Não Autorizado:

Monitorizar os controlos de acesso e identificar casos em que utilizadores não autorizados tentam aceder a sistemas ou dados críticos, ajudando a prevenir potenciais violações de dados ou manipulação não autorizada de dados.

Fugas de Dados:

Detetar casos em que dados sensíveis estão a ser transmitidos de forma insegura ou fora de redes seguras, ajudando a prevenir fugas de dados e garantindo a conformidade com regulamentos de proteção de dados.

Questões de Conformidade:

Ajudar as organizações a identificar situações de não conformidade com políticas internas ou regulamentos externos, garantindo que todos os processos estejam de acordo com os padrões necessários e reduzindo o risco de penalizações regulamentares.

Cifragem Inadequada:

Identificar casos em que os dados não estão adequadamente cifrados, garantindo que informações sensíveis estejam protegidas contra acesso ou interceção não autorizados.

Ataques de Phishing e Engenharia Social: Ajudar a detetar padrões ou atividades suspeitas que possam indicar a presença de ataques de phishing ou tentativas de engenharia social, permitindo que as organizações adotem medidas preventivas para proteger os seus sistemas e funcionários. Ao monitorizar ativamente essas vulnerabilidades, os sistemas de IPA podem contribuir para a postura de segurança geral de uma organização, ajudando a identificar e abordar proactivamente ameaças potenciais antes que se transformem em incidentes de segurança mais significativos.

O nosso objetivo será principalmente a automação e deteção de vulnerabilidades de Acessos não autorizados e Fugas de dados.

## 1.3 Objetivos

Um dos objetivos deste Trabalho Final de Curso é desenvolver uma solução automatizada que utiliza webscraping para extrair informação sobre as novas vulnerabilidades.

Outro objetivo é gerar um relatório em formato .xlsx com as informações que foram extraídas anteriormente.

Futuramente vamos desenvolver uma análise de dados automatizada com personalização dos relatórios e uma monitorização continua.

## 1.4 Estrutura do Documento

Na Secção 1 é apresentada uma breve introdução do trabalho.

Na secção 2 é apresentada a análise da viabilidade e pertinência do trabalho desenvolvido.

Na secção 3 é falado sobre as especificações e modelação do trabalho.

Na secção 4 falamos sobre o Estado da Arte.

Na secção 5 falamos sobre o enquadramento teórico e científico e sobre as tecnologias utilizadas.

Na secção 6 falamos sobre a solução proposta e sobre algum do trabalho já desenvolvido.

# 2 Pertinência e viabilidade

## 2.1 Pertinência

Com a evolução dos sistemas tecnológicos a aumentarem cada vez mais, implicando também o aumento da exposição dos dados e dos crimes dentro da cibersegurança é cada vez mais importante termos os nossos dados protegidos da forma mais segura possível.

Estudos indicam que o mercado de cibersegurança relacionada com a automação vai ter um grande aumento como mostra o estudo seguinte: [7]

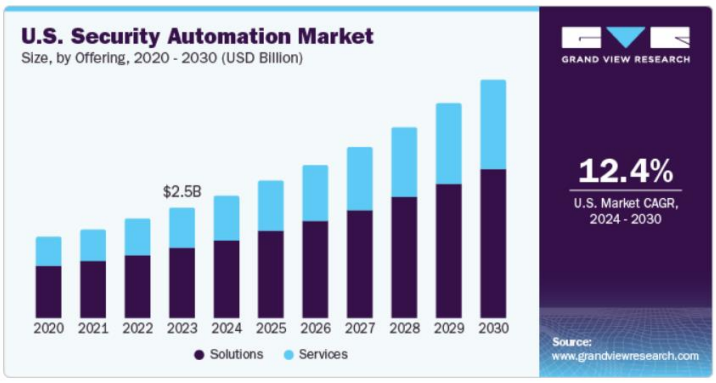


**Figura 3 - Aumento do mercado de automação na cibersegurança**

Automatizar a deteção de Acessos Não Autorizados e Fugas de Dados é crucial por várias razões fundamentais, como por exemplo:

Resposta Imediata: A automação permite uma deteção rápida e contínua de acessos não autorizados e fugas de dados, possibilitando uma resposta imediata para interromper essas atividades maliciosas antes que causem danos significativos.

