ACADEMIA MILITAR

Departamento de Estudos Pós-Graduados

Mestrado em Guerra da Informação

Modelo de Gestão de Vulnerabilidades e Risco no Suporte à Decisão.

Projeto de Investigação para a obtenção do grau de Mestre em GUERRA DA INFORMAÇÃO

Lisboa, 2019

ACADEMIA MILITAR

Mestrado em Guerra da Informação

Modelo de Gestão de Vulnerabilidades e Risco no Suporte à Decisão.

Projeto de Investigação para a obtenção do grau de Mestre em
GUERRA DA INFORMAÇÃO

Orientando: José Tolentino Da Silva Martins
Orientador: Prof. Doutor José Alberto de Jesus Borges
Coorientador: Prof. Doutor Miguel Filipe Leitão Pardal

Lisboa, 2019

Índice Geral

Índice de Figuras

Agradecimentos

Aos meus Pais, a quem devo o que sou.

À minha mulher, Maria João, e aos meus filhos Guilherme, David e Madalena pela compreensão, pela paciência e por terem suportado o fardo adicional, induzido por este esforço, eles que são o sol da minha vida

À minha cunhada, Maria João, ao meu cunhado Luís, aos meus sobrinhos Pedro e Rita e ao meu sogro João Luís.

A minha irmã Carla, ao meu irmão Rui, à Sara e ao meu sobrinho Miguel.

Aos meus Amigos, que sabem quem são e a quem durante este tempo não pude dar a atenção que mereciam.

Aos Professores da AM, que me deram a oportunidade de aprender e fizeram rever o gosto de ensinar.

Ao Professor Doutor José Borges, meu Orientador, pela paciência e flexibilidade sem a qual não teria sido possível levar a bom porto esta tarefa.

Ao Professor Doutor Miguel Pardal, meu Coorientador, pelo ânimo que conseguiu transmitir e pelo apoio incansável.

Aos meus Camaradas de Curso.

Abstract

An integrated approach to decision support in Information Security through proactive monitoring and management of vulnerabilities and risk which affect corporate assets, and consequently risk management associated to those assets, will need a model allowing decision makers to own, acquire and have, conspicuous timely available information providing them with capabilities to support decisions required by such management. A model is proposed that allows through information acquisition, evaluation and modelling, to provide vulnerability, risk and business impact metrics, and indicators related with corporate risk objectives, risk appetite and business impact assessment, Additionally, that information is complemented with results produced through data mining models, that are also supplied to decision makers and that can produce leading and lagging indicators also supporting decision process and contributing to a decision supporting system. This model provides the basic vectors to support the construction of a proactive. conspicuous, graphical and integrated dashboard that gives decision makers an agile and effective decision process able to deal with constrains of information security environment.

Keywords: Information Security, Vulnerabilities, Risk Management, BIA, Decision Support, Neural Networks, Data Mining Models

Resumo

Uma abordagem integrada do suporte à decisão no domínio da segurança da informação através de uma monitoria e gestão proactiva das vulnerabilidades e dos riscos que afetam os ativos corporativos e a consequente gestão do risco associado a esses mesmos ativos, necessitará de um modelo que permita aos decisores deterem e adquirirem, a informação, necessária e em tempo útil, que lhes permita tomar as decisões decorrentes e necessárias a essa mesma gestão. Propõe-se um modelo que permita através da aquisição, avaliação e modelação da informação, fornecer o nível de exposição das vulnerabilidades existentes nos diferentes ativos da organização e fornecer também indicadores relacionados com os objetivos corporativos de risco, apetite de risco e impacto no negócio. Adicionalmente, esta informação será complementada com informação produzida por modelos de exploração de dados, também eles fornecidos aos decisores, podendo produzir indicadores de desempenho e preditivos também eles capazes de contribuir para um sistema de suporte à decisão. Este modelo fornece os vetores básicos que permitem aos decisores construírem um painel de controlo, proactivo, conspícuo, gráfico e integrado suportando um processo de decisão ágil e efetivo capaz de lidar com os desafios colocados por este tipo de processo no âmbito da segurança da informação.

Palavras-chave: Segurança da Informação, Vulnerabilidades, Análise de Impacto no Negócio, Gestão de Risco, Suporte à Decisão, Redes neuronais, Modelos de Exploração de Dados,

Glossário de Termos

Ameaça/*Threat* – Ator ou ação capaz de explorar uma vulnerabilidade existente num ativo ou sistema de informação e por via desse facto provocar um impacto negativo no mesmo ou nos serviços que aquele suporta.

Análise de risco/*Risk Analysis*– Identificação e caracterização dos riscos associados a um evento ou ação e respetivo impacto.

Apetite de Risco / *Risk Appetite* – Nível de risco que uma organização está disposta a assumir na prossecução dos seus negócios, ou para um determinado ativo ou serviço.

Ataque/*Attack* - Tentativa de destruir, expor, alterar, desativar, retirar ou adquirir acesso não autorizado a um ativo.

Ativo/*Asset* - Qualquer bem com valor para a organização (informação, *software*, serviços, pessoas, bens intangíveis como reputação e imagem).

Ativo de informação/*Information asset* – Dados, informação ou conhecimento que possuem valor para a organização.

Autenticação – Verificação de que uma determinada característica reclamada de uma entidade está correta;

Autenticidade – Propriedade de uma entidade ser quem diz ser, ou de a informação por ela produzida poder ser verificada como autêntica.

Caminho de ataque/*Attack Path* – Possíveis caminhos utilizados pelos atacantes que podem envolver um ou diversos sistemas ou ativos da organização para realizar um ataque.

Confidencialidade – Propriedade da informação que assegura que a mesma não é disponibilizada ou acessível a pessoas, entidades ou processos não autorizados.

Controlo - Meio de gestão do risco que inclui políticas, processos, linhas de orientação, práticas ou estruturas organizacionais que podem ser administrativas, tecnológicas, de gestão ou legais.

Disponibilidade – Propriedade da informação estar acessível e utilizável a pedido de uma entidade autorizada.

Evento – Ocorrência de um conjunto particular de circunstâncias.

Exposição ao risco- Conjunto das vulnerabilidades existentes nos ativos da organização num determinado momento (Superfície de Ataque), as quais em função da possibilidade e resultado da sua exploração podem provocar danos à organização

Incidente de segurança- Ocorrência singular de evento ou série de eventos de segurança que revelam uma possibilidade de comprometer a segurança da informação e/ou as operações da organização.

Integridade – Proteção da precisão e da plenitude dos dados ou sistemas.

Intelligence **-** Produto resultante da recolha, processamento, integração, análise, avaliação e interpretação da informação recolhida de diferentes fontes com o objetivo de a transformar em ativos acionáveis e adquirir vantagens competitivas.

Impacto – Mudança negativa no nível do serviço, prestação, indicadores ou objetivos do negócio.

Malware **–** Designação genérica obtida pela agregação das palavras "*malicious software*" para referir programas ou aplicações escritas para provocar disrupções ou realizar ações não pretendidas e na qual se podem incluir diversos tipos de software malicioso, como por ex. vírus, *worms, trojan horses* e *spyware*.

Não-repúdio / *Non Repudiation* – Capacidade para demonstrar evidências inequívocas de que um determinado evento realmente aconteceu ou de que uma alegada ação foi realizada, e de que esses eventos ou ações foram realizadas por uma entidade e que tiveram uma particular origem.

Negação de serviço/*Dos*–*Denial of Service* - Tipo de ataque que visa a disrupção de um serviço, normalmente por exaustão do mesmo**.**

Negação de serviço Distribuída/*DDoS- Distributed Denial of Service* - Tipo de ataque que utiliza um número variável, normalmente milhares ou mais, de computadores como fonte de um conjunto continuado de pedidos sobre um determinado servidor ou serviço visando a disrupção do mesmo por esgotamento de recursos ou falta de capacidade de processamento;

Padrões de Ataque / *Attack Patterns* – Conjunto de ações comuns realizadas pelos atacantes para atingir determinados ativos que devido ao tipo e repetição podem constituir-se como um padrão para um determinado ataque.

Patch – atualização de software, drivers ou duma aplicação, normalmente de caracter temporário para corrigir um problema que ocorre entre a distribuição de versões dessa mesma aplicação ou software

Precisão/*Precision*- Precisão é definida como o rácio entre as identificações positivas e o somatório do total das identificações (positivas e falsas positivas). Pretende responder à questão: que percentagem das identificações positivas está de facto correta.

***RedTeam*- Equipas de segurança de informação de uma organização que desempenham o papel de atacantes, com o objetivo de detetar falhas nos recursos humanos, processo e tecnologia que a suportam. Por oposição os defensores são designados por *BlueTeam*.

Responsabilidade – O estado ou facto de ter o dever de gerir algo ou alguém.

Revisão/*Recall* – Revisão é definida como o rácio entre as identificações positivas e o somatório do total das identificações positivas com os casos de falsos negativos,

Risco de Segurança da Informação – potencial que uma determinada ameaça, explore uma vulnerabilidade de um ativo ou grupo de ativos e por essa via cause dano à organização ou aos seus objetivos de segurança ou risco.

Segurança da Informação – Preservação das propriedades de confidencialidade, integridade, disponibilidade, autenticidade, responsabilidade, não-repudio e confiabilidade associadas à informação a proteger.

Stakeholders – partes interessadas no processo ou negócio

Superfície de ataque- Conjunto das vulnerabilidades existentes nos diferentes ativos da organização num determinado instante temporal

Vulnerabilidade – Fraqueza de um ativo ou controlo que pode ser explorada por uma ameaça, com recurso a um *exploit* ou método de ataque.

***Warfare* –** Atividades e recursos envolvidos na guerra, conflito ou competição: utilizada no contexto deste documento para referir as atividades que as empresas desenvolvem em mercados competitivos.

Abreviaturas

API-Application Programming Interface – conectores definidos e específicos que permitem conectar uma aplicação ou serviço a outras aplicações ou serviços.

BIA – Análise do Impacto no Negócio/*Business Impact Analysis* – Análise do impacto ou consequências para o negócio que podem advir de um ataque bem-sucedido e identificação dos tempos necessários à recuperação dos sistemas ou ativos e do estado para que se pretende que os mesmos regressem quando recuperados em consequência desse mesmo ataque.

CERT – Computer Emergency Response Team – Grupo técnico especializado na resposta a incidentes de segurança da informação, normalmente envolvendo mais do que uma organização, entidade ou sector de negócio, podendo revestir-se de caracter nacional (CERT-PT) ou transnacional CERT-EU (Ver também ***CSIRT***)

COP- Centro de Operações de Segurança/*SOC-Security Operations Center* – Conjunto de recursos humanos, processos e tecnologia que te por objetivo prestar os serviços de recolha, identificação, armazenamento, análise, observação e resposta a incidentes de segurança da informação.

CSIRT- Computer Security Incident Response Team - Grupo técnico especializado na resposta a incidentes de segurança da informação, envolvido normalmente na primeira fase de resposta a um incidente de segurança e normalmente interno à organização,

InfoOPS- Information Operations – Operações de informações – ações realizadas para afetar as capacidades de informação e dos sistemas de informação do adversário ao mesmo tempo que preserva as próprias.

ISMS – Information Security Management System - Conjunto de recursos humanos, processos e tecnologias utilizados para, baseados na gestão do risco do negócio, estabelecer, implementar, operar, monitorar, rever, manter e melhorar a segurança da informação da organização.

KPA´s*- Key Performance Areas*

KPI´s*-Key Performance Indicators*

MTO (Maximum Tolerable Outage) – Tempo máximo que um serviço ou ativo pode estar indisponível).

P2P -Peer to Peer- Sistema constituído por nós de computação com capacidades e funções equivalentes (os pares). Sistema distribuído que não tem componentes que possam ter pontos centrais de falha.

POC- *Proof Of Concept* -Prova de Conceito

RTO -*Recovery Time Objective*- Tempo de recuperação pretendido para um determinado serviço ou ativo, após falha do mesmo sistema ou serviço.

RPO -Recovery Point Objective – Instante no tempo passado, para o qual a recuperação dos dados ou informação tem que ser realizada, após uma falha do sistema ou serviço que implique a reinicialização do mesmo.

SAD – Sistema de Apoio à decisão.

SecOPS – Security Operations – Operações de Segurança - No contexto do presente trabalho, são as operações de segurança de sistemas de informação e incluem a componente civil das InfoOPS (Information Operations) sendo normalmente realizadas nos SOC (Security Operations Center) corporativos ou nos CSIRT (Computer Security Incident Response Teams).

VUCA -*Volatile, Uncertain, Complex and Ambiguous*- Volátil, Incerto, Complexo e Ambíguo – características comuns aos sistemas relacionados com segurança de informação interligados em redes

Capítulo 1
Introdução

A presente investigação pretende apresentar uma metodologia e ferramentas que permitam modelar e suportar em tempo real a gestão de vulnerabilidades e do risco dos sistemas de informação. Esta modelação poderá depois constituir-se como um Sistema de Apoio à decisão (SAD), visando a proteção dos sistemas de informação face às ciber ameaças e ciber ataques a que os mesmos possam vir a estar sujeitos.

Considerando que o suporte à decisão em sistemas de tempo real e, no caso concreto das ciber ameaças e ataques a que os mesmos estão expostos, é característico de um ambiente VUCA[1](Yarger, 2006), a tomada de decisão num ambiente com este contexto parece poder e dever ser suportada na aquisição e manutenção da superioridade da informação que a componente civil de *InfoOPS*[2] permite.

Se considerarmos que no instante t_0, a superioridade da informação estará na posse do defensor devido ao conhecimento de que dispõe sobre a infraestrutura que defende, parece podermos afirmar, que somente uma estratégia suportada na gestão da exposição ao risco, de acordo com os objetivos corporativos e apostada em manter a vantagem competitiva inicial, poderá ser eficaz neste contexto.

Isto porque o atacante dispõe das vantagens de poder escolher o tempo do ataque t_a, o alvo a atacar (*Asset* - A_i) ou a(s) vulnerabilidade(s) (*Vulnerability* - V_i) a explorar. Estas últimas, por sua vez, alteram-se de forma dinâmica, imprevisível e desconhecida no instante inicial, e os diferentes métodos de ataque (*Attack Methods* - A_{mi}), caminhos de ataque (*Attack Paths* - A_{Pi}), padrões de ataque (*Attack Patterns* - A_{PTi}) e estratégias de diversão possíveis, vêm trazer vantagens adicionais ao atacante.

[1] *VUCA -Volatile, Uncertain, Complex and Ambiguous- Volátil, Incerto, Complexo e Ambíguo – características comuns aos sistemas relacionados com segurança de informação interligados em redes.*

[2] *InfoOPS*: Operações de informação utilizando ações para preservar a integridade dos sistemas de informação próprios da exploração, corrupção ou disrupção, ao mesmo tempo que procuram explorar corromper ou disromper as do adversário, tendo como objetivo adquirir e manter a superioridade de informação. No contexto civil/empresarial apenas as primeiras são legítimas pelo que aqui se consideram como a componente civil daquelas.

Será então necessário que os resultados decorrentes da implementação destes conceitos e modelos, permitam determinar de forma dinâmica o nível de exposição ao risco. Este risco estará materializado na análise da informação que se consiga obter sobre a superfície de ataque exposta pelo conjunto de ativos em cada momento. É também necessário que os referidos modelos, possam fornecer aos decisores as informações que permitam uma tomada de decisão em tempo real, e que simultaneamente lhes permita fazer a gestão dos ativos pelos quais são responsáveis.

Esta informação deverá considerar os objetivos de segurança desses mesmos ativos e da organização, e simultaneamente fornecer de forma intuitiva e conspícua as diferentes possibilidades de resposta, idealmente quantificadas, para que o decisor possa identificar a forma mais eficiente de resposta para um determinado contexto de *SecOPS* (*Security Operations*[3].)

Considerando outra das componentes importantes dos SAD, a interface com o utilizador, esta deveria permitir integrar e interagir de forma intuitiva com estas informações. Idealmente, sobre a forma de visualizações gráficas, com o objetivo de facilitar ao decisor os elementos de suporte à decisão, capazes de poder potenciar uma atuação proactiva, e permitindo, a visualização em continuo da superfície de ataque e do risco associado a cada um dos ativos corporativos em todo o tempo. Adicional e desejavelmente deveria ser possível disponibilizar indicadores de performance passada, do estado atual e indicadores preditivos.