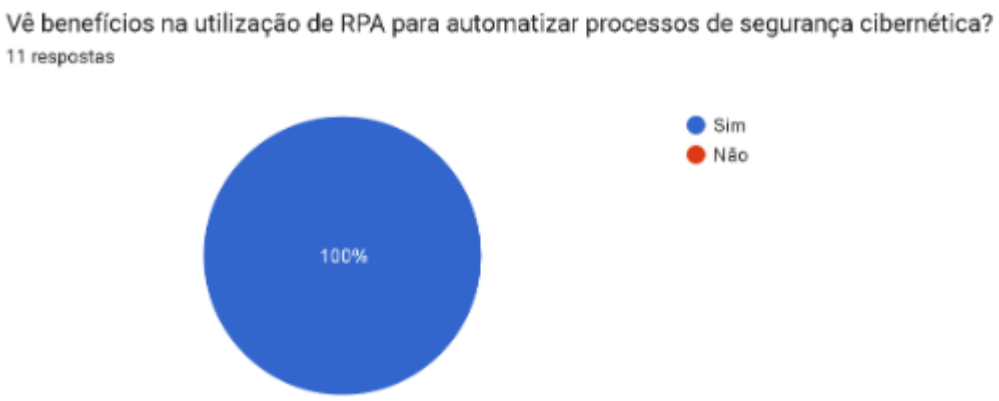


**Figura 4 - Resultados do questionário**

Redução de Riscos e Danos: A deteção precoce de acessos não autorizados e fugas de dados ajuda a mitigar riscos e reduzir potenciais danos financeiros, reputacionais e legais que podem resultar de violações de segurança.

Conformidade Regulatória: A automação na deteção dessas violações ajuda as organizações a manter a conformidade com as regulamentações de proteção de dados, evitando penalidades e sanções associadas a violações de privacidade e segurança de dados.

Proteção de Dados Sensíveis: Ao automatizar a deteção de fugas de dados, as organizações podem proteger informações sensíveis e confidenciais, garantindo a privacidade e a segurança dos dados dos clientes e funcionários.

Eficiência Operacional: A automação libera recursos humanos valiosos, permitindo que as equipas de segurança de TI se concentrem em atividades de análise mais complexas e na implementação de medidas preventivas mais robustas para fortalecer a postura de segurança geral da organização.

Prevenção de Ataques Cibernéticos: A deteção automatizada de acessos não autorizados e fugas de dados pode ajudar a identificar tentativas de intrusão e atividades maliciosas antes que os hackers tenham a oportunidade de comprometer significativamente os sistemas e dados da organização. A automação desses processos críticos não apenas aumenta a eficácia e a agilidade da deteção, mas também fortalece a capacidade de uma organização de proteger-se contra ameaças informáticas e salvaguardar a integridade dos seus dados confidenciais.

## 2.2 Viabilidade

O desenvolvimento de uma IPA envolve custos que podem variar significativamente, dependendo da escalabilidade da plataforma escolhida e da qualidade do desenvolvimento do processo robótico. Esses fatores são cruciais, pois uma plataforma escalável permite que o sistema cresça com o aumento da procura, enquanto um desenvolvimento de alta qualidade reduz os riscos de falhas e de custos de manutenção. Quando o desenvolvimento de uma IPA não atinge um padrão adequado de qualidade, as organizações podem enfrentar custos elevados de manutenção, pois problemas de inoperacionalidade nos robôs projetados para proteger e otimizar seus sistemas acarretam despesas significativas. Estes custos de manutenção, aliados ao tempo e aos recursos necessários para corrigir falhas, comprometem a rentabilidade esperada da automação.

Para que uma implementação de IPA seja bem-sucedida, não basta apenas adotar a tecnologia, é fundamental adotar uma abordagem abrangente e estratégica. Isso inclui a integração das melhores práticas de segurança para garantir que a automação não introduza vulnerabilidades e que os dados críticos da empresa permaneçam protegidos. Além disso, a gestão cuidadosa do

ciclo de vida dos produtos de IPA é essencial. Desde o planejamento e o desenvolvimento, passando por testes rigorosos, até a manutenção e eventual atualização.

A implementação de IPA deve ser vista como um compromisso contínuo, em que a organização monitora e aprimora o desempenho do robô, ajustando-o conforme necessário para que continue a agregar valor e atender às necessidades operacionais, garantindo, assim, a sustentabilidade da automação ao longo do tempo.

Alem disso, visto que é uma tecnologia recente e em constantes atualizações e descobertas, a medida que vai evoluindo pode até ser possível automatizar outras tarefas relacionadas com as vulnerabilidades, permitindo assim um progresso continuo deste projeto.

## 2.3 Análise Comparativa com Soluções Existentes

### 2.3.1 Soluções existentes

Dentro do contexto deste trabalho e aprimorando ainda mais a eficiência e precisão dos sistemas de segurança já existentes pretende-se fazer uma Automatização Avançada de Resposta a Incidentes: Integrar sistemas de resposta a incidentes totalmente automatizados que possam isolar instantaneamente partes afetadas da rede, interromper o acesso não autorizado e minimizar o impacto de eventuais fugas de dados. Para além disso, pretende-se fazer uma Análise Comportamental em Tempo Real: Desenvolver sistemas de análise comportamental em tempo real que possam detetar anomalias instantaneamente e tomar medidas corretivas imediatas para prevenir violações de segurança.

Como podemos ver na figura 3 o preço mensal seria 2704.63 para 10 robôs enquanto para um recurso em início de carreira seria um salário de 1400 € brutos que dá um total de cerca de 2000€ de custo para uma empresa hipotética. Conforme descrito na página da IBM [3].

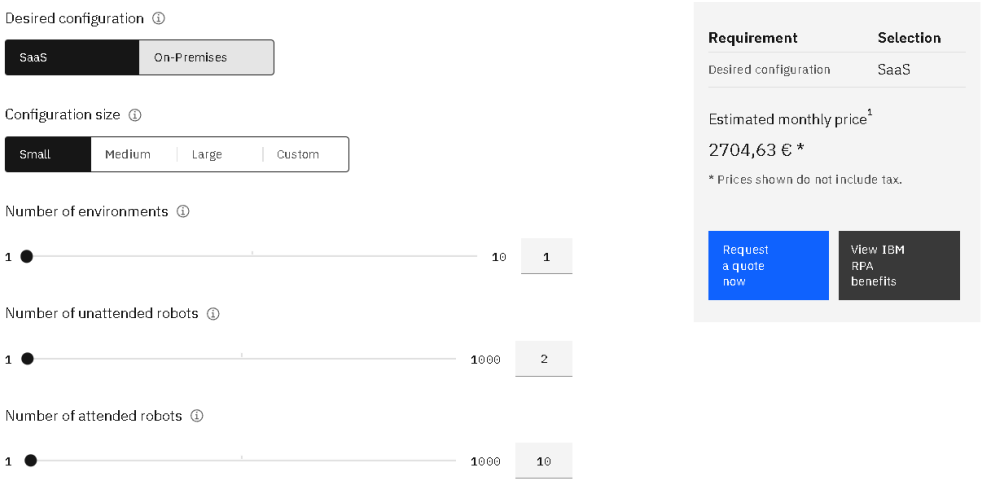


**Figura 5- IBM Robotic Process Automation Price Estimator**

### 2.3.2 Análise de benchmarking

| Funcionalidades | IBM | McAfee |
|---|---|---|
| **Resposta a incidentes em tempo real** | x | |
| **Automatização de Resposta a Ameaças** | x | x |
| **Análise de Comportamento Anômalo** | x | |
| **Segurança de Dados e Prevenção contra Perda de Dados (DLP)** | x | x |
| **Gestão de Patches** | x | |
| **Resposta a Incidentes em Tempo Real*** | x | x |
| **Soluções de Segurança para Blockchain** | | x |

**Tabela 1 - Funcionalidades**

A nossa solução propõe uma automação avançada que otimiza significativamente a resposta e deteção de incidentes, ao contrário de outras abordagens no mercado que não oferecem esta solução. Esta automação elimina processos manuais demorados e reduz a possibilidade de falhas humanas na obtenção e na comunicação das vulnerabilidades. Alem disso ao utilizar a nossa proposta a equipa de segurança consegue focar-se em outras atividades mais estratégicas.

## 2.4 Proposta de inovação e mais-valias

A solução apresenta uma abordagem inovadora no que toca a gestão de vulnerabilidades, automatizando a extração de dados, geração de relatórios e monitorização continua diferenciando-se por sua proatividade, personalização e custo-eficiência.

Para a empresa a nossa abordagem promete sustentabilidade maximizando o retorno ao reduzir os custos operacionais, mas ainda é uma alternativa acessível as soluções comerciais como também provoca um alívio na dependência de processos manuais.

## 2.5 Identificação de oportunidade de negócio

A solução pode ser explorada comercialmente como uma plataforma SaaS acessível, direcionada a pequenas e médias empresas. O diferencial está na sua acessibilidade, personalização de relatórios e monitorização contínua, oferecendo uma alternativa eficaz e de baixo custo às soluções comerciais tradicionais. Este modelo fomenta o empreendedorismo tecnológico, atendendo à crescente procura por cibersegurança eficiente e adaptada às necessidades do mercado.

# 3 Especificação e Modelação

## 3.1 Analise de Requisitos

### Requisitos funcionais:

| ID | Journey Classification | Description | MoSCoW |
|---|---|---|---|
| 1 | Identify operationl risk | O programa é executado e começa por fazer a identificação das ultimas 20 vulnerabilidades no website do NVD | Must Have |
| 2 | Identify operationl risk | Extração da informação sobre cada vulnerabilidade para um ficheiro Excel | Must Have |
| 3 | Assess operationl risk | Envio de forma automatica de um email para a equipa de segurança | Could Have |
| 4 | Assess operationl risk | O gestor deve ser capaz de ver todos os riscos disponíveis, bem como aceder a uma breve descrição, em palavras simples, sobre o propósito dos riscos. | Must Have |
| 5 | Assess operationl risk | O gestor deve ser capaz de aceder a uma descrição detalhada, em palavras simples, sobre o propósito do produto e todas as suas características e coberturas. | Sould Have |
| 6 | Make risk decision | O portal deve perguntar ao gestor se este permite o uso de informações de cookies (obrigatórios, analíticos, etc.). | Could Have |

**Figura 6 - Requisitos funcionais**

### Requisitos não funcionais:

| ID | Area | Description |
|---|---|---|
| ULHTR-5 | Availability | O programa deve ser executado a cada hora. |
| ULHTR-6 | Compatibility | O programa deve suportar os principais motores de busca |
| ULHTR-7 | Manutenção | O código deve seguir as boas práticas de programação para ter uma fácil manutenção |
| ULHTR-8 | Confiabilidade | Deve ser implementado um mecanismo de recuperação para o caso de falhas na extração da informação. |
| ULHTR-9 | Usuabilidade | O programa deve ter mensagens de erros explicitas e informar sobre o estado da execução |
| ULHTR-10 | Usuabilidade | O programa deve ter a capacidade de executar de forma inteligente, evitando a duplicação de informação |