[3] *SecOPS* - No contexto do presente trabalho, são as operações de segurança de sistemas de informação e incluem a componente civil das *InfoOPS (Information Operations)* sendo normalmente realizadas nos *SOC (Security Operations Center)* corporativos ou nos *CSIRT (Computer Security Incident Response Teams)*

1.1. Problema

No contexto atual as vulnerabilidades e o risco que as mesmas representam para os ativos corporativos e para as próprias empresas, são caraterizados por uma constante volatilidade, e pelo crescimento exponencial da informação que os diferentes sistemas acedem, processam, trocam e armazenam. De igual modo a informação trocada através destes sistemas está sujeita aos riscos induzidos pelas vulnerabilidades existentes nos sistemas que suportam todas essas transações de dados.

Este crescimento de transações e de dados previsivelmente crescerá ainda de forma mais acelerada com a operacionalização crescente dos dispositivos que constituem e virão a constituir a *IoT*[4], a *IoE*[5] e a *IoNT*[6] (Shukla, Chaturvedi e Simmhan, 2017).

Assim, também a quantidade de informação de segurança, disponibilizada e a disponibilizar aos decisores de topo (através de, por exemplo painéis de controlo*/dashboards*) e às equipas de resposta a incidentes e gestão operacional da segurança (*SOC´s*[7] *e CSIRT´s*[8]), tenderá a crescer, pelo que uma gestão eficiente das vulnerabilidades e do risco corporativo, apenas será possível, se esta mesma informação puder ser trabalhada, processada e disponibilizada aos decisores, em tempo útil, ou seja, muito próximo ou em tempo real.

Mas não será suficiente apresentar um conjunto de dados em bruto. Será necessário que esses dados possam ser transformados em informação pertinente para a tomada de decisão. Adicionalmente, deverá ser possível incorporar neste processamento mecanismos de suporte à decisão que permitam identificar, em tempo real, o nível de exposição ao risco dos diferentes ativos e idealmente, porque se trata de uma quantidade apreciável de informação, trabalhá-la e apresentá-la aos decisores de forma eficiente ou seja através de interfaces gráficos.

Estas interfaces devem, por outro lado, apesar da quantidade de informação que têm que processar, ter capacidade de apresentar a cada instante a informação pertinente, necessária e suficiente para o processo de decisão e apresentá-la de forma suficientemente conspícua para que de facto, habilitem o decisor a tomar uma decisão consciente,

[4] *IoT-Internet of things-*
[5] *IoE-Internet of Everything*
[6] *IoNT-Internet of Nano Things*
[7] *SOC-Security Operations Center*
[8] *CSIRT- Computer Security Incident Response Team*

suportada pela informação necessária e atualizada, sob pena de comprometerem o processo de decisão que seria suposto suportarem.

Ainda e idealmente a informação apresentada deveria ser somente a necessária e suficiente para o processo decisório e, portanto, desprovida de ruido.

O próprio processo de tomada de decisão não pode ser moroso, e por via desse facto, ineficiente colocando em risco a capacidade dos decisores e da organização agirem em tempo útil e expondo-a por esse facto a níveis de risco superiores àqueles que ela definiu através dos seus apetites pelo risco (*Risk Appetite*[9]), ainda que tenha que ter capacidade para processar as cada vez maiores quantidades de informação,

1.2. Objetivo

O objetivo do presente trabalho foi criar um modelo que permita identificar, classificar, e quantificar as vulnerabilidades, o risco associado aos diferentes ativos duma organização, de forma dinâmica, considerando as vulnerabilidades que cada um destes ativos exibe ao longo do tempo e suportar, através duma interface gráfica que exiba essa informação, os processos de decisão em contexto de operações de segurança de informação (*SecOPS*).

Assim pretendeu-se, que o modelo de gestão de vulnerabilidades e de risco criado possa depois suportar uma interface gráfica, que permita, em tempo real:

1. Visualizar a superfície de ataque de uma determinada organização, decorrente das vulnerabilidades identificadas;
2. Visualizar o nível de risco associado aos diferentes ativos decorrentes das vulnerabilidades identificadas, em cada momento e do valor dos referidos ativos para a organização;
3. Suportar o processo de decisão de *SecOPS* através da referida interface e disponibilizar *dashboards* operacionais e corporativos.

[9] *Risk Appetite*- Nível de risco que uma organização está disposta a assumir na prossecução dos seus negócios, ou para um determinado ativo ou serviço;

1.3. Justificação do tema

As ameaças atuais aos sistemas de informação podem caracterizar-se por três vetores elementares:

- a diminuição da dependência dos conhecimentos técnicos para a realização do ataque;
- o aumento da oportunidade de realização dos mesmos, diretamente relacionada com a superfície de ataque exposta em cada momento, a qual aumenta consistentemente quer porque aumentam o número de sistemas existentes, quer porque aumentam o número de vulnerabilidades conhecidas;
- movimentos cooperativos de aprendizagem e partilha de recursos entre os atacantes. (NCSC, 2017).

Assim verifica-se uma diminuição acentuada das capacidades técnicas necessárias à realização de ataques de *Malware* ou *DDoS*[10], podendo em muitos casos as ferramentas ou os próprios ataques ser obtidos ou contratados por valores relativamente baixos, na chamada *dark web/deep web*[11], o que aumenta substancialmente o número de atores capazes de os realizar.

O aumento do número de dispositivos existentes e ligados em rede ou à Internet, que aumenta por sua vez a superfície de ataque, uma vez que todos estes dispositivos terão vulnerabilidades passiveis de exploração.

Este último facto faz com que também o número de dispositivos, passiveis de ser utilizados como veículos de execução dos ataques, aumente substancialmente fornecendo uma grande quantidade de recursos para fins de C2C[12], ou como veículos diretos utilizando *bots* e *botnets*[13].

A ilustração seguinte permite observar o crescimento do número de vulnerabilidades detetadas, bem como o crescimento dos diferentes tipos de *scores* das

[10] *DDoS- Distributed Denial of Service - Negação de serviço através de ações realizadas com origem em diversos pontos da internet;;*
[11] *Dark web/Deep web*- Termo que designa um conjunto de sites/sistemas existentes em redes encriptadas e que não são passiveis de ser referenciados ou acedidos através dos motores de busca ou browsers utilizados normalmente;
[12] *C2C-Command and Control Centers*
[13] *Bot e Botnet*- programas de computador desenhados para executarem um conjunto de tarefas de forma automática, entre as quais poderão estar a distribuição de tarefas e o comando da execução das mesmas em rede designada *botnet*

mesmas sendo acentuado o crescimento de todos os tipos, mas particularmente agressivo os dos *scores Medium* e *High*.

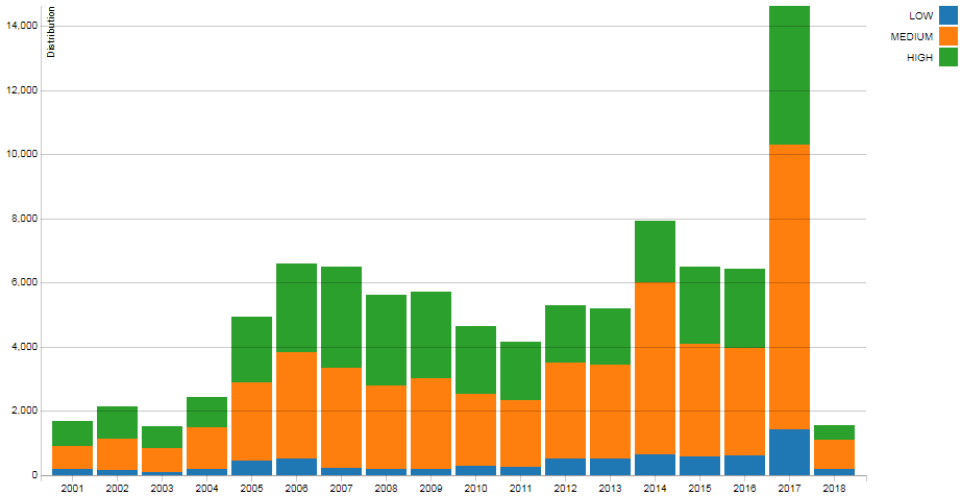


Ilustração 1- CVSS Severity Distribution Over time[14]

Finalmente a forma de atuar dos grupos e atores envolvidos neste tipo de atividades tem evoluído para um estado de maior promiscuidade e incerteza, dificultando a identificação dos atores das ações, sejam eles Estados, grupos de ativistas ou atores isolados. Esta forma de atuação dificulta a associação do tipo de ações aos atores, uma vez que estas, sejam elas ataques imitando Estados, ataques a instituições financeiras, roubos de propriedade intelectual e ataques de *ramsonware*[15], passaram a ser efetuadas indiscriminadamente pelos diferentes tipos de atores (NCSC, 2017).

Estes factos têm provocado um aumento do número de ataques detetados e reportados pelas empresas. No Reino Unido 63% das maiores empresas declararam ter detetado quebras de segurança ou ataques em 2016 (NCSC, 2017). A deteção de *malware* aumentou significativamente entre os primeiros trimestres de 2016 e de 2017 (ENISA, 2017), o número de vírus para o sistema operativo Windows aumentou a sua percentagem na totalidade do *malware* distribuído de 37 para 46% (ENISA, 2017).

Uma análise simples da distribuição das vulnerabilidades (Ilustração 2) reportadas permite verificar que mais de 50%, são classificadas com *scores* superiores a seis,

[14]Fonte: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time (*LOW, MEDIUM and HIGH is based upon the CVSS V2 Base score*)

[15] *Ramsonware*-tipo de ataque, que impede ou limita a utilização dos recursos de um computador, ou dos recursos de uma rede de computadores, exigindo o pagamento de um resgate para libertar esses mesmos recursos.

podendo, portanto, ser consideradas sérios riscos à segurança da informação dos ativos corporativos.

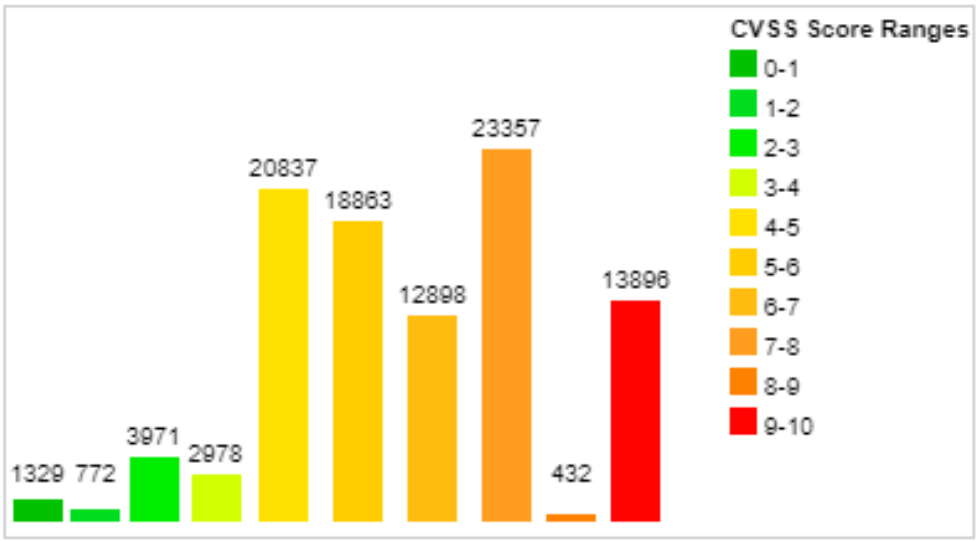


Ilustração 2- Distribuição das vulnerabilidades pelos diferentes scores CVSS[16]

No seu conjunto, o que significam estes factos para o contexto empresarial? Significam que o número, a complexidade e o âmbito destes ataques vão continuar a aumentar, bem como a sua sofisticação. Que os desafios relativos à deteção, prevenção, contenção e resposta tendencialmente crescerão quer em volume e complexidade. Que a resposta aos incidentes de maior escala terá que ser ela própria uma resposta em rede e da rede. Que este crescimento aumentará o valor relativo da aplicação de metodologias "*intelligence*[17]*-driven*"[18] e de analítica de segurança suportada em *big data* (Olstik e Esg, 2013) e analítica dedicada ao contexto da segurança da informação e dos ativos. Tudo isto em detrimento de aproximações tradicionais baseadas em defesa estática e do perímetro. Especificamente aumentará o valor da deteção das ameaças ativas e da partilha de informação e análise colaborativa da mesma (Moyle e Loeb, 2017) e dos processos de suporte à decisão neste contexto.

Estamos a entrar na era em que a gestão do risco e a prevenção, já não são suficientes. As necessidades que permitam uma visão proactiva aos CISOs (SOCs) do

[16] Fonte: https://www.cvedetails.com/cvss-score-distribution.php acedida em 15 de abril de 2018
[17] *Intelligence* – produto resultante da recolha, processamento, integração, análise, avaliação e interpretação da informação recolhida de diferentes fontes com o objetivo de a transformar em ativos acionáveis e adquirir vantagens competitivas.
[18] *Intelligence-driven* – suportada nos diferentes processos de *intelligence;*

estado da segurança dos ativos corporativos, quer dos tecnológicos, quer dos processos e recursos humanos envolvidos nos mesmos, e ainda das interfaces com o mundo exterior, em tempo real, implicam a utilização de analítica de segurança suportada em *big data*. São estas as ferramentas que vão permitir dotar as empresas de perceção situacional e *security intelligence* que lhes vai permitir afinar as respostas de segurança da informação, priorizar ações a tomar, ajustar os controles de segurança, acelerar a deteção de incidentes e aperfeiçoar os *workflows* e a coordenação, inter e extra organização, de resposta aos mesmos em tempo útil. (Webb, 2015).

1.4. Contribuições

O presente trabalho permitiu implementar um modelo que avalia o impacto das vulnerabilidades e do nível de exposição ao risco dos diferentes ativos corporativos, nas variáveis diretamente relacionadas com os impactos no negócio. Produzir e apresentar métricas e a respetiva representação gráfica das mesmas, facilitando a sua comparação e o processo decisório e obter uma visão global do nível de exposição ao risco dos diferentes ativos. Disponibilizar simuladores capazes de gerar estas mesmas para a totalidade dos ativos corporativos e ainda introduzir no processo decisório capacidades preditivas geradas a partir e três modelos de classificação.

1.5. Organização global do documento

O restante documento está organizado da seguinte forma. O capítulo 2 apresenta uma revisão da literatura e conceitos relevantes para o problema tratado e solução proposta. O capítulo 3 descreve as questões de investigação, analisa e descreve a informação utilizada e apresenta genericamente os fluxos de dados e a arquitetura da solução. O capítulo 4 descreve os processos utilizados para recolher, analisar e organizar os dados e os diferentes *datasets* utilizados. O capítulo 5 descreve os critérios utilizados para a seleção da plataforma e tecnologias a utilizar e descreve os componentes utilizados para a elaboração dos trabalhos. O capítulo 6 apresenta os resultados obtidos pelo modelo, simuladores e a análise preditiva realizada e exemplos de componentes gráficas. O capítulo 7 descreve as conclusões decorrentes do trabalho realizado e aponta possíveis linhas de investigação futura. O capítulo 8 contem as referências bibliográficas e o Anexo 9 informação complementar ou acessória referida ao longo do trabalho.

Capítulo 2
Revisão da literatura

Este capítulo apresenta uma revisão da literatura relevante para o problema tratado e a solução proposta. Aborda os conceitos de segurança de informação, vulnerabilidades e métricas que lhes estão associadas. Discute as operações de segurança da informação em contexto empresarial e a forma como as mesmas podem contribuir para melhorar a resposta corporativa aos incidentes de segurança da informação abordando as questões afetas ao processo de decisão e dos sistemas de suporte às mesmas. Descreve um processo de gestão continua e proactiva de risco e as questões relativas à análise do impacto no negócio. Aborda conceitos relativos a redes neuronais e diferentes algoritmos de resolução e de lógica difusa e ainda de exploração e visualização dos dados.

2.1. Vulnerabilidades, métricas, ataques e segurança

A segurança de informação é regulada do ponto de vista normativo pela família de normas ISO/IEC 27000, *Information Technology – Security Techniques*, onde são descritos os termos e definições utilizados naquelas (ISO/IEC 27000:2009, 2009). Pare efeitos do presente trabalho vamos abordar seguidamente um conjunto de conceitos e termos que nos permitirão uma melhor contextualização do problema.

Consideremos um sistema de informação de informação genérico o qual é composto por diversos conjuntos de ativos ou serviços (*Assets*), como sejam a infraestrutura de rede que o suporta internamente (equipamentos ativos de rede, *switches* e *routers*) e externamente (*Websites, firewall, proxies*, etc.), os sistemas de gestão das Bases de dados (SGBD) e as aplicações utilizadas nessa organização, compostas genericamente por servidores, que disponibilizam os serviços e respetivos clientes (aplicações especificas, mail server e clientes de mail, processadores de texto, etc.).