**Figura 7 - Requisitos não funcionais**

## 3.2 Use cases

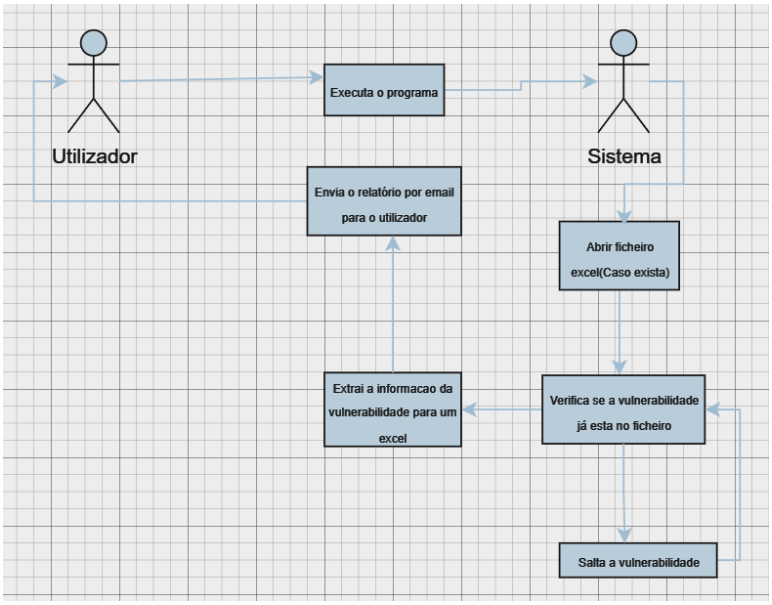


**Figura 8 - Diagrama de use cases**

# 4 Estado da arte

Há uma crescente adoção de soluções de automação para deteção de acessos não autorizados e fugas de dados, tanto por parte de empresas de tecnologia especializadas quanto por organizações que implementam soluções personalizadas para atender às suas necessidades específicas. Muitas empresas de cibersegurança oferecem plataformas e ferramentas especializadas que utilizam algoritmos avançados e inteligência artificial para identificar atividades suspeitas e possíveis violações de segurança em tempo real. Essas soluções geralmente incluem: Sistemas de Monitoramento de Segurança: Plataformas que monitoram constantemente as atividades de rede e sistemas para identificar comportamentos anómalos e potenciais ameaças. Ferramentas de Análise de Dados: Soluções de software que analisam grandes conjuntos de dados para detetar padrões incomuns ou atividades que possam indicar uma violação de segurança. Sistemas de Prevenção de Fugas de Dados (DLP): Ferramentas que monitoram e controlam o tráfego de dados dentro e fora da rede, evitando a transferência não autorizada de informações sensíveis. Sistemas de Gestão de Identidade e Acesso (IAM): Soluções que controlam e monitoram os acessos dos utilizadores aos sistemas e dados da organização, garantindo que apenas utilizadores autorizados tenham permissão para aceder a informações confidenciais. Plataformas de Segurança de Endpoint: Soluções que protegem dispositivos finais, como computadores e dispositivos móveis, contra malware, ameaças externas e possíveis violações de segurança. À medida que a necessidade de segurança cibernética robusta continua a crescer, mais empresas e organizações estão a investir em tecnologias de automação avançadas para proteger os seus ativos digitais e salvaguardar os dados sensíveis contra acessos não autorizados e fugas indesejadas.

# 5 Enquadramento teórico e científico do problema

**Cibersegurança:**

No decorrer dos anos, os sistemas informáticos evoluíram de um mero meio de comunicação para uma infraestrutura computacional ubíqua. As redes tornaram-se maiores, mais complexas, mais rápidas e altamente dinâmicas. O uso diário e generalizado de tecnologias de computação e redes em todos os aspetos da vida transformou as questões de segurança informática em questões críticas para as organizações e até mesmo em questões de segurança nacional[9].Ou seja, os sistemas precisam de ser projetados e testados com a segurança em mente desde o início e não apenas um acréscimo ou uma reflexão posterior.

Ao projetar um sistema seguro, a segurança é apenas um atributo desejável a mais para o sistema. É necessário que o foco não esteja apenas em uma solução amigável para os seus utilizadores e eficiente, mas sim existir uma solução equilibrada em todos os aspetos[10].

**Automação de Processos Robóticos (RPA):**

A Automação de Processos Robóticos (RPA) é uma tecnologia que permite automatizar tarefas repetitivas e baseadas em regras, normalmente realizadas por humanos, utilizando robôs de software ou inteligência artificial. Esses robôs são programados para executar tarefas com precisão e consistência, seguindo instruções definidas por desenvolvedores, que podem usar métodos como gravação de tela, definição de variáveis e fluxos de trabalho específicos. Algumas tarefas que o RPA pode realizar vão desde: aceder a aplicações, copiar e colar dados, enviar e-mails, preencher formulários, gerar relatórios periódicos, entre outros.