Cada um destes serviços

$$S_a$$

ou ativos

$$A_a$$

possui um determinado valor

$$€_a$$

para o negócio e possui em cada instante no tempo, vulnerabilidades.

O conjunto das vulnerabilidades existentes num determinado instante, i, no tempo, no conjunto de ativos da organização constitui a superfície de ataque,

$$Ats_t = \sum_{t=i}^{t} \vec{V}_i$$

da organização, nesse mesmo instante no tempo.

As vulnerabilidades conhecidas, *Common Vulnerabilities and Exposures*, afetando os diferentes componentes de um sistema de informação são mantidas numa base de dados aberta disponível em https://cve.mitre.org/ (MITRE, 2016), contendo para cada uma delas um identificador único, uma data de criação, descrição da vulnerabilidade, lista de referências e outra informação pertinente que pode incluir informação do vendedor do produto ou sistema afetado.

A cada uma das referidas vulnerabilidades (MITRE, [s.d.]; *NVD - Vulnerability Metrics*, [s.d.]) está por norma associada uma métrica, CVSS (*Common Vulnerability Scoring System)*, agora na versão 3, (FIRST, 2015), frequentemente usada pela indústria e pela investigação para identificar características de cada uma dessas vulnerabilidades. Essa métrica é composta por três vetores, cada um deles com um subconjunto de métricas, *base scores* (características inatas da vulnerabilidade)

$$\vec{V}_{bs}$$

temporal scores (métricas variáveis no tempo devido a acontecimentos externos à vulnerabilidade)

$$\vec{V}_{ts}$$

e *environmental scores* (métricas dependentes do impacto da vulnerabilidade numa organização especifica)

$$\vec{V}_{es}$$

.

Devido às características dos vetores referidos apenas o primeiro é disponibilizado, podendo os outros ser calculados, por cada organização, através de uma aplicação web que permite o cálculo das métricas atentas as especificidades dos respetivos *scores* $\vec{V}_{ts}$ e $\vec{V}_{es}$ (*NVD - Vulnerability Metrics*, [s.d.]).

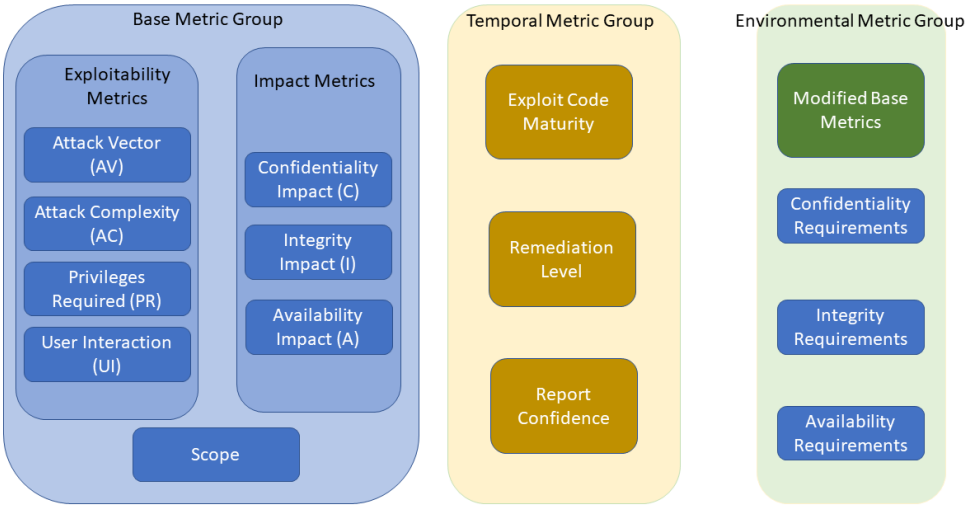


Ilustração 3- CVSS v3.0 grupos de métricas baseado em (FIRST, 2015)

Considerada como uma norma de facto, a informação disponibilizada permite atribuir métricas independentes dos fornecedores, sendo estas comummente usadas por diversos investigadores nas suas pesquisas (Cheng *et al.*, 2014; Joh e Malaiya, 2011; Noel e Jajodia, 2014).

As métricas resultantes da monitoria do estado de segurança de um sistema, obtidas pelas ferramentas de suporte à decisão, devem representar, com a maior precisão possível, o estado atual de segurança desse mesmo sistema.

Este pode ser traduzido pela sua capacidade de resistir a possíveis ataques ou à dificuldade que um atacante teria de enfrentar para conseguir explorar as vulnerabilidades existentes nesse mesmo sistema (Ortalo, Deswarte e Kaâniche, 1999) e ainda pelo diferencial entre o estado atual de segurança do sistema, face aos objetivos de segurança a definir pela organização e que o mesmo deve cumprir.

As métricas de segurança devem ser independentes das ameaças que o sistema tem de enfrentar: sendo o sistema o mesmo, independentemente do número, competência e tenacidade dos atacantes, então as suas métricas de segurança deverão ser as mesmas. O que não significa que esse mesmo sistema não seja mais facilmente permeável em função da perícia dos atacantes (Ortalo, Deswarte e Kaâniche, 1999).

Estas métricas estão diretamente relacionadas com os objetivos de segurança, sendo possível que, desde que estes mesmos objetivos não sejam violados, possam ser realizadas ações ilegítimas (Ex: aceder a informação *classificada como pública* ainda que não se tenham permissões de acesso ao sistema) (Ortalo, Deswarte e Kaâniche, 1999). E estão ainda sujeitas a alterações induzidas pelo tempo (fator temporal que afeta as

vulnerabilidades, aparecimento de novas vulnerabilidades), às alterações efetuadas ao sistema (políticas de segurança, aplicação de *patches*[19] que permitem a eliminação de vulnerabilidades conhecidas, novas vulnerabilidades decorrentes de novas funcionalidades adicionadas ao sistema) e devem ser capazes de refletir essas mesmas alterações.

O principal objetivo destas métricas será o de permitir perceber a tendência das mesmas, ou seja, ter indicadores sobre a performance da segurança do sistema. (Ortalo, Deswarte e Kaâniche, 1999), os quais podem ser do tipo *lag*[20], *current* ou *leading*.

Devem, também e ainda, permitir aferir a ameaça colocada por uma determinada vulnerabilidade se considerarmos como lineares as relações entre a valorização do fator *exploitability*[21] e a valorização do fator *impact*[22].

Disponibilizado publicamente o *Common Attack Pattern Enumeration and Classification (CAPEC™)*[23] constitui um catálogo de padrões de ataque classificados de forma intuitiva e que contém uma descrição dos ataques relacionados com cada um deles. Os padrões de ataque são descrições de elementos comuns e de técnicas utilizadas para explorar as vulnerabilidades existentes num determinado contexto. Cada um deles caracteriza a forma como cada um dos passos do ataque pode ser executado, fornecendo dessa forma informação pertinente para uma defesa eficiente e eficaz face aos mesmos.

Ataques coordenados e em larga escala (*DDoS*, *Phishing*, *Ramsonware*), que ocorrem simultaneamente em diferentes locais do globo, não são passiveis de deteção pelos *IDS´s*[24] e *IPS´s*[25] corporativos, de forma isolada, uma vez que estes estão expostos apenas a uma parte da internet e porque não detêm toda a informação disponível na rede. A

[19] *Patch* – atualização de software, drivers ou duma aplicação, normalmente de caracter temporário para corrigir um problema que ocorre entre a distribuição de versões dessa mesma aplicação ou software;
[20] Indicadores *lag*, *current*, *leading* – medidas de performance relativas respetivamente a acontecimentos passados, estado atual e preditivas sobre a performance futura.
[21] *Exploitability* – conjunto de métricas utilizadas no base score (attack vector, attack complexity, previleges required e user interaction) que permitem quantificar a facilidade de exploração de uma vulnerabilidade;
[22] *Impact* – conjunto de métricas utilizadas no base score (scope, confidentiality, integrity e availability) que permitem quantificar o impacto da exploração de uma vulnerabilidade;
[23] CAPEC - https://capec.mitre.org/- é um dicionário e uma taxonomia de classificação de ataques. Está estruturada segundo dois domínios, compostos por várias categorias que agrupam ataques que partilham características comuns;
a) Domínios de ataque: Esta vista organiza os padrões de ataque de forma hierárquica de acordo com os domínios de ataque (*Social engineering, Supply chain, communications, software, Physical security e hardware*).
b)Mecanismos de Ataque :Esta vista organiza os padrões de ataque de forma hierárquica considerando os mecanismos que são mais frequentemente utilizados para explorar uma vulnerabilidade (*Collect and analyse information, inject unexpected items, engage in deceptive interactions, manipulate timing and state, abuse existing functionality, employ probabilistic technics, subvert access control, manipulate data structures, manipulate system resources*).(MITRE, [s.d.])
[24] *IDS-Intrusion Detection System* – Sistema de deteção de Intrusões
[25] *IPS-Intrusion Prevention System*- Sistema de Prevenção de Intrusões

necessidade de suprir esta falta de informação fez surgir os *CIDS* (*Collaborative Intrusion Decision Systems)* que por sua vez levaram a dois desafios adicionais: as arquiteturas deste tipo de sistemas e os algoritmos de correlação de eventos.

As primeiras podem ser dos tipos centralizado (uma unidade de correlação central e várias unidades de deteção), hierárquico (vários níveis hierárquicos cada um deles constituído por uma unidade de deteção e outra de correlação recebendo das unidades de deteção inferiores a informação) e distribuídos (cada nó com uma unidade de correlação e outra de deteção) colaborando numa rede P2P.

Os segundos empregam técnicas de correlação de eventos que podem ser classificadas em quatro grupos: similaridade, cenário de ataque, múltiplo estágio e filtragem. Os desafios destas técnicas são comuns e podem classificar-se em dois tipos: os relativos aos recursos necessários para aumentar a eficiência, e os relativos à maximização das capacidades de deteção minimizando as necessidades de largura de banda para as comunicações entre os nós. (Zhou, Leckie e Karunasekera, 2010).

Para alem destes desafios temos ainda as dificuldades decorrentes das questões relacionadas com a privacidade, nomeadamente a relativa à disponibilidade dos pares participantes nestas redes para partilhar toda a informação necessária, relativa às suas redes e aos seus utilizadores, para por exemplo aumentar a capacidade de deteção, quando esta partilha lhes coloca desafios de privacidade, relativos por exemplo a dados dos seus utilizadores e simultaneamente pode contribuir para expor as fragilidades da sua infraestrutura. (Zhou, Leckie e Karunasekera, 2010).

A que acresce o facto de as capacidades de deteção dos IDS e os alertas disponibilizados pelos mesmos serem conhecidamente imprecisos e comportando um número significativo de falsos alertas, os quais muitas vezes mais não são que tráfego normal na rede ou ataques falhados (Wang, Liu e Jajodia, 2006).

A defesa contra ataques com múltiplos passos necessita da correlação entre os alertas ou ações isoladas e os padrões de ataque, e também que essa correlação seja feita em tempo útil, para o que, por questões de performance são utilizadas indexações em memória. Considerando que esta é finita, o conjunto de resultados de correlação apenas pode ser conservado numa *sliding window*, facto que pode ser utilizado pelos atacantes para, utilizando técnicas de espaçamento temporal dos eventos do ataque ou gerando eventos de diversão, conseguirem destruir a correlação referida. A forma de contornar este

problema foi sugerida por (Wang, Liu e Jajodia, 2006) utilizando *queue graphs*, consistindo na retenção do último alerta de cada tipo e na correlação entre alertas baseada na ordem temporal dos mesmos.

Por sua vez a quantidade de dados gerados pelas aplicações, cresce de forma acentuada, potenciada pelo maior número de aplicações na rede e pela cada vez maior quantidade de informação trocada pelas mesmas. E se a capacidade de recolher e guardar esta mesma quantidade de dados tem acompanhado este crescimento o mesmo não tem acontecido com a capacidade de analisar toda essa informação. Este facto colocou novos desafios, quer motivados pela capacidade de análise, quer pela forma de apresentar essa mesma análise aos decisores, por forma a poder dotá-los dos meios que lhes permitisse ter uma perceção situacional mais próxima da realidade, identificação conspícua de informação e para permitir uma tomada de decisão mais rápida, levando ao aparecimento de áreas como os *visual analytics*, permitindo lidar com quantidades massivas, heterogéneas e dinâmicas de volumes de informação e suportando os *dashboards* dos sistemas de decisão (Keim *et al.*, 2008).

2.2. *InfoOPS* em contexto empresarial

As ações desencadeadas no mundo empresarial, à semelhança das militares, são também realizadas sobre uma realidade em constante mutação, sujeitas a: alterações inesperadas e profundas, a um conjunto de fatores não controláveis, às pressões temporais e de contexto, decididas num contexto de informação imperfeita e pressupõem que estamos preparados para responder aos movimentos dos nossos concorrentes e competidores, estaremos assim perante uma aproximação entre os contextos estratégicos militar e empresarial (Abreu, 2002).

Assim o que diferencia, em concreto, a estratégia militar da estratégia empresarial é o uso da força física ou da violência mortífera das armas (Abreu, 2002). De igual modo, se uma estratégia nacional pode assumir uma dimensão integral, subdividida nas suas dimensões sectoriais, correspondentes às principais modalidades de coação, recursos, capacidades e instrumentos de poder – *Diplomatic, Information, Military, Economic* (*DIME*)[26], podemos assumir, no domínio da estratégia empresarial, dimensões similares se considerarmos como componente do ramo diplomático, os recursos e capacidades

[26] *DIME* – Diplomática, Informação, Militar e Económica – dimensões sectoriais da estratégia

utilizados no âmbito das relações externas e como componente do ramo militar os recursos e capacidades utilizados no âmbito das operações empresariais. Os instrumentos de poder económicos e de informação serão comuns às duas esferas atentas as especificidades e capacidades dos Estados e das Empresas.

A forma como as entidades empresariais operacionalizam as suas estratégias nos diferentes mercados, seja sob a forma de cooperação, de competição ou de conflito, e o *warfare*[27] utilizado, tem vindo a sofrer alterações ao longo do tempo. Estas tornaram-se, tão mais evidentes quanto mais foram influenciadas pelas alterações proporcionadas pelas tecnologias de informação e pela forma como as mesmas alteraram e alterarão a forma como observamos, compreendemos, decidimos e comunicamos (Waltz, 1998).

O ambiente da informação é o espaço virtual e físico no qual a informação é recebida processada e transmitida e consiste na informação propriamente dita e nos sistemas de informação (Branch, 2005). Este espaço é composto pelo conjunto de indivíduos, organizações e sistemas que recolhem, processam, disseminam ou atuam sobre a informação. Entre estes atores estão os líderes, os decisores, os indivíduos e as organizações e entre os recursos utilizados, nestas diferentes atividades, estão os sensores e sistemas utilizados para a respetiva recolha, analise, aplicação e disseminação.

Este ambiente é o local onde os humanos e os sistemas automatizados observam, orientam, decidem e agem em ciclo (*Observe, Orient, Decide and Act – OODA Loop*) sobre a informação disponível, constituindo assim o principal ambiente de tomada de decisões (Sharp, 2006).

Constituído por três dimensões, a física, a cognitiva e a da informação propriamente dita, que se consideram entrelaçadas, pelos desenvolvimentos tecnológicos que permitem que a recolha, o processamento, a disseminação, a apresentação e a proteção da informação, sejam realizadas em quantidades e velocidades difíceis de prever (Sharp, 2006), este ambiente vem trazer novos desafios e problemas adicionais. Dentro desses podemos destacar os seguintes: (1) como armazenar as enormes quantidades de informação geradas; (2) como extrair desta quantidade de informação aquela que é de facto pertinente para o processo de decisão e para a organização e (3) como tornar utilizável, em tempo útil, tal informação no ciclo e processos de suporte à decisão.

[27] *Warfare* – atividades envolvidas na guerra, conflito ou competição: utilizada no contexto deste documento para referir as atividades que as empresas desenvolvem em mercados competitivos.

Como veremos adiante um dos critérios para definir a qualidade de informação[28] é precisamente a oportunidade, ou seja, a sua disponibilidade a tempo de ser incluída no processo de decisão.

Sendo possível considerar vários critérios para aferir a qualidade da informação, face aos objetivos para que a mesma concorre, e considerando que estes condicionam os critérios de avaliação daquela como valiosa, não se poderá deixar de considerar também os recursos e o tempo necessários à produção da mesma sob pena de não ser exequível a sua utilização em tempo útil no processo de decisão (Sharp, 2006).

Idênticas questões se colocam relativamente à qualidade da informação em contexto empresarial se considerarmos os valores do *time to market*[29] impostos pelas atuais condições de concorrência.

A informação, e a interação com a mesma, afetam a competição empresarial de três formas vitais: mudam a estrutura das indústrias, e por isso alteram as regras da concorrência, criam vantagens competitivas que possibilitam às empresas novas formas de superar as suas rivais e geram novos negócios muitas vezes originados ou potenciados pelas operações existentes (Porter e Millar, 1985).

Teremos, assim e ainda, que considerar as mutações e desenvolvimentos tecnológicos, as ferramentas e aplicações que suportam a recolha, tratamento e difusão dos dados e os processos e recursos utilizados nos mesmos, os quais se afiguram como imprescindíveis para possibilitar, preservar e permitir que a informação disponibilizada tenha as qualidades necessárias para que possa ser utilizada no processo de decisão e nos sistemas que no mundo empresarial concorrem para a mesma.

Inserem-se neste contexto as ferramentas, processos e recursos utilizados para b*ig data, machine learning* e d*ata* a*nalytics* e as ferramentas de *business intelligence*, *knowledge management* e SAD (sistemas de apoio à decisão), muitas delas baseadas em redes neuronais.

Mas o ambiente da informação tem ainda camadas adicionais de complexidade motivadas pela alteração constante dos conteúdos e pelo tempo. Assim os desafios de planeamento e execução de operações militares num determinado instante e localização,

[28] *Joint Publication 3-13 Information Operations* (Figura I-2) considera os seguintes critérios de qualidade de informação: Precisão: pertinente para a situação; Relevância: que se aplica à missão atividade ou situação; Oportunidade: disponível a tempo de ser incluída no processo de decisão; Utilizável: apresentada de forma entendível; Completa: que fornece ao decisor toda a informação necessária ao processo; Breve: que possui o nível de detalhe suficiente; Segura: que foi protegida de interferências se e quando necessário.

[29] *Time to Market* – tempo necessário para uma organização conseguir passar da ideia de produto até à colocação desse mesmo produto no mercado.

estão permanentemente a ser influenciados por um conjunto ininterrupto de fatores que alteram o ambiente da informação no longo, médio e curto prazo (Sharp, 2006).

É este também o ambiente em que têm que operar as estruturas empresariais das sociedades modernas. A informação e as tecnologias de informação estão a afetar todos os processos que as companhias usam na sua operação e a afetar a sua cadeia de valor. Este conjunto de atividades ou processos interdependentes, encontram-se ligados por diferentes elos de tal modo que, a forma como uma atividade é realizada, influencia o custo ou eficiência das outas atividades.

Estes elos não só ligam e afetam as atividades ou processos internos como criam interdependências entre a cadeia de valor da empresa e a dos seus fornecedores e clientes. Cada elemento da cadeia de valor tem uma componente material e uma componente de informação. E se durante a maior parte da história industrial os progressos tecnológicos afetaram somente o elemento físico da cadeia de valor, assistimos agora ao facto de esta afetação incidir nas duas componentes, material e de informação, mas sobretudo na componente da informação e dos fluxos de informação (Porter e Millar, 1985).

Assistimos assim a uma produção de um fluxo de dados contínuo, gerado ao longo de toda a cadeia de valor, que tornam esses mesmos dados, a informação que transportam e o conhecimento que permitem gerar em elementos críticos para a criação de vantagens competitivas.

As tecnologias de informação não estão apenas a afetar a cadeia de valor. Estão também a transformar a natureza da cooperação, da competição e dos mercados. Assim podemos afirmar que a informação e a tecnologia têm um poderoso efeito em termos de vantagem competitiva quer na afetação dos custos quer na exploração das mudanças do ambiente competitivo (Porter e Millar, 1985).

As mudanças conjunturais potenciadas por uma sociedade de atores permanentemente ligados à rede, uma rede onde os clientes, os fornecedores, os competidores e a cadeia de distribuição podem estar em todo o lado, em todo o tempo, vem também introduzir fatores adicionais de mudança, como sejam a compressão do *time to market* e a geração de quantidades massivas de dados e informação que ainda mais potenciam a necessidade da introdução de mecanismos de processamento dessa mesma informação, e a sua transformação em conhecimento e em vantagens competitivas tangíveis ao longo de toda a cadeia de valor da empresa (Porter e Millar, 1985).

De igual modo neste contexto onde as forças estão permanentemente ligadas em rede e onde esta possibilita a capacidade de partilhar e trocar informação entre unidades e

elementos dispersos geograficamente: sensores (independentemente da plataforma), atores e promotores de efeitos (independentemente do serviços), decisores e organizações de suporte (independentemente da localização) uma força em rede é uma força interoperável, com acesso global a informação de qualidade quando e onde for preciso (Branch, 2005), e que visa adquirir e manter a superioridade de informação relativamente aos seus competidores.

As organizações comerciais, têm vindo a liderar este processo, e a adotar e implementar os conceitos decorrentes da era da informação impulsionadas pela competitividade acrescida, pela remoção das barreiras à entrada de novos concorrentes, e pelas vantagens competitivas que esta mesma adoção, potenciada nos novos competidores por estruturas mais jovens e mais ágeis lhes garante.

Acresce que a própria sociedade de informação permite o acesso mais fácil às estratégias ou opções utilizadas pelos diferentes competidores possibilitando uma aprendizagem mais rápida pelos novos participantes que tiram assim partido dos erros eventualmente cometidos pelos *first movers* ou pelos dominantes(Alberts, Garstka e Stein, 1999)

Uma lição fundamental que emergiu de vários domínios foi a de que o poder de uma nova tecnologia podendo ser inicialmente disruptivo, não é por si só suficiente para garantir uma superioridade de informação ou competitiva sustentada, se o mesmo não for suportado pela capacidade simultânea da organização em se adaptar e adaptar os seus processos de negócio a essa mesma tecnologia(Alberts, Garstka e Stein, 1999).

As diferentes fases observadas no tecido empresarial que permitiram construir a superioridade de informação, potenciadas pelos princípios da *Network Centric Warfare*, podem ser enumeradas considerando um espaço de duas dimensões, uma tecnológica e outra de Organização e Processos.

Materializada inicialmente por uma integração vertical (tecnologicamente suportada pelos Mainframes e com débeis componentes de organização e processos) seguida de uma fase de "produção e venda" (caracterizada pela utilização dos PC´s e fases iniciais de implementação de organização e processos), progredindo para a fase de "integração virtual" (baseada em arquiteturas cliente servidor e maturação dos processos corporativos) depois materializada na fase de "*Sense and Respond*" (suportada na internet e no inicio da disrupção dos modelos hierárquicos organizativos) e por fim nas duas ultimas fases "Self-syncronization" e "Competitive Space Awareness"(Alberts, Garstka e Stein, 1999)

Estas duas ultimas fases caraterizam-se pela cada vez maior utilização de tecnologias em rede ou distribuídas, cada vez mais baseadas na nuvem, e pela capacidade que estas têm de introduzir no modelo de negócio a produção de indicadores de desempenho, do estado atual e preditivos, gerada pela banalização de modelos preditivos e de inteligência artificial, que permitem a quem os adota a aquisição de vantagens competitivas e de superioridade de informação.

Na vertente organizativa a superioridade de informação caracteriza-se por modelos organizativos menos rígidos e com menos níveis hierárquicos, que permitem a operacionalização dessa mesma superioridade de informação através da sua transferência ao longo de toda a "rede" e da autonomização da capacidade de resposta, até às operações as quais serão tendencialmente suportadas pelos SAD, materializando a desejada superioridade de informação e utilizando-a em todos os processos do negócio.

Para a realização de operações neste contexto será necessário que a organização disponha de um mínimo de quatro capacidades: a capacidade de percecionar a situação, a capacidade de atuar em cooperação com os seus parceiros, a posse dos meios necessários à realização das ações pretendidas e a capacidade de empregar de forma coordenada e atempada esses mesmos meios (Alberts e Hayes, 2003).

Os princípios da guerra centrada em rede *Network Centric Warfare (NCW)* fornecem a base para uma cadeia de valor que se estende a partir de um conjunto de capacidades específicas para a agilidade e eficácia operacionais. Esta cadeia de valor pode proporcionar um contexto para avaliar tanto o valor de mudanças numa medida ou conjunto de medidas, como o contexto para determinar a validade dos próprios princípios da guerra centrada em rede. As quatro capacidades acima mencionadas, perceção situacional, atuação cooperativa, disponibilidade de meios e emprego coordenado de forças juntamente com as características e atributos necessários à ação e a sua relação são características das forças da Era da Informação (Alberts e Hayes, 2003).

É importante notar que não se tratam de variáveis apenas afetas ao ator no sentido individual, mas de variáveis que dizem respeito à equipa, grupo, ou organização e às capacidades de tomada de decisão. Estas equipas, grupos e atributos organizacionais incluem o grau em que a informação é partilhada e a consciência da partilhada alcançada. Estão no centro dos processos colaborativos e comportamentos de auto sincronização que a *Network Centric Warfare (NCW)* procura explorar (Alberts e Hayes, 2003).

2.3. Sistemas de Apoio à Decisão

Os Sistemas de Apoio à Decisão (SAD), baseiam-se em sistemas computacionais e no auxílio fornecido pela utilização desses mesmos sistemas no processo decisório (Keen, 1980). Assim, estes sistemas tornam-se principalmente valiosos na escolha de uma solução final para um problema de tomada de decisão complexo, permitindo ao decisor uma ponderação eficiente de diferentes critérios com vista à obtenção de uma decisão satisfatória. Este processo permite auxiliar a escolha, ordenação e classificação de diferentes alternativas no processo de tomada de decisão.

As principais características associadas à tomada de decisões em ambientes complexos, e que consideram fatores como: a competitividade, questões conflituantes, recursos limitados, excesso e dispersão de informação, necessidade de decisões em tempo-real, custos associados e qualidade da decisão, são todos atributos nucleares dos sistemas de apoio à decisão (Borges, 2015)

Como componentes fundamentais dum SAD, teremos então, os dados, o modelo e a interface de utilizador que suporta o processo de tomada de decisão.

Relativamente aos dados teremos que considerar o local e forma como se encontram armazenados (SGBD[30], memória, texto, etc.), como chegam aos SAD (*Data Sources, Data Feeders, Data Pools e Data Lakes)*, a sua origem (interna ou externa), a forma como e se estão organizados (em bruto[31], correlacionados ou processados), como alimentam o processo de tomada de decisão (em tempo real ou históricos), o tipo de dados (contínuos ou discretos) e se fazem ou não parte de um conjunto recolhido ao longo do tempo (séries temporais ou valores individuais).

O modelo que suporta o processo de decisão representa de forma simplificada e abstrata os diferentes componentes, estados, operadores e funções de um determinado problema.

A interface de utilizador permite interagir com o processo de tomada de decisão e fornecer ao utilizador a informação pertinente à tomada de decisão, de forma conspícua, facilmente manipulável e idealmente com recurso a ferramentas gráficas.

[30] SGBD- Sistemas de Gestão de Bases de Dados

[31] Dados em bruto - dados tal qual como resultaram do processo de recolha dos mesmos, sem qualquer tipo de tratamento, classificação ou processamento.

Considerando a impossibilidade de representar todos os estados possíveis de uma determinada realidade os sistemas de apoio à decisão precisam de uma forma simplificada de representar essa mesma realidade.

Para essa representação recorre-se a modelos, ou seja, a representações simplificadas da realidade, suportada por uma estrutura de conceitos, representando uma "observação" parcial dessa mesma realidade. No caso dos sistemas muito complexos é muitas vezes utilizada uma aproximação que passa pela criação de modelos simples, os quais, uma vez concatenados, permitem a modelação do sistema complexo.

Qualquer sistema poderá ser descrito ou composto por estados, conjuntos de operadores, funções de teste do objetivo e funções de utilidade. Os estados possíveis num determinado sistema, espaço dos estados, é constituído por todos os estados passíveis de existência no domínio desse sistema, ou seja, todos os estados iniciais, intermédios ou finais observáveis no sistema.

Os operadores são o conjunto de operações que uma vez realizadas sobre um determinado estado permitem a passagem para um outro estado. O caminho que, no espaço de estados, une o estado inicial ao estado final representa a solução e a forma de a atingir (Borges, 2015).

Os tipos de problemas colocados neste contexto podem ser classificados como problemas estruturados, semiestruturados e não estruturados.

Os problemas estruturados são aqueles cuja resolução resulta de processos de decisão que podem ser previamente especificados, que se caracterizam por serem repetitivos ou sistemáticos, por terem modelos de solução padronizados e por via desse facto, permitirem processos de decisão passíveis de serem automatizados.

Por outro lado, os problemas não estruturados caracterizam-se por, resultarem de eventos únicos ou pouco frequentes, não ser possível determinar para os mesmos, soluções padronizadas, carecerem de avaliação por peritos e não sendo possível antecipadamente definir os processos de decisão, não terem soluções padrão.

Os problemas semiestruturados por sua vez são caracterizados por conterem nalgumas fases do processo de decisão fases ou elementos repetitivos ou sistemáticos, poderem ser abordados com processos de decisão pré-definidos, mas estes não serem suficientes para uma recomendação definitiva relativamente à decisão.

A procura da solução, no caso dos problemas solucionáveis, que têm uma ou mais soluções, sendo que uma das soluções será potencialmente a melhor, é realizada através de um processo iterativo de busca dessa mesma solução.

A abordagem utilizada na procura da solução pode ser derivativa ou generativa.

A abordagem derivativa é passível de utilização em problemas em que o espaço dos estados possíveis é completa e previamente conhecido, cada um destes estados é uma potencial solução e os estados iniciais são consequência dos dados do problema. Temos assim que todas as hipóteses de resolução do problema são conhecidas, consistindo a resolução do problema na derivação de hipóteses que permitam encontrar um "caminho" que ligue os estados iniciais e os estados solução.

A abordagem generativa é utilizável quando conhecendo os estados de partida possíveis, os estados possíveis seguintes apenas são conhecidos aquando da sua criação e esta criação pode ser condicionada por conjuntos de restrições e ou critérios de avaliação os quais incluem conhecimento heurístico.

2.4. Perceção situacional e decisão em contexto de incerteza

O modelo de três níveis de perceção situacional desenvolvido por (Endsley, 2000), foi elaborado para ambientes onde se pretendia que os humanos enfrentassem situações caracterizadas por contextos em constante e rápida mudança, e aplicado inicialmente a atividades relacionadas com a aviação. Contudo esta aproximação é aplicável a qualquer atividade complexa que exija que os humanos estejam atentos e reajam a eventos (Endsley, 2000).

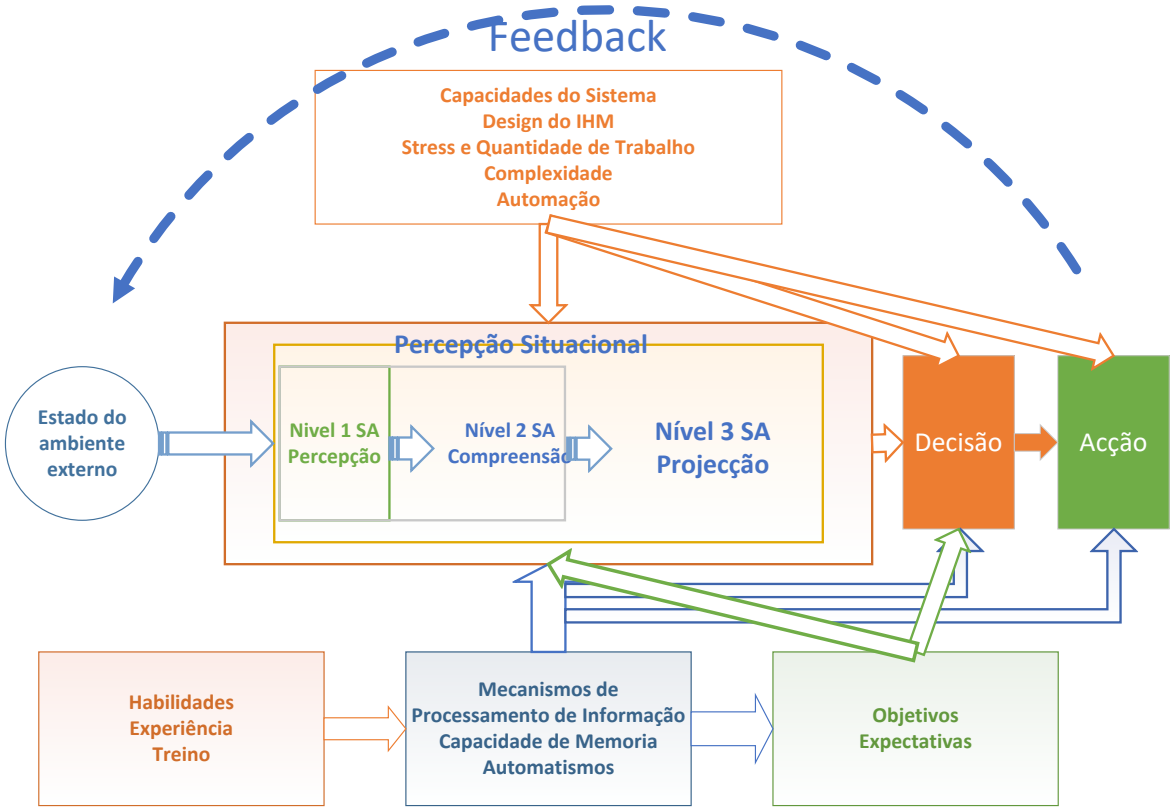


Ilustração 4- Atividades e processos de perceção situacional[32]

Este modelo é composto por três níveis hierárquicos de perceção situacional, sendo cada um dos níveis necessário, mas não suficiente para suportar o nível seguinte, hierarquicamente superior. O modelo identifica atividades de processamento de informação que vão desde a perceção, passando pela interpretação e terminando na predição tal como observável na ilustração seguinte.