De acordo com Van der Aalst, "RPA é um termo abrangente para ferramentas que operam na interface do utilizador de outros sistemas de computador"[11]. Embora formas tradicionais de automação de processos, como gravação de tela, scraping e macros, também dependam da interface do usuário, a principal característica do RPA é sua capacidade de identificar elementos da interface diretamente, ao invés de confiar em coordenadas de tela ou seleções XPath. Isso permite uma interação mais robusta e menos propensa a erros, melhorando a confiabilidade do processo.

Desde 2020, os fornecedores de RPA relatam um aumento significativo na demanda por suas soluções, com projeções que indicam um crescimento ainda maior até 2030. Além do setor empresarial, ferramentas de RPA estão sendo cada vez mais aplicadas em áreas como auditoria, forense digital e automação industrial, mostrando-se essenciais para a transformação digital desses setores.


**Figura 9 - Aumento do mercado RPA [4]**

Com o avanço da Indústria, o RPA tornou-se uma ferramenta essencial para otimizar tarefas operacionais e oferecer vantagens competitivas, especialmente em setores que buscam a digitalização de processos. Através da integração de dados obtidos de dispositivos conectados, o RPA permite que empresas automatizem uma grande variedade de tarefas comerciais de rotina, melhorando a eficiência e reduzindo o tempo necessário para executá-las.

Diferente dos métodos tradicionais de automação, o RPA opera sobre a infraestrutura de TI existente, não necessitando de alterações significativas nos sistemas subjacentes. Esse fator reduz a complexidade da implementação, evita altos níveis de intrusão nos sistemas corporativos e permite uma integração rápida e de baixo custo.

Estudos conduzidos pela Deloitte apontam que a implementação de RPA traz melhorias significativas em aspetos essenciais para as empresas: [5]

- **92% de melhoria na conformidade**, o que garante que os processos estejam alinhados com normas e regulamentações.
- **86% de aumento na produtividade**, permitindo que as empresas realizem tarefas mais rapidamente e com maior eficiência.
- **90% de melhoria na qualidade**, reduzindo erros e aumentando a confiabilidade das operações.
- **59% de redução de custos**, aliviando as pressões financeiras e liberando recursos para outras iniciativas estratégicas.

No entanto, por ser uma tecnologia relativamente nova, o RPA ainda apresenta desafios no que diz respeito à segurança e à gestão de riscos. Como qualquer aplicação de software, o RPA está sujeito a vulnerabilidades. Para reduzir esses riscos, é fundamental que as empresas sigam princípios de segurança específicos e integrem o RPA em um quadro robusto de governança[13].

O primeiro passo para garantir a segurança é estabelecer uma estrutura de governança apropriada. Isso inclui a criação de uma estratégia de avaliação de riscos, que identifique e analise potenciais ameaças e vulnerabilidades associadas ao uso do RPA. Além disso, é essencial implementar controles de segurança, monitoramento contínuo e políticas de atualização, assegurando que os robôs operem em conformidade com os padrões de segurança da empresa e possam responder de forma ágil a novos riscos emergentes.

**Automação de processos inteligente (IPA):**

Um IPA representa a evolução das tecnologias de automação. Esta tecnologia combina RPA com Inteligência Artificial (IA) e Machine Learning (ML).

Enquanto o RPA tradicional limita-se apenas a executar tarefas repetitivas e baseadas em regras pré-programadas, o IPA eleva a automação ao próximo nível, permitindo que os sistemas aprendam e melhorem continuamente á medida que realizam mais tarefas.

Com a integração de IA e ML, os IPA são capazes de interpretar e processar grandes volumes de dados de forma rápida e eficiente. Alem disso ainda conseguem identificar padrões, tomar decisões complexas e até mesmo adaptar-se a novas situações sem a intervenção Humana. Ao contrário de uma automação estática, um IPA tem um enorme potencial de aprendizagem continua o que o torna mais eficiente e dinâmico a longo prazo.

Prevê-se um grande aumento na procura de soluções relacionadas com esta tecnologia, conforme ilustrado no gráfico a seguir.