Associados a cada um destes níveis estão um conjunto proposto de critérios de desenho da interface com o utilizador para permitir uma melhor perceção situacional, (Stanton, Chambers e Piggott, 2001), a saber:

i. Redução da necessidade de realização de cálculos pelo utilizador;
ii. Apresentação da informação por forma a facilitar a sua usabilidade nos níveis superiores, compreensão e predição;
iii. Organização da informação de acordo com os objetivos exigidos ao utilizador;

[32] Fonte: adaptado de Endsley, 2000

iv. Utilização de indicadores relativos ao estado presente da situação percecionada;
v. Utilização de alertas conspícuos para captar a atenção na sequência de eventos críticos;
vi. Representação da perceção situacional global relativa aos objetivos de cada utilizador;
vii. Geração pelo sistema da projeção de eventos e estados futuros;
viii. Sistema modular e apresentação de dados por fusão das diferentes fontes em vez de sequencialmente situação global

O problema com os sistemas atuais, e que se agravará no futuro, não é a falta de dados, mas sim encontrar a informação necessária em tempo útil e quando necessário. Existe uma lacuna entre a quantidade de dados produzidos e disponibilizados e a capacidade de os humanos encontrarem os dados necessários, correlacionarem os mesmos, integrarem e interpretarem-nos corretamente e produzirem a informação necessária ao processo de decisão (Endsley, 2000).

2.5. Gestão de risco

O processo de gestão de risco de segurança de informação está normalizado pela norma ISO27005, esquematicamente representado na figura seguinte. Esta gestão do risco relacionada com a segurança de informação, tem características comuns com as referidas anteriormente, ou seja, também tem que ser realizada num contexto *VUCA*, onde as questões de perceção situacional adquirem particular relevância, revelando-se assim como uma atividade complexa e difícil. O facto dessa mesma gestão ter de ser realizada numa rede de *stakeholders*[33]que partilham tecnologias comuns e, portanto, vulnerabilidades e riscos comuns e correlacionados, aumenta a complexidade e dificulta a atribuição de responsabilidades, algumas das quais podem estar ligadas aos processos de gestão de risco dos diferentes *stakeholders* nomeadamente às atividades e questões relacionadas com opções de mitigação do risco por transferência do mesmo sob a forma de seguros.

[33] Stakeholders – partes interessadas no processo ou negócio

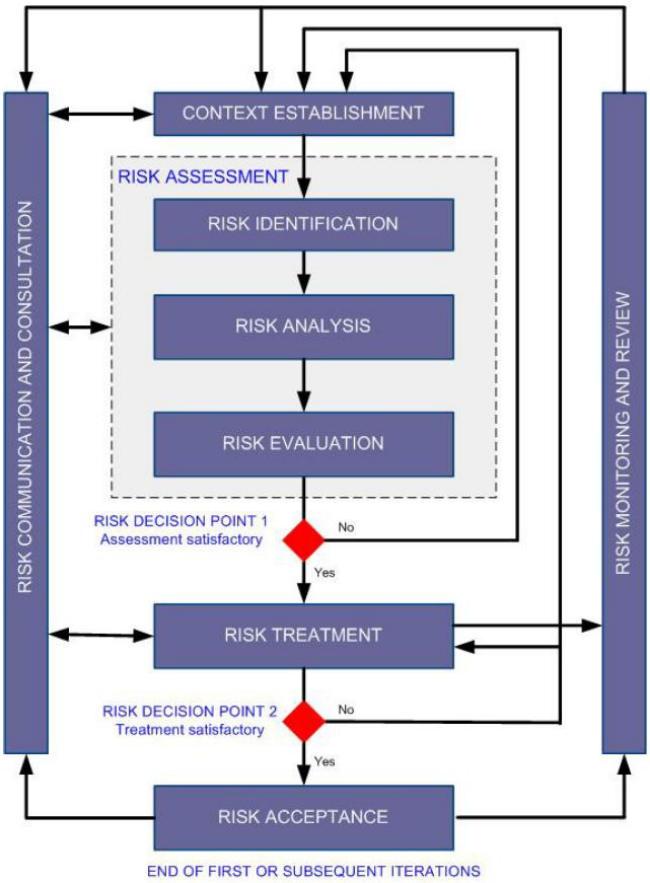


Ilustração 5- Processo de gestão de risco de acordo com (ISO/IEC 27005:2011, 2011)

Acresce que no caso vertente poderemos estar a falar de perdas tangíveis e intangíveis, como por exemplo, perdas reputacionais, de *goodwill*[34] e de *competitive intelligence*[35] sendo estas últimas de difícil quantificação. (Öğüt, Raghunathan e Menon, 2011)

A determinação do valor acrescentado para o negócio gerado pelo conjunto de serviços e produtos fornecidos e a estimativa de perdas em que se incorre pelo facto de os mesmos terem de ser fornecidos em modo degradado ou mesmo não poderem ser fornecidos num determinado período é crucial para a perceção do risco afeto a cada um destes ativos. A valorização dos ativos e das perdas originadas pelos mesmos e pelos processos de negócio em que estão envolvidos, e a correlação dos mesmos com os outros

[34] *Goodwill* – valor intangível de força atrativa de uma empresa capaz de acrescentar mais valias ao negócio, incluindo imagem corporativa, relações corporativas com fornecedores e clientes, qualidade percebida dos bens e serviços fornecidos, qualidade e conduta dos funcionários, normalmente construída ao longo do ciclo de vida da empresa.

[35] *Competitive Intelligence* – ações visando a obtenção, análise e distribuição de conhecimento sobre produtos, competidores e outros aspetos do negócio que alimentam os processo de suporte à decisão empresariais.

riscos do negócio é pois essencial para uma análise de risco holística e para uma avaliação de risco (Kosub, 2015)

2.5.1. Identificação de Riscos

A identificação dos riscos de segurança da informação afigura-se como uma atividade vital para a gestão dos ativos corporativos e desses mesmos riscos. Eles existem na organização nos três vetores associados à segurança de informação, os recursos humanos, os processos de negócio e a infraestrutura tecnológica que os suporta. Importa assim identificar para cada um destes ativos corporativos qual o seu valor para o negócio e as vulnerabilidades e consequentemente o risco a que os mesmos estão expostos (ISO/IEC 27005:2011, 2011).

A avaliação da exposição aos riscos de segurança da informação implica, a existência de processos proactivos que permitam uma contínua identificação, avaliação, controle e monitoria do estado e das vulnerabilidades de cada um e de todos os ativos corporativos. Considerando que estes mesmos riscos decorrem das vulnerabilidades existentes em cada um dos ativos corporativos que compõem os diferentes processos e serviços (Kosub, 2015) e que portanto constituem a superfície de ataque exposta pela organização em cada instante.

Considerando que a exposição ao risco pressupõe em primeira instância a existência de uma vulnerabilidade e de uma ameaça que explore essa particular vulnerabilidade (ISO/IEC 27005:2011, 2011) a identificação dos riscos implicará a identificação de todas as vulnerabilidades e do impacto que a exploração das mesmas pode vir a ter relativamente a todos os ativos corporativos.

Acresce como referido anteriormente que esta superfície de ataque muda com frequência e está frequentemente a ser alimentada com novas vulnerabilidades.

Importa, ainda e também, nesta análise considerar os controlos implementados nos diferentes níveis, pessoas, processos e tecnologia e que devem decorrer dos seus objetivos de segurança e dos níveis de risco (*risk appetite* e *risk objective*) cuja gestão deve contribuir para a redução da referida exposição e controlo do risco dentro dos limites definidos pela gestão de topo(Kosub, 2015).

2.5.2. Avaliação e Valoração dos Riscos

As normas (ISO/IEC 27001:2013, 2013) e (ISO/IEC 27005:2011, 2011) determinam a avaliação das perdas e das probabilidades do impacto gerados pela exposição aos diferentes riscos. Este processo implica a identificação das vulnerabilidades e riscos associados existentes em cada instante, a probabilidade de sucesso decorrentes de um ataque que explore as referidas vulnerabilidades e as consequências para a organização do referido ataque, permitindo obter uma matriz de risco.

Esta será depois avaliada em função dos objetivos de risco permitindo determinar quais os riscos aceitáveis e quais aqueles que por não serem aceitáveis devem ser objeto de tratamento. A ilustração seguinte mostra uma possível matriz de avaliação decorrente do exposto.

Table E.1 a)

	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Ilustração 6- Exemplo de Matriz de avaliação de risco (ISO/IEC 27005:2011, 2011)

A avaliação do impacto decorrente de um ataque bem-sucedido deverá considerar as perdas tangíveis (indisponibilidade do serviço, tempo, recursos e esforço para a reposição do mesmo em condições normais de operação) e as intangíveis (reputacionais, impacto nos clientes, etc.) (Kosub, 2015).

Esta análise é normalmente realizada considerando graus ou níveis de impacto expectáveis ou percecionados pela organização e a definição de quais os níveis aceitáveis, toleráveis e intoleráveis para a mesma, resultando numa aproximação similar à da ilustração seguinte(CANSO, 2014)..

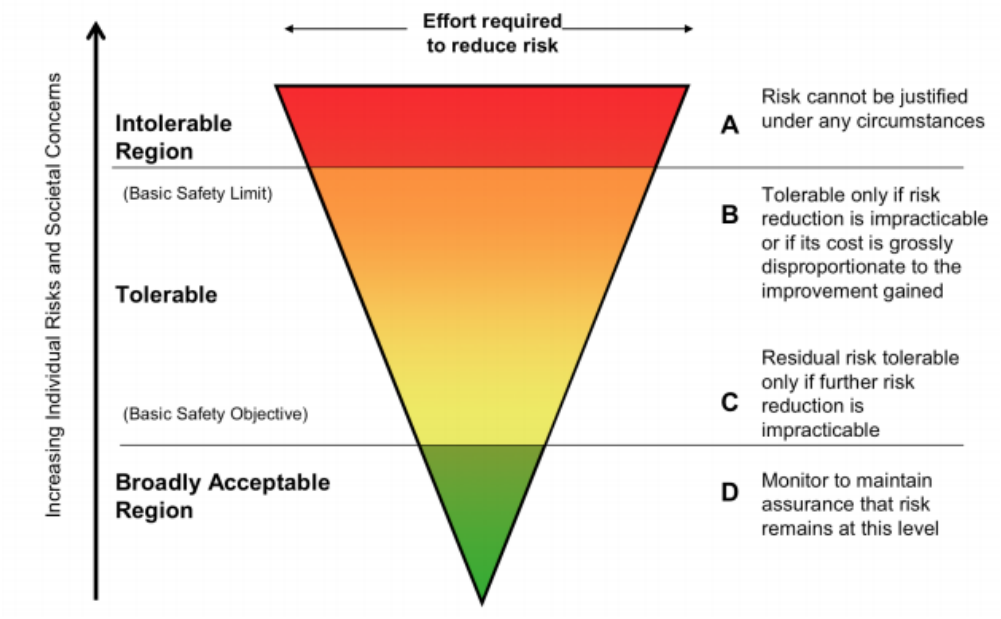


Ilustração 7- Impacto e níveis de aceitabilidade de risco de acordo com (CANSO, 2014)

Podemos assim afirmar que, neste caso a região de risco tolerável determinará os objetivos de risco para um determinado ativo ou serviço: *risk objective*, o mais baixo e *risk appetite*, o mais alto.

A avaliação do risco necessita também de uma normalização dos diferentes parâmetros de avaliação para facilitar as operações e a perceção do mesmo, pelo que se deverão procura usar métricas consistentes ao longo de todo o processo de avaliação, isto é atribuir os valores mais baixos às situações onde o risco ou impacto é menor e os mais altos onde aqueles são potencialmente maiores.

Para normalizar a avaliação nos diferentes vetores em que a mesma vai ser realizada, e no âmbito do presente trabalho, definiu-se a grelha de níveis, qualitativos, quantitativos e respetiva normalização (Ilustração 8) que será utilizada no presente trabalho.

Nível de risco/ Impacto	Quant.	Qual.	Indisp. (horas)	Vuln. Score (Quant.)	Vuln. Score (Qual.)	Impacto (Quant.)
Mto.Alto	**5**	**vHigh**	**<=2**	**>7.5**	**High**	**>7.5**
Alto	**4**	**High**	**<=4**	**>6**		**>6**
Médio	**3**	**med**	**<=6**	**>5**	**Med**	**>5**
Baixo	**2**	**low**	**<=12**	**>2,5**		**>2,5**
Mto. Baixo	**1**	**vlow**	**<=24**	**<2,5**	**Low/None**	**<2,5**

Ilustração 8- Tabela de normalização dos níveis qualitativos e quantitativos a utilizar no âmbito do presente trabalho.

Utilizando os valores utilizados e publicados por diferentes entidades (por ex. a atribuição dos scores realizada pelo sistema CVSSv3 utiliza valores entre 0 e 10 para os diferentes níveis atribuídos aos vetores das vulnerabilidades e *High*, *Low*, *None* para impactos nas componentes CIA da segurança da informação) pareceu necessário normalizar esses mesmos valores, com outros existentes e utilizados frequentemente (por ex. os processos de avaliação de risco consideram normalmente valores entre um e cinco) e com aqueles que foi necessário definir no âmbito do presente trabalho.

2.5.3. Resposta ao Risco

Considerando os resultados decorrentes da avaliação de risco, é necessário identificar que medidas de tratamento do mesmo devem ser aplicadas. A norma (ISO/IEC 27001:2013, 2013) identifica um conjunto de controlos, objetivos e medidas que podem ser aplicados para mitigar os riscos identificados.

As opções para o tratamento do risco de acordo com (ISO/IEC 27001:2013, 2013) são: a modificação, a retenção, a evasão e a partilha. Como corolário da aplicação destas medidas de tratamento e considerando que o risco nulo não será possível de atingir de forma prática e economicamente viável, podemos afirmar que o objetivo do tratamento será o de obter um valor de risco pós tratamento, ou se quisermos um risco residual que deverá estar abaixo do *risk appetite* da organização.

A ilustração seguinte pretende representar a forma como foi implementado o processo de gestão de risco e de vulnerabilidades no contexto da presente investigação.

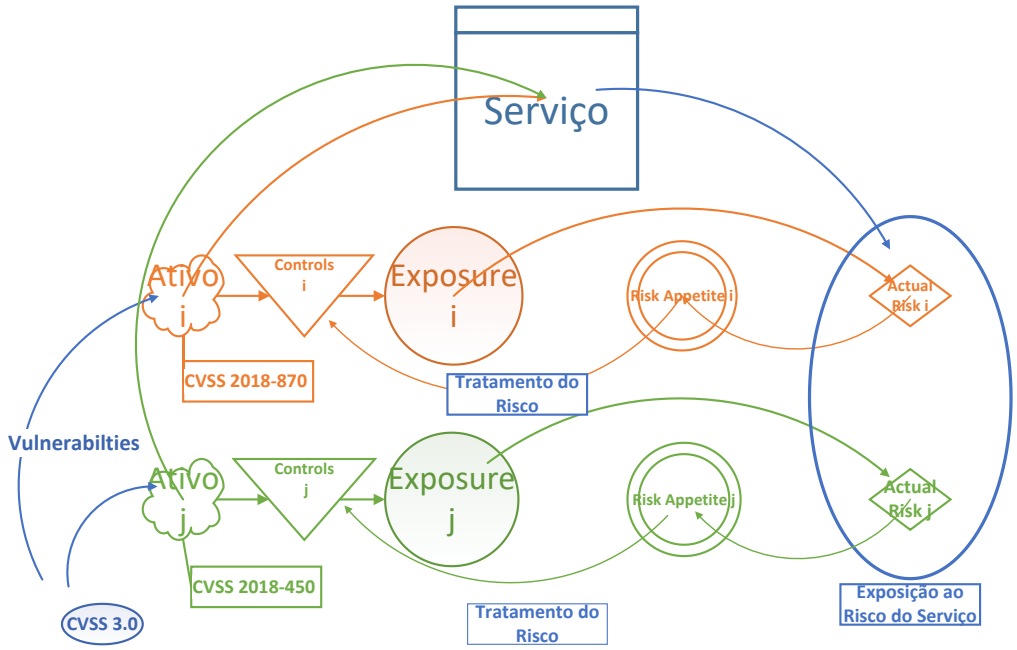


Ilustração 9- Modelo de gestão de risco.

2.5.4. Análise do Impacto no Negócio[36] (BIA)

Se o risco associado a um determinado ataque depende do tipo e da sofisticação do ataque ele também depende da capacidade de resistir a esse mesmo ataque por parte da organização. Esta capacidade é definida como a capacidade de se preparar e planear para absorver, recuperar e se adaptar a estas circunstâncias adversas ou resiliência da organização (CISSP, 2012)

A resiliência normalmente incorpora os seguintes domínios: o domínio físico (*hardware, software* e outros ativos da infraestrutura tecnológica), o domínio da informação (dados e informação e todos os processos relacionados com a aquisição, a transmissão, o acesso, processamento, armazenamento e destruição desses dados ou informação e a respetiva visualização ou apresentação) o domínio cognitivo (análise da informação e sistema e processos de suporte à decisão) e o domínio social (recursos humanos, considerações éticas e sociais relevantes para o negócio)

A análise do impacto no negócio visa identificar, para cada área de negócio ou serviço disponibilizado, as funções, serviços e os ativos que suportam essas mesmas

[36] Análise do Impacto no Negócio/BIA – Business Impact Analysis

funções ou serviços, identificar a sua criticidade e medir o impacto que ocorreria no negócio em caso de disrupção dos respetivos ativos ou serviço.

Esta análise é feita considerando este impacto em primeiro lugar em cada um dos serviços ou ativos e posteriormente nas diferentes áreas do negócio (*KPA´s- Key Performance Areas*) desde o impacto na tecnologia, nos diferentes serviços prestados e que suportam o normal funcionamento da empresa, até ao impacto em questões legais ou regulatórias, nos recursos humanos e ou na reputação da organização. Em sectores específicos e nomeadamente em sectores críticos as diferentes KPA´s podem ter que incluir áreas impostas pela regulação do negócio.

Outro dos objetivos da análise de impacto no negócio é determinar os objetivos de recuperação para cada ativo ou serviço, a saber o MTO (*Maximum Tolerable Outage* – ou o tempo máximo que um serviço ou ativo pode estar indisponível) o RTO (*Recovery Time Objective*- ou o tempo de recuperação pretendido para um determinado serviço ou ativo) e o RPO (*Recovery Point Objective* – ou o tempo passado para o qual a recuperação dos dados ou informação tem que ser realizada)

Os planos de continuidade de negócio (*BC-Business Continuity*) e de recuperação de desastres (*DR- Disaster Recovery*) resultam dos mesmos processos de decisão saídos da condução das análises de impacto no negócio (CISSP, 2012) e são estes processos, a montante, que terão que ser acionados quando a resposta corporativa a um incidente de segurança de informação, no caso presente, não puder ser contida pelos procedimentos operacionais implementados nos *SOC´s* (Security *Operations Centres)*, ou quando o processo de decisão em sede de gestão de crises decidir acionar a escalada para um destes procedimentos.

Os três passos deste processo de acordo com (ISO/IEC 27001:2013, 2013) são:

1. Identificar os recursos de TI críticos;
2. Identificar os impactos provocados por uma disrupção e objetivos temporais (RTO, MTO, RPO);
3. Desenvolver prioridades de recuperação

Estes três passos são comparáveis com os propostos pela norma, *British Standard* BS25999 de acordo com (CISSP, 2012)

2.6. Redes Neuronais

A implementação de Sistemas de Apoio à Decisão, a complexidade associada aos mesmos e similitudes com a forma como o cérebro humano processa e usa a informação parecem fazer das redes neuronais uma das tecnologias mais promissoras para suportar a respetiva implementação.

2.6.1. Conceitos gerais

Inspirados pelo modo como o cérebro processa informação, McCulloch e Pitts desenvolveram em 1943, um modelo matemático capaz de obter conhecimento sobre o que conseguem fazer as redes de unidades simples através da aprendizagem por exemplos (Russell & Norvig, 2009).

As redes neuronais representam conjuntos de neurónios (nós), sendo estes constituídos por: várias camadas, a camada de entrada, uma camada escondida e uma ligação de saída, pesos atribuídos aos valores de entrada que podem ser adaptados durante o processo de aprendizagem, denominada ligação de entrada, o nó da rede propriamente dita que representa um somatório e finalmente uma função de ativação que produz uma decisão com base num critério enviando a resposta para a ligação de saída (Russell & Norvig, 2009), como pode ser observado na ilustração seguinte.

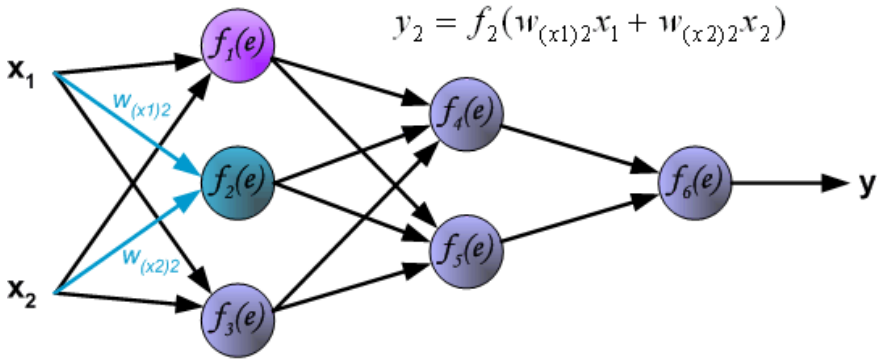


Ilustração 10- Representação de uma rede neuronal (fonte:TeX Stack Exchange).

Os valores de entrada de uma rede neuronal são sujeitos a estímulos (pesos positivos), ou a fatores inibidores (pesos negativos), sendo posteriormente alvo de uma soma ponderada - cujos resultados, por aplicação da função de ativação, atingem um dado limiar, proporcionando uma saída de valor 0 ou 1. É importante que a função de ativação

seja uma função não-linear, para evitar que a saída se concretize precisamente numa combinação linear das entradas. Estas são habitualmente funções sigmoides, tangentes hiperbólicas, função seno, logarítmica ou função degrau ou limiar, sendo estas funções diferenciáveis e de diferentes contradomínios (Cruz, 2008).

Os tipos mais comuns de redes neuronais são as redes alimentadas para a frente e as redes retro propagadas. As redes alimentadas para a frente subdividem-se em redes mono camada de perceptores e redes multicamada de neurónios. Este tipo de redes implementa funções, não possuindo estado interno. As redes neuronais recorrentes ou retro propagadas são, por exemplo as redes de *Hopfield* cujos pesos são simétricos e as máquinas de *Boltzmann* que utilizam funções de ativação estocásticas. Este tipo de rede sofre de introdução de atrasos nos ciclos dirigidos (Cruz, 2008).

As redes neuronais permitem vários tipos de utilização: modo de treino, modo de generalização e modo de inovação (Borges, 2015). No primeiro modo, os neurónios são treinados para responder a determinados padrões, sendo isto possível através da adaptação dos pesos atribuídos a cada entrada, com o objetivo de obter uma determinada resposta previamente fornecida. Neste modo, a aprendizagem converge para uma função consistente, para qualquer conjunto de dados linearmente separável. O modo de generalização permite produzir um valor de saída mesmo que os valores de entrada sejam vagos ou incompletos. No modo inovação, são produzidas novas relações entre as entradas e as saídas com resultados distintos dos utilizados no treino.

Segundo (Borges, 2015), o prolongamento da aprendizagem leva habitualmente a um problema de sobre ajustamento, caracterizado por uma boa classificação do conjunto de treino, mas uma deficiente avaliação do conjunto de validação. Um número reduzido de nós escondidos poderá impossibilitar a aprendizagem da função. Os exemplos de treino devem compreender todos os aspetos significativos do conjunto de chegada.

O número de observações de treino, se for reduzido, poderá restringir a capacidade de generalização, por outro lado, se for em excesso poderá causar sobre ajustamento. Como regra prática, poder-se-á calcular o número de exemplos como sendo entre 5 e 10 vezes o número dos pesos e que para classificar um treino de rede com precisão *1-e*, são necessários o mesmo número de exemplos de treino e de pesos, divididos por *e* (Cruz, 2008).

Um dos métodos utilizados para a calibração dos modelos é o método *early stopping*. Nesta técnica os dados disponíveis são divididos em três partes, sendo a primeira, que geralmente reúne cerca de 70% dos dados disponíveis, utilizada para o treino da rede e as restantes duas partes iguais (15%) respetivamente para a validação e teste do modelo.

Estas percentagens podem ser ajustadas com o objetivo de tornar o treino da rede mais eficiente e evitar o *overfit* da mesma.

O treino da rede consiste no cálculo do gradiente e na atualização dos pesos e polarizações da mesma. O segundo conjunto de dados permite fazer a validação da rede. O erro medido com o conjunto de validação é monitorizado durante o processo de treino e normalmente decresce na fase inicial de treino tal como o erro do conjunto de teste.

Contudo quando a rede começa a ficar *overfitted*, o erro no conjunto de validação tipicamente começa a aumentar e quando este aumento se manifesta durante um número específico (parametrizável) de iterações, o treino da rede é parado e são considerados os valores dos pesos e enviesamento obtidos aquando do erro de validação mínimo.

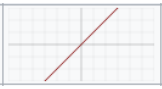
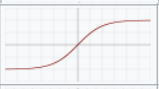
O conjunto de dados de teste não é utilizado durante o treino, mas é utilizado para comparar diferentes modelos e para o cálculo do erro do conjunto de dados de teste. Se o erro do conjunto de dados de teste atingir um mínimo ao longo do processo de teste numa interação significativamente diferente daquela em que o conjunto de validação também atinge um mínimo isso poderá significar que o conjunto de dados não estará corretamente dividido em termos de representatividade entre os diferentes conjuntos.

2.6.2. Funções de Ativação

As funções de ativação ou funções de transferência definem o valor de saída de um determinado nó face ao valor ou valores de entrada desse mesmo nó. Permitem a introdução de uma componente não linear nas redes neuronais, permitindo que estas adquiram capacidades de aprendizagem para alem daquelas que são inferidas das relações lineares entre as variáveis dependentes e independentes. Algumas funções de ativação, as não lineares, contribuem para acelerar a aprendizagem das redes neuronais. Podemos afirmar que uma rede neuronal sem função de ativação é um modelo de regressão linear.

Existem várias funções de ativação, de que referiremos seguida e brevemente apenas aquelas disponíveis na *framework Orange (usada na implementação do modelo e descrita na secção 5.5)*, ou sejam as funções *identity, logistic, tanh e ReLu.*

Os gráficos seguintes representam estas funções.

Identity		$f(x) = x$	$f'(x) = 1$	$(-\infty, \infty)$
Logistic (a.k.a. Sigmoid or Soft step)		$f(x) = \sigma(x) = \frac{1}{1+e^{-x}}$ [1]	$f'(x) = f(x)(1-f(x))$	$(0, 1)$
TanH		$f(x) = \tanh(x) = \frac{(e^{x} - e^{-x})}{(e^{x} + e^{-x})}$	$f'(x) = 1 - f(x)^2$	$(-1, 1)$
Rectified linear unit (ReLU)[15]		$f(x) = \begin{cases} 0 & \text{for } x < 0 \\ x & \text{for } x \geq 0 \end{cases}$	$f'(x) = \begin{cases} 0 & \text{for } x < 0 \\ 1 & \text{for } x \geq 0 \end{cases}$	$[0, \infty)$
Leaky rectified linear unit (Leaky ReLU)[16]		$f(x) = \begin{cases} 0.01x & \text{for } x < 0 \\ x & \text{for } x \geq 0 \end{cases}$	$f'(x) = \begin{cases} 0.01 & \text{for } x < 0 \\ 1 & \text{for } x \geq 0 \end{cases}$	$(-\infty, \infty)$

As funções de ativação não lineares permitem dar capacidades representativas às redes neuronais, embora tornem a otimização mais complicada uma vez que como consequência fazem com que a superfície de custo se torne não convexa.

A função de ativação tangente hiperbólica (*tanh*), tem, como a função sigmoide um formato em "S", com a diferença que varia entre os valores -1 e 1, ao contrário de 0 e 1 naquela, o que a aproxima mais da função identidade pelo que é mais atrativa do que a função sigmoide como ativadora para as camadas ocultas das redes neuronais, pelo que a sua utilização é recomendada quando se pretendem usar funções de ativação sigmoides.

A função *ReLU*, ativação linear retificada, também conhecida como função rampa, permite uma otimização simples, sendo parecida com a função identidade, com a exceção em que a saída da função é zero para valores negativos do domínio. A sua ativação é mais eficiente do que as funções sigmoidais referidas anteriormente e a sua utilização é apontada como um contributo para a popularização da aprendizagem em profundidade. Uma das suas desvantagens está relacionada com o efeito absorvente, que ocorre quando a soma ponderada antes da aplicação da *ReLU* é negativa provocando uma saída zero, o que, como nessa região a respetiva derivada tem também o valor zero, tem como consequência que os parâmetros desse nó deixem de ser atualizados com gradientes descendentes. Para obviar a este inconveniente foi criada a função *LeakyReLU*, que se aproxima mais da função identidade na região negativa permitindo obviar aos efeitos da *ReLU* nessa zona (Goodfellow, Bengio e Courville, 2013).

2.6.3. Classificação de dados

Classificação é uma forma de análise de dados que permite a extração de modelos, denominados classificadores, que descrevem classes de dados, e que permitem a predição de categorias discretas e não ordenadas de dados. Foram propostos diversos métodos de classificadores para o reconhecimento de padrões e estatísticas, na sua maioria utilizando algoritmos residentes em memória e assumindo conjuntos de dados não muito grandes. Recentemente as técnicas de *data mining* evoluíram para técnicas de predição e classificação escaláveis, ou seja com capacidade para processarem maiores quantidades de dados, e para domínios de aplicação como a deteção de fraudes, marketing personalizado, predição de performance e diagnóstico médico (Han, Kamber e Pei, 2011), e para a classificação da informação, quer para evitar o seu acesso indevido, quer para evitar a sua disponibilização, comprometendo a segurança da mesma e por essa via expondo o negócio a riscos acrescidos (Gai, Qiu e Elnagdy, 2016).

A classificação é um processo que é composto por dois passos, onde no primeiro se constrói um modelo de classificação (fase de aprendizagem), utilizando dados existentes, e num segundo passo, se avalia a precisão desse mesmo modelo e sendo essa precisão considerada aceitável se utiliza o mesmo para a classificação de novos dados (fase de classificação) (Han, Kamber e Pei, 2011)

Para avaliar a precisão do modelo de classificação podem usar-se diversas métricas como por exemplo a curva ROC (*Receiver Operating Characteristic Curve*) representação gráfica da performance do modelo de classificação no domínio de todos os níveis críticos de classificação, a taxa de verdadeiros positivos (TPR) e a taxa de falsos positivos (FPR).

2.6.4. Algoritmos de Resolução

A *framework Orange* dispõe de algoritmos mais eficientes que o original BFGS(*Broyden–Fletcher–Goldfarb–Shanno*), que pode ser considerado como uma aproximação ao método de Newton, para a classificação de palavras ou frases e para aproximações hibridas, na deteção de sentimentos associados a frases, que implicam uma primeira classificação das frase em tipologias e uma posterior análise do sentimento (Chen et al., 2017).

Estão disponíveis os seguintes algoritmos de resolução, L-BFGS-B, SGD e Adam. O algoritmo L-BFGS-B é essencialmente o mesmo algoritmo que o BFGS, utilizando recursos limitados da memória das máquinas utilizadas na resolução e incorporando *box constraints*, significando este último termo que para cada variável podem ser atribuídos um limite mínimo e máximo. São algoritmos mais eficientes que o original BFGS, utilizados em classificação de palavras ou frases e em aproximações hibridas, na deteção de sentimentos associados a frases, que implicam uma primeira classificação das frase em tipologias e uma posterior análise do sentimento (Chen et al., 2017)

SGD (*Stochastic gradient descent)* é um algoritmo utilizado em diversos modelos de *machine leaning* entre os quais *SVM-Support vector machines* e regressão logística. Este algoritmo é muitas vezes combinado com o algoritmo *backpropagation*, e considerado um *standard* para treino de redes neuronais.