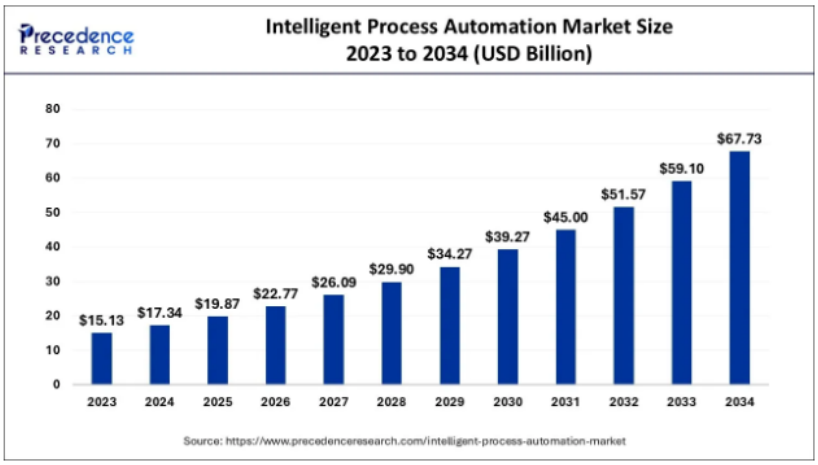


**Figura 10 - Aumento do IPA[8]**

**Selenium WebDriver:**

O Selenium é uma ferramenta poderosa no que toca à automação em navegadores, é amplamente utilizada para testes de software e, cada vez mais, utilizada estando agora em uma das ferramentas mais utilizadas para web scraping como mostra o seguinte estudo:

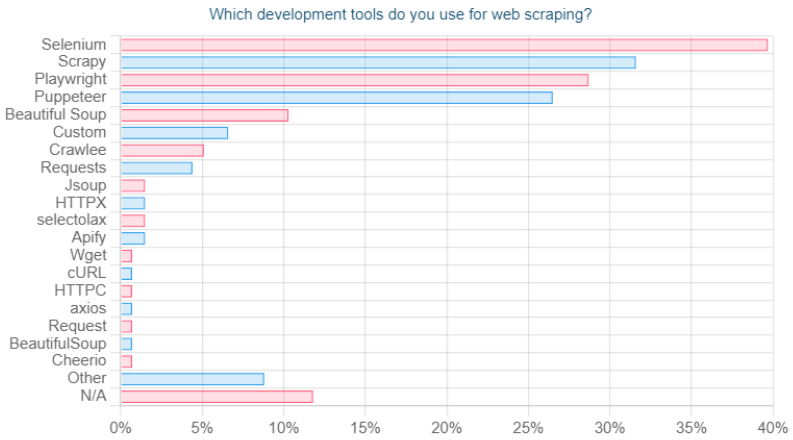


**Figura 11 - Ferramentas mais utilizadas para web scraping[6]**

O Selenium utiliza drivers específicos para cada navegador funcionando agora para todos os navegadores mais conhecidos. Os drivers servem para realizar interações com os elementos da interface dos utilizadores, como botões, tabelas, campos de texto, etc.

A obtenção de dados do website é feita a partir da identificação de elementos HTML e CSS que estão presentes no código do website, possibilitando assim a obtenção de dados mesmo em páginas que dependem de JavaScript para carregar a informação.

Desde a sua criação que tem vindo a evoluir de forma significativa, passando de uma ferramenta para automatizar testes básicos a um ecossistema que suporta vários tipos de automações complexos e com uma integração em escala. O Selenium teve um grande impacto na automação sendo utilizado por empresas não apenas para web scraping mas também para automatizar vários processos corporativos diminuindo assim o tempo gasto pelos profissionais nestas tarefas.

# 6 Solução Proposta

No âmbito da segurança cibernética, este projeto foca-se principalmente na conceção de uma solução de automação inteligente, com o objetivo de automatizar integralmente o processo de monitorização e report de vulnerabilidades cibernéticas.

A solução pretende extrair, de forma periódica e automática, informações relevantes sobre vulnerabilidades registadas no website oficial National Institute of Standards and Technology (NIST), gerar relatórios detalhados e enviar os mesmos á equipa de segurança por email.

Esta solução é altamente vantajosa, pois economiza uma hora diária do trabalho de um engenheiro, otimizando recursos, reduzindo custos e permitindo que o profissional se concentre em tarefas mais estratégicas.

## 6.1 Processo de obtenção de vulnerabilidades

A extração da informação sobre vulnerabilidades será realizada a partir da ferramenta Selenium Webdriver, uma ferramenta poderosa para automação de interações com websites. A partir desta abordagem é possível realizar um processo automático para aceder regularmente ao website do NIST (https://nvd.nist.gov) e recolher informações sobre as últimas 20 vulnerabilidades.

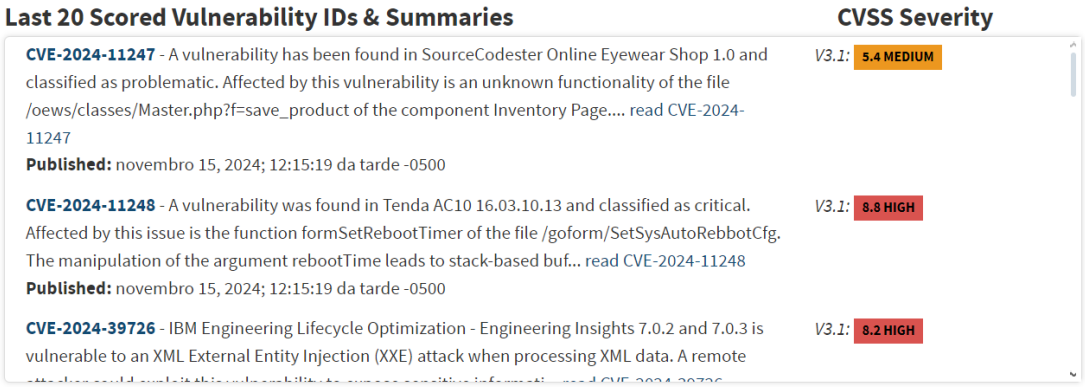


**Figura 12 - Últimas 20 vulnerabilidades**

A partir desta secção temos acesso as últimas 20 vulnerabilidades das quais vamos obter as seguintes informações: ID, descrição, severidade, data de entrada, data de publicação e a data da última modificação.