Adam (*Adatative Moment Estimator*) é um algoritmo, criado a partir duma otimização do RMSProp (*Root Mean Square Propagation*). Trata-se de um algoritmo baseado em otimização de funções estocásticas baseado em estimativas adaptadas de momentos de baixa ordem. Reclamado como de fácil implementação, eficiente do ponto de vista da computação, com necessidades muito pequenas de memória e especialmente eficiente em problemas com muitos dados ou parâmetros (Kingma e Lei Ba, 2013).

2.6.5. Random forest

Random Forest é um algoritmo de aprendizagem supervisionada, baseado em árvores de decisão treinadas utilizando o método de *bagging*, que consiste numa combinação de modelos de aprendizagem, com a convicção de que através desta combinação de diferentes modelos de aprendizagem se consigam obter predições mais estáveis e mais precisas.

A sua maior vantagem é que pode ser utilizada quer para problemas de classificação quer de regressão. Outra das suas vantagens é que, ao contrário das árvores de decisão que tendem a sofrer de *overfitting*, previne este problema através da criação de *subsets* aleatórios das caraterísticas com os quais constrói "arvores" mais pequenas, que depois combina.

É também considerado um algoritmo um algoritmo facilmente utilizável porque mesmo com os parâmetros por omissão, que são em número limitado e fáceis de entender,

consegue apresentar boas predições. Trata-se de um algoritmo com uma complexidade de treino muito baixa e que devido à sua simplicidade permite obter com facilidade a importância das diferentes caraterísticas dos dados ao que acresce que pode ser usado em diferentes categorias de dados, como por exemplo dados binários, categorias ou numéricos. (Breiman, 2001)

2.6.6. Naive bayes

Naïve Bayes, também conhecido como *Simple Bayes*, é um algoritmo que usa o Teorema de *Bayes* para classificar objetos, assumindo uma independência forte entre os variáveis dos dados constituintes dos mesmos. Muito utilizados em *machine learning* devido ao facto de serem simples de implementar são utilizados em diversas aplicações populares como por exemplo filtros de spam e análise de texto.

Apesar da assunção de que os atributos são todos independentes possa não estar totalmente correta, este facto simplifica dramaticamente as tarefas de classificação, permitindo o cálculo separado para cada variável sem, contudo, afetar o resultado final, de forma relevante, principalmente nas proximidades dos limites de decisão, permitindo assim uma boa qualidade de classificações e de performance.

2.7. Lógica difusa (*Fuzzy Logic*)

A lógica difusa ganhou notoriedade na década de 60 do século passado pelo trabalho desenvolvido por Lofti A. Zadeh. Contrariamente à lógica clássica, cujos valores assumem valores discretos, isto é, valor 0 ou 1, a lógica difusa baseia-se em graus de pertença ou inclusão, ou seja, valores contínuos compreendidos no intervalo fechado onde $min(x) = 0$, significando que o elemento não pertence ao conjunto e $max(x) = 1$, que significa pertença total ao conjunto (Borges, 2015).

É uma forma conveniente de relacionar um espaço de entradas com um espaço de saídas. Assemelha-se ao pensamento humano, estando mais próxima da experiência quotidiana e permitindo a gestão de ambiguidades e falhas (Lobo, 2010). Permite ainda o aumento da precisão de soluções em sistemas complexos onde um modelo matemático é inexistente. Por outro lado, pode tornar-se imprecisa e de difícil gestão de interação entre diferentes condicionantes do problema proposto.

A sua utilização permite uma aproximação mais intuitiva para a resolução de problemas complexos, é flexível, tolerante a dados imprecisos, permite a modelação de funções não lineares de complexidade arbitraria e a partir de qualquer conjunto de dados, pode ser misturada com técnicas de controlo convencional e é baseada na linguagem natural.

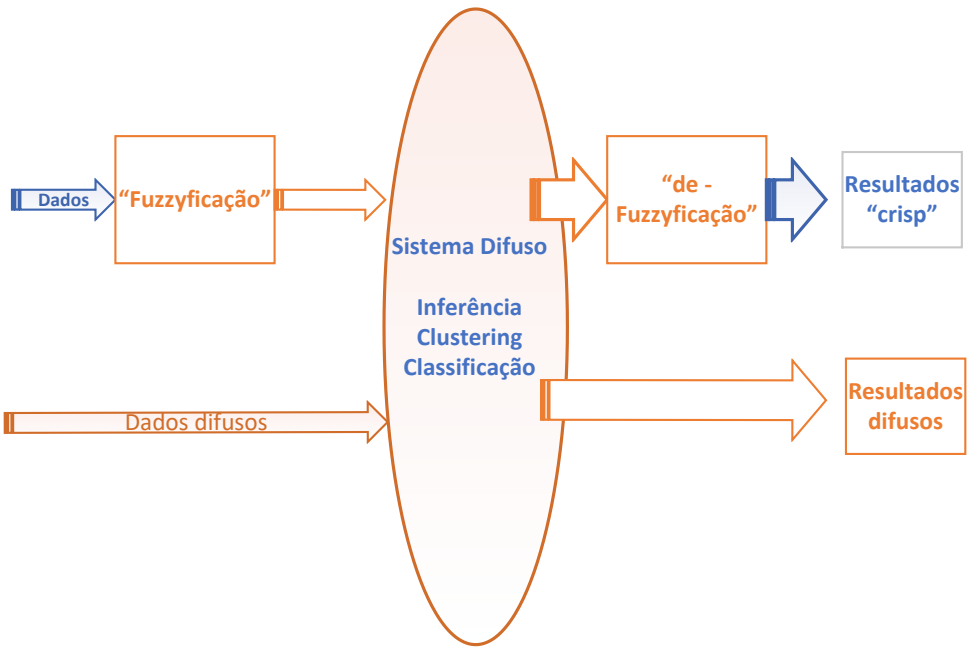


Ilustração 11- Arquitetura de sistemas de lógica difusa.

A lógica difusa começa pela definição de um *Fuzzy Set*, que é um conjunto sem uma fronteira claramente definida, um conjunto de elementos difusos, que podem conter cada um deles diferentes graus parciais de pertença a cada um dos conjuntos (*fuzzy sets*), num processo conhecido por fuzzificação.

2.7.1. Terminologia associada

Uma variável linguística é aquela cujos valores estão associados à linguagem natural. O conjunto desses valores denomina-se de conjunto de termos, ou Gama, e cada valor nesse conjunto é uma variável *fuzzy* definida sobre a variável base, isto é, sobre o universo de discurso (Borges, 2015).

A única condição a que uma função de pertença tem de obedecer é que tem que variar entre 0 e 1. A função poderá assim assumir qualquer forma arbitrária que torne mais fácil, mais eficiente ou mais rápido o seu processamento. Um conjunto clássico pode ser expresso da seguinte forma:

$$A = \{x | x > 5\}$$

Um conjunto *fuzzy* é uma extensão desse conjunto clássico. Se considerarmos X como o universo dos valores possíveis e os seus elementos representados por x, então um conjunto *fuzzy* A em X será definido por um conjunto de pares ordenados,

$$A = \{x, \mu_A(x) | x \epsilon X\}$$

Onde $\mu_A(x)$ é a função de pertença de x em A. Esta função atribui a cada elemento de X um valor da função pertença entre 0 e 1.

2.7.2. Operações em Lógica Difusa

É possível realizar um conjunto variado de operações sobre conjuntos *fuzzy* (Borges, 2015), tais como as operações definidas seguidamente e representadas na ilustração seguinte.

i. Intersecção: $\mu A \cap B\ (x) = \min\big(\mu A\ (x), \mu B\ (x)\big)$;
ii. Negação ou complemento: $\neg A\ (x)\ = 1 - \mu A\ (x)$;
iii. Reunião: $\mu A \cap B\ (x)\ = max\ (\mu A\ (x), \mu B\ (x))$

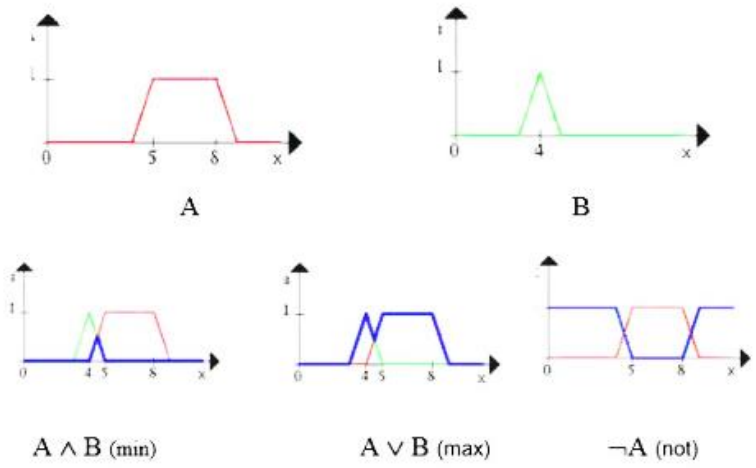


Ilustração 12- Operadores lógicos sobre conjuntos difusos.

A lógica difusa permite essencialmente resolver problemas de classificação, com principal foco no modo como determinado sistema deverá funcionar em detrimento da modelação do seu funcionamento. Assim, os conjuntos *fuzzy* assumem particular interesse em problemas de classificação de padrões ou no processamento de informação. (Zadeh, 1965), permitindo também implementar processos de resposta automatizada.

Estas caraterísticas da lógica difusa, têm vindo a ser reconhecidas como necessárias nos casos com especial complexidade, e onde tendo sido propostos diversos processos de medir a disponibilidade e integridade com recurso a medidas precisas, como por exemplo, o numero exato de ataques, eficiência dos mecanismos de controlo na proteção da disponibilidade e integridade ou o impacto financeiro de cada ataque em termos de disponibilidade e integridade, na exata medida em que mesmo estas medidas ditas precisas são muitas vezes incertas no mundo real (Tavana, Trevisani e Kennedy, 2015)

A incerteza pode ter duas fontes: a imprecisão ou a ambiguidade. A lógica de *fuzzy* e os conjuntos difusos que lhe estão associados conseguem representar estas duas variáveis de forma semelhante à que o humano utiliza, tornando a sua aplicação particularmente interessante neste tipo de problemas, tendo sido proposto para a avaliação de riscos de segurança da informação para os centros de comando e controlo dos militares americanos (Tavana, Trevisani e Kennedy, 2015)

2.8. Exploração e Visualização de Dados

A exploração e visualização de dados, especialmente nos casos em que esses mesmos dados são em quantidade apreciável, deve ter como objetivo permitir que os seus últimos consumidores, os seres humanos, consigam apreender a informação critica que os dados que a suportam podem transmitir.

O ser humano percebe e compreende com muito maior facilidade gráficos ou imagens do que letras ou números, e também interpreta muito mais facilmente a informação se a mesma for apresentada de uma forma gráfica. O objetivo da componente de visualização dos dados é pois o de transmitir a informação pertinente de um conjunto de dados, o de permitir que o humano percecione o conhecimento que esses mesmos dados contêm, e também a melhor forma de extrair, de preferência de forma autónoma e automática, o conhecimento que aqueles encerram.

A análise dos dados pode dividir-se em duas fases, ou categorias e vários processos em cada uma delas: Análise Exploratória dos Dados[37] e Análise Qualitativa dos Dados[38] (Alazmi e Alazmi, 2012).

Os processos de análise exploratória de dados iniciam-se normalmente pela respetiva classificação. A classificação de dados consiste na divisão e catalogação dos dados em vários tipos, formas ou classes e na determinação da função que permita essa mesma classificação.

Na fase seguinte, a regressão, procura-se determinar a função que permite relacionar um item dos dados com uma variável que permita a predição do valor desse mesmo item. Esta predição é tendencialmente tanto mais precisa quanto maior for a correlação entre as variáveis utilizadas (Fayyad, Piatetsky-Shapiro e Smyth, 1996).

O processo de Clustering consiste em identificar um conjunto finito de categorias que permitam descrever os dados a processar e identificar as diferentes relações e interdependências entre essas mesmas categorias as quais podem ter diferentes relações e interdependências de âmbito, mutuamente exclusivas e exaustivas, ou hierárquicas permitindo por exemplo identificar populações específicas, no conjunto de dados a analisar.

Outra fase consiste na estimativa da probabilidade da densidade, a qual visa determinar a função conjunta de densidade de probabilidade de um conjunto parcial de

[37] Análise Exploratória dos Dados / Exploratory Data Analysis
[38] Análise Qualitativa dos Dados / Qualitative Data Análisys

variáveis, extraído do conjunto total de variáveis dos dados em análise ((Fayyad, Piatetsky-Shapiro e Smyth, 1996)).

Segue-se o processo que permite identificar características especificas de um dos subconjuntos de dados, a sumarização, que envolve métodos como a determinação da média (*mean*) e do desvio padrão (*std*) dos diferentes dados de forma a permitir identificar uma descrição precisa característica de um dos subconjuntos dos dados.

Com a modelação de dependências, procura-se identificar um modelo que descreva importantes dependências entre as variáveis e determinar a intensidade dessa mesma dependência de forma quantitativa.

Importa ainda e por fim determinar alterações e desvios que o conjunto de dados possa apresentar relativamente a dados ou conjuntos de dados anteriores (Fayyad, Piatetsky-Shapiro e Smyth, 1996).

2.9. Sumário

Este capítulo apresentou uma revisão da literatura relevante para o problema tratado e para a solução proposta nomeadamente abordando as questões relacionadas com as temáticas e contextos operativos da segurança da informação em ambiente empresarial, gestão do risco e as diferentes metodologias e algoritmos capazes de ajudar a construir a solução pretendida de suporte à decisão.

Capítulo 3
Metodologia

Neste capítulo apresenta-se a metodologia seguida para a realização do trabalho partindo da questão de investigação.

3.1. Questão de investigação

Será possível basear um sistema de suporte à decisão de segurança de informação (*SecOPS*) na gestão das vulnerabilidades e do risco?

3.2. Análise da Informação

As questões derivadas que se seguem serão consideradas quando se proceder ao tratamento dos dados e implementação das metodologias e dos processos que permitam a implementação do sistema de suporte à decisão:

QD1. Será possível obter uma perceção situacional do estado da segurança de um sistema de informação através da sua superfície de ataque e do risco associado aos respetivos ativos?

QD2. De que forma será possível adquirir e manter a superioridade de informação relativamente aos ativos corporativos utilizando um SAD?

QD3. De que forma será possível obter uma perceção situacional da superfície de ataque exposta em cada momento?

QD4. De que forma será possível obter uma perceção situacional da exposição ao risco em cada momento?

QD5. Como minimizar a incerteza relativamente à superfície de ataque exposta em cada momento?

QD6. Como minimizar a incerteza relativamente ao risco em cada momento?

QD7. De que forma poderá ser apresentada a informação relativa a um determinado ativo relativamente à superfície de ataque exposta e ao risco inerente?

QD8. De que forma poderá ser apresentada a informação para que o processo de decisão possa ser eficiente?

3.3. Hipóteses

Para cada uma das questões derivadas formulou-se a respetiva hipótese de trabalho:

H1. Se a superfície de ataque e o risco associado aos ativos corporativos constituem os elementos de suporte ao processo de decisão de um sistema de segurança de informação, de que forma se pode materializar essa perceção situacional?

H2. Se a superioridade de informação no contexto deste SAD depende das vulnerabilidades e risco existentes num determinado momento como conseguir que essa mesma superioridade se mantenha?

H3. Se a perceção situacional da superfície de ataque em cada momento é um elemento decisivo no processo de tomada de decisão de que forma a mesma deverá ser atualizada e disponibilizada?

H4. Se a perceção situacional da exposição ao risco em cada momento é um elemento decisivo no processo de tomada de decisão de que forma a mesma deverá ser atualizada e disponibilizada?

H5. Se a superfície de ataque em cada momento é função das vulnerabilidades que métodos de redução de incerteza relativamente aquela podem ser utilizados?

H6. Se o nível de exposição ao risco em cada momento é função da superfície de ataque e esta das vulnerabilidades, que métodos de redução de incerteza relativamente àquele podem ser utilizados?

H7. Se se pretender apresentar a informação da superfície de ataque e exposição ao risco de um determinado ativo de que forma deverá a mesma ser apresentada por forma a poder suportar de forma efetiva o processo de decisão?