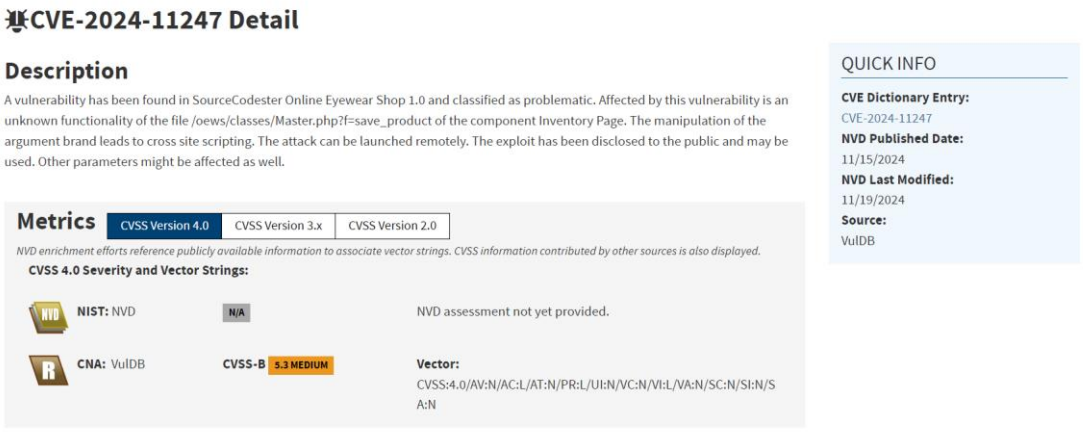


**Figura 13 - Informações sobre as vulnerabilidades**

## 6.2 Relatório

Após a obtenção da informação sobre as vulnerabilidades é gerado um relatório Excel que depois vai ser enviar por email. Este processo vai ser totalmente automatizado a partir de uma IPA permitindo assim a deteção rápida de novas vulnerabilidades.

Detalhes das informações extraídas:

- ID da vulnerabilidade (CVE)
- Descrição
- Score
- Hyperlinks
- Vector
- CWE-ID
- Nome do CWE
- Data

Esta recolha de dados vai configurada para correr automaticamente em intervalos de tempo pré-definidos, garantido assim que a equipa de segurança tem sempre as informações mais atualizadas.

## 6.3 Geração e envio do relatório

Uma vez que os dados estejam extraídos, será gerado um relatório em Excel que vai apresentar todas as informações sobre as vulnerabilidades de forma clara e percetível. O relatório vai incluir tabelas com as informações detalhadas e possivelmente gráficos para facilitar a analise.

| CVE | Descrição | Score | Hyperlinks | Vector | CWE-ID | CWE Name | Source | Data |
|---|---|---|---|---|---|---|---|---|
| CVE-2018- | In decrypt of ClearKe | 8.8 HIGH | Hyperlink Resourcehttps://source | NVD, CVSS:3.1/AV:N/AC | CWE-787 | Out-of-bounds Write | Android (ass | 11/19/2024 |
| CVE-2018- | In analyzeAxes of For | 5.5 MEDIUM | Hyperlink Resourcehttps://source | NVD, CVSS:3.1/AV:L/AC | CWE-125 | Out-of-bounds Read | Android (ass | 11/19/2024 |

Figura 10 Apresentaão de todas as informações sobre as vulnerabilidades de forma clara e percetível

Após a criação do relatório, será implementado um processo de envio automático por email para a equipa de segurança. Este processo vai ser totalmente integrado na solução de IPA, reduzindo o tempo de resposta e garantindo que os responsáveis tenham acesso a informações críticas sem atrasos.

A implementação da IPA garante que todo este ciclo, desde a obtenção da informação no website até ao envio por email, seja feito sem a intervenção manual. Este processo automático não só melhora a eficiência do projeto assim como reduz significativamente o risco de erro humano, promovendo uma vigilância continua e ativa das novas vulnerabilidades.

## 6.4 Abrangência

Nesta solução as disciplinas que achamos pertinentes para este TFC foram:

- Fundamentos de programação – Fundamentos de programação foi importante para sabermos como iniciar o projeto em python e utilizar a biblioteca Selenium
- Engenharia de software – Engenharia de software foi importante para nos conseguirmos organizar e conseguir entregar o trabalho a tempo.
- Linguagens de programação 1 – Foi fundamental para conseguirmos aceder automaticamente a um ficheiro excel.

# 7 Calendário

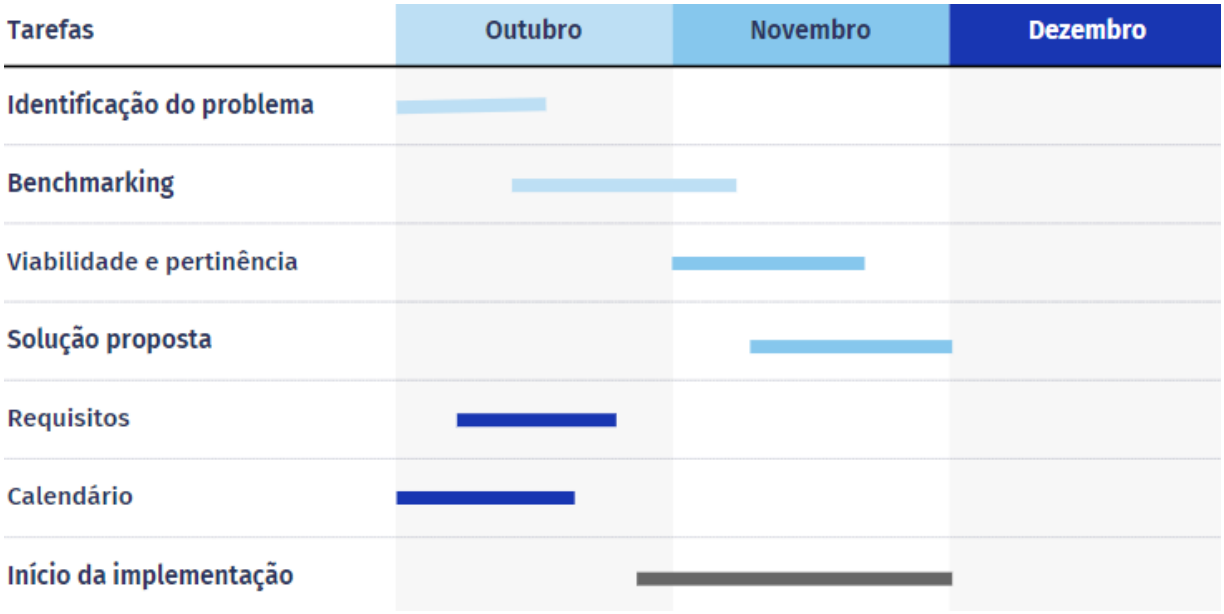


**Figura 14 - Calendário de Gaant**

# Bibliografia

[1] "Cibersegurança - Explorar - Google Trends." Accessed: Nov. 03, 2023. [Online]. Available: https://trends.google.com/trends/explore?date=all&q=Ciberseguran%C3%A7a&hl=pt-PT

[2] "Robotic Process Automation - Explorar - Google Trends." Accessed: Nov. 03, 2023.[Online].

Available: https://trends.google.com/trends/explore?date=all&q=Robotic%20Process%20Automation&hl=pt-PT

[3] "Pricing - IBM Robotic Process Automation." Accessed: Nov. 03, 2023. [Online]. Available: https://www.ibm.com/products/robotic-process-automation/pricing

[4] "Increase of robotic process automation" – Statista. Acessed: Nov.11, 2024.[Online].

Available:https://www.statista.com/statistics/1259903/robotic-process-automation-market-size-worldwide/

[5] "Melhorias da RPA nas empresas"-Deloitte. Acessed: Nov. 11, 2024.[Online]

Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-global-rpa-survey-infographic.pdf

[6] "State of Web Scraping"-Scraping Fish. Acessed: Nov. 20, 2024.[Online]

Available: https://scrapingfish.com/blog/survey-2023-results

[8] "Increase of Intelligence Process Automation" – Precedence. Acessed: Nov. 23, 2024 [Online]

Available:https://www.precedenceresearch.com/intelligent-process-automation-market

[9] Vodafone Portugal alvo de ciberataque – VodafonePortugal."https://www.vodafone.pt/press-releases/2022/2/vodafone-portugal-alvo-de-ciberataque.html"

[10] R. A. Kemmerer, “Cybersecurity,” Proceedings - International Conference on Software Engineering, pp. 705–715, 2003, doi: 10.1109/ICSE.2003.1201257.

[11] W. M. P. van der Aalst, M. Bichler, and A. Heinzl, “Robotic Process Automation,” Business and Information Systems Engineering, vol. 60, no. 4, pp. 269–272, Aug. 2018, doi: 10.1007/S12599-018-0542-4/FIGURES/1.

[12] F. Kosi, “Mercy College Robotic Process Automation (RPA) and Security A Thesis,” 2019.

# Anexo 1 – Questionário

https://docs.google.com/forms/d/1wa-9D3zWGWtbb2qpODVwG-X9_NACW49A-G649NhQUBE/edit

# Anexo 2 – Vídeo da solução implementada

https://youtu.be/f0ejzzPoDwc

# Glossário

| | |
|---|---|
| LEI | Licenciatura em Engenharia Informática |
| LIG | Licenciatura em Informática de Gestão |
| TFC | Trabalho Final de Curso |
| RPA | Automação robótica de processos |
| IPA | Automação Inteligente de Processos |