H8. Se o processo de decisão depende da informação disponível, mas também considerando a quantidade e complexidade da mesma, da forma conspícua como aquela é apresentada ao decisor de que forma poderá isso ser feito?

3.4. Recolha de Informação

O presente trabalho utilizará um conjunto de dados disponibilizados pelo Laboratório Nacional de Los Alamos[39], que compreende 58 dias consecutivos de eventos de dados coligidos de cinco fontes da rede interna daquele laboratório. As fontes de dados incluem eventos de autenticação em plataformas *Windows,* em computadores individuais, servidores e nos controladores do domínio AD (*Active Directory*) (auth.txt), no DNS (*Domain Name Service*) (dns.txt), eventos na rede recolhidos em diversos *routers* da infraestrutura (flows.txt) e um conjunto de eventos de comprometimento da infraestrutura gerados por uma *RedTeam*[40] (redteam.txt). Os referidos dados estão anonimizados e totalizam cerca de 1,6 milhões de eventos, gerados por 12 mil utilizadores em 18 mil computadores e 63 mil processos e estão referidos no tempo à *time epoch 1* com uma resolução de 1 segundo.

Cada ficheiro está disponível numa sintaxe própria. Cada evento está apresentado numa linha, contendo informação sobre o utilizador e o domínio que originou a transação, o utilizador e o domínio destinatários da transação, o computador de origem, o computador de destino, o tipo de autenticação e o estado resultante da mesma. Estão também disponíveis os processos e os utilizadores associados ao mesmo, bem como o estado do processo.

A título de exemplo, apresentam-se dados de eventos disponíveis.

"1, C653$@DOM1,SYSTEM@C653,C653,C653,Negotiate,Service,LogOn,Success"

"1, C553$@DOM1,C553,P25,End"

"1,9, C3090,N10471,C3420,N46,6,3,144"

Como se pode observar no primeiro dos eventos disponíveis, que se inicia com as aspas e que tem os dados do evento separados por virgulas, trata-se de um evento com *timestamp* 1, originado pelo utilizador C653, autenticado no domínio DOM1, com uma transação de sistema originada no computador C653, tendo como origem o computador

[39] A. D. Kent, "Comprehensive, Multi-Source Cybersecurity Events," Los Alamos National Laboratory, http://dx.doi.org/10.17021/1179829, 2015.

[39] *RedTeam*- Equipas de segurança de informação de uma organização que desempenham o papel de atacantes, com o objetivo de detetar falhas nos recursos humanos, processo e tecnologia que a suportam. Por oposição os defensores são designados por *BlueTeam.*

C653, como destino o computador C653, uma transação de negociação, dum serviço de *LogOn*, que teve como resultado o sucesso.

3.5. Dados adicionais

A caraterização do cenário será complementada com dois conjuntos de dados adicionais. Um desses conjuntos contém as vulnerabilidades presentes ou detetadas na infraestrutura num determinado instante temporal (cvss.csv), gerado a partir das últimas cem vulnerabilidades declaradas em https://cve.mitre.org/, nos seus três vetores de métricas, *base score*

$$\vec{V}_{bs},$$

temporal score

$$\vec{V}_{ts},$$

e *environmental score*

$$\vec{V}_{es},$$

Quando disponíveis e passíveis de atribuição a computadores do cenário, sendo que como já referido, na generalidade dos casos os segundos vetores, *temporal* e *environmental* não estão disponíveis, devendo ser calculados pelo organização que possui o sistema em causa uma vez que, o primeiro destes, depende do tempo em que a vulnerabilidade, foi detetada ou existe, no sistema a analisar e o segundo depende da arquitetura e configuração na qual o *host* que detém a vulnerabilidade está instalado. Seguidamente apresenta-se um exemplo, desses dados adicionais que estão separados por virgulas e que correspondem respetivamente ao CVE_ID (Identificação única na base de dados de vulnerabilidades), versão do CVSS, *BaseS, ImpactS, ExploitabilityS, Attack Vector, Attack Complexity, Previleges Required, User Interaction, Scope, Confidentiality, Integrity and Availability.*

No segundo destes registos podemos constatar que se trata da Vulnerabilidade CVE-2018-0235, da versão 3 do CVSS, com os seguintes valores: um base score de 7.4, um impact score de 4.0, um *exploitability score* de 2.8, um *attack vector Adjacent, user interaction none, scope none, confidentiality none, integrity none, availability high.*

"CVE_ID,Ver,BaseS,ImpactS,ExploitabilityS, AV,AC,PR,UI,S,C,I,A"

"CVE-2018-0235,3,7.4 ,4.0,2.8, A, L, N, N, C, N, N, H"

O segundo conjunto de dados adicional (assets.csv) permitirá definir, para cada ativo ou serviço, o seu valor para a organização bem como os dados seguintes:

"destinationC,AssetV,RiskApp,RiskObj,RPO,RTO,MTO"

"C2388,5.5,9.4,7.8,13.7,17.5,13.4"

Respetivamente o computador/host de destino ou seja aquele a que os dados dizem respeito, o seu valor para a organização, apetite de risco, objetivo de risco, *Recovery Point Objective, Recovery Time Objective, e Maximum Time Outage.*

3.6. Diagrama do fluxo de dados

A figura seguinte representa o fluxo dos dados envolvidos, os tipos de processamento a realizar nas diferentes fases do processo e os diferentes processos de tratamento dos mesmos, pretendendo ilustrar de forma simplificada os diferentes componentes com que se pretende implementar numa solução bem como possíveis exemplos de visualizações de suporte aos processos de decisão que constituirão os resultados e serão disponibilizados pela solução.

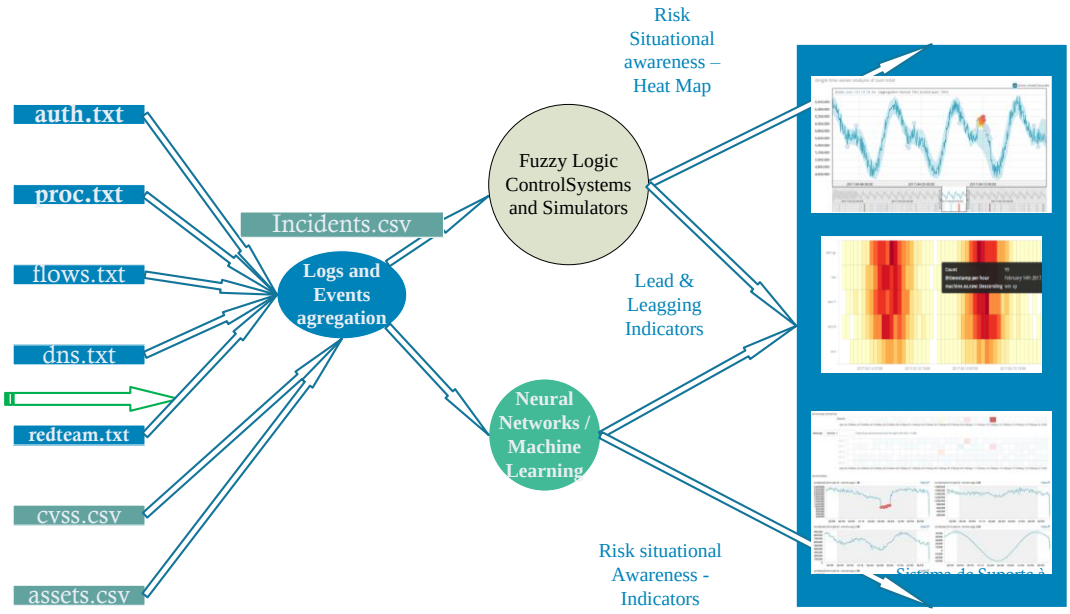


Ilustração 13- *Diagrama do fluxo de dados.*

Capítulo 4
Análise de Dados

4.1. Processos de análise dos Dados

Para se proceder a análise dos dados foi geralmente utilizada a ferramenta gráfica *Orange3* disponibilizada pela *framework Anaconda*.

A aplicação permite desenhar de forma intuitiva diagramas de fluxos de dados, alimentá-los a partir de diferentes *conjunto de dados*, realizar processo de filtragem por coluna ou linha, etc. e também dispõe de um conjunto de módulos que facilitam a análise dos dados e modelos. O *workflow* da figura seguinte e outros similares foram usados para validar modelos de extração de dados e para obter diversas representações dos dados deste trabalho.

Tem ainda como características o facto de se poder selecionar a propagação automática dos dados ao longo do *workflow* significando este facto que se os dados de entrada forem gerados a partir por exemplo do *tail*, de um ficheiro de log podem ser propagados, bem como a forma como afetam os diferentes nós do *workflow* do principio ao fim do mesmo e vir a afetar as visualizações que estiverem e os respetivos interfaces.

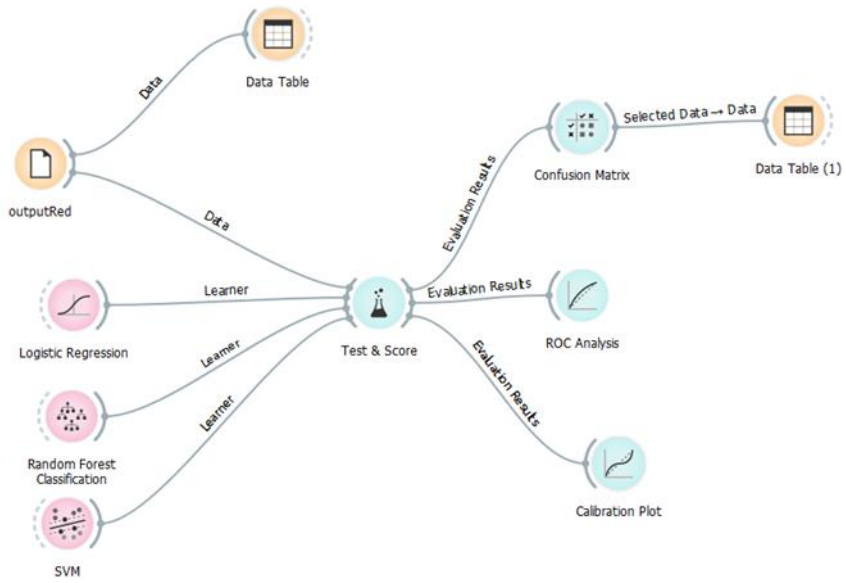


Ilustração 14- Diagrama do fluxo de dados usado para avaliar os diferentes modelos (Conjunto de dados RedTeam)

A figura seguinte permite observar no tempo os eventos do conjunto de dados gerados pelo *RedTeam*, sendo possível identificar os computadores originadores dos mesmos, eixo vertical e os alvos, ou destinos, dessas mesmas ações, eixo horizontal, os quais, para maior legibilidade são apresentados seguidamente:

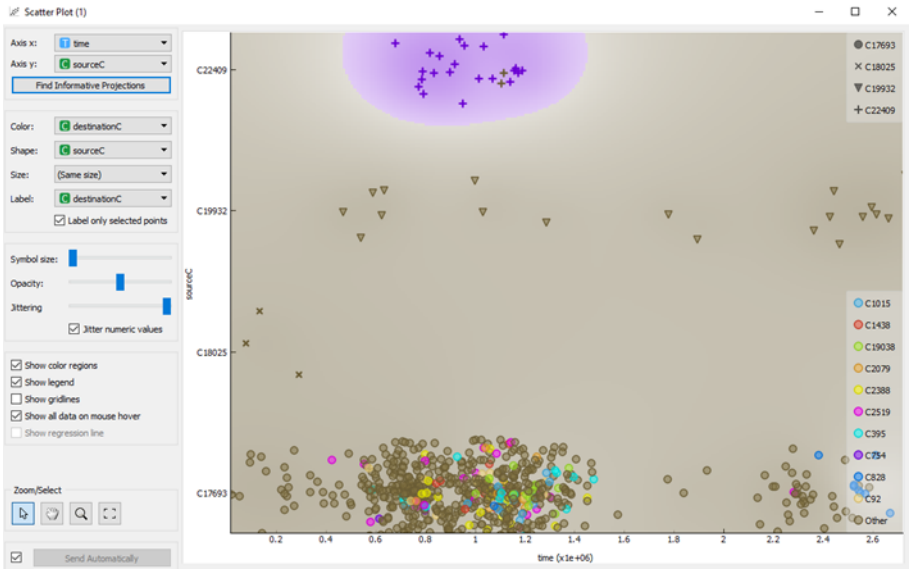


Ilustração 15- *Scatter plot* dos dados recolhidos no *conjunto de dados outputRed.csv* gerados, com a ferramenta gráfica *Orange*, a partir de eventos do *RedTeam*.

```
In [4]: 1 dfRed['sourceC'].value_counts()

Out[4]: C17693    701
        C22409     26
        C19932     19
        C18025      3
        Name: sourceC, dtype: int64

In [5]: 1 dfRed['destinationC'].value_counts()

Out[5]: C2388     27
        C754      26
        C2519     21
        C395      15
        C1015     15
        C19038    12
        C1438     11
        C92       11
        C828      10
        C2079     10
```

Ilustração 16- Distribuição dos originadores e destinatários dos eventos realizados pelo *RedTeam.*

Pelo exposto é possível perceber que a generalidade destes eventos teve origem em quatro computadores e que a maioria dos eventos teve como destino um também muito limitado conjunto de computadores, dez, sendo que os restantes computadores da rede do LANL, foram alvo de menos de dez ações desta equipa.

A *framework Orange* permite também realizar um conjunto de validações sobre os modelos escolhidos e realizar análises comparadas dos resultados obtidos por cada um deles perante determinados conjuntos de dados.

Das análises possíveis destacam-se pela sua importância as que permitem avaliar os parâmetros seguintes.

A curva *ROC* (*Receiver Operating Characteristic Curve*) é uma representação gráfica da performance do modelo de classificação no domínio de todos os níveis críticos de classificação. Através desta curva podemos avaliar dois parâmetros: a taxa de verdadeiros positivos (*TPR-True Positive Rate*) e a taxa de falsos positivos (*FPR-False Positive Rate*).

O primeiro destes rácios é um indicador de necessidade de revisão e é definido como o rácio entre o número total de positivos e o somatório do total de positivos com os falsos negativos:

$$TPR = \frac{TP}{TP + FN}$$

A Taxa de Falsos Positivos (FPR), por sua vez é definida pelo rácio entre o número de falsos positivos e a soma do total de falsos positivos com o total de negativos ou seja:

$$FPR = \frac{FP}{FP + TN}$$

A curva *ROC* apresenta os valores destes rácios para os diferentes níveis críticos de classificação. Se baixarmos o nível de classificação obteremos mais classificações positivas aumentando assim tanto os falsos positivos como os verdadeiros positivos. A figura seguinte é um exemplo de uma curva *ROC.*

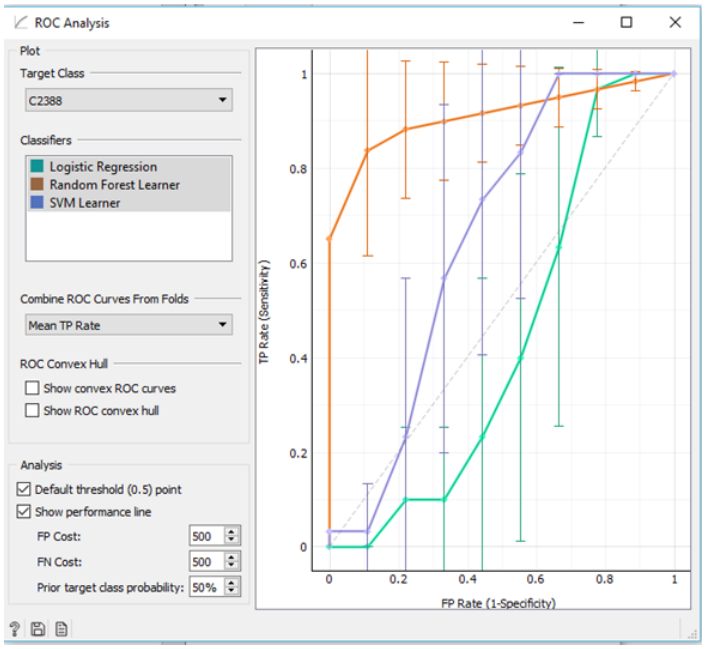


Ilustração 17- Análise ROC para o C2388 do conjunto de dados outputRed.csv como exemplo de curvas ROC

A área definida pela curva *ROC* (*AUC- Area Under ROC Curve*) dá-nos o valor da área limitada pela curva *ROC* e as retas (0,0) (0,1) e (1,0) (1.1). A figura seguinte representa uma das *AUC* obtidas durante a elaboração do trabalho, para os modelos *Logistic Regression, Random Forest Learner e SVM Learner*.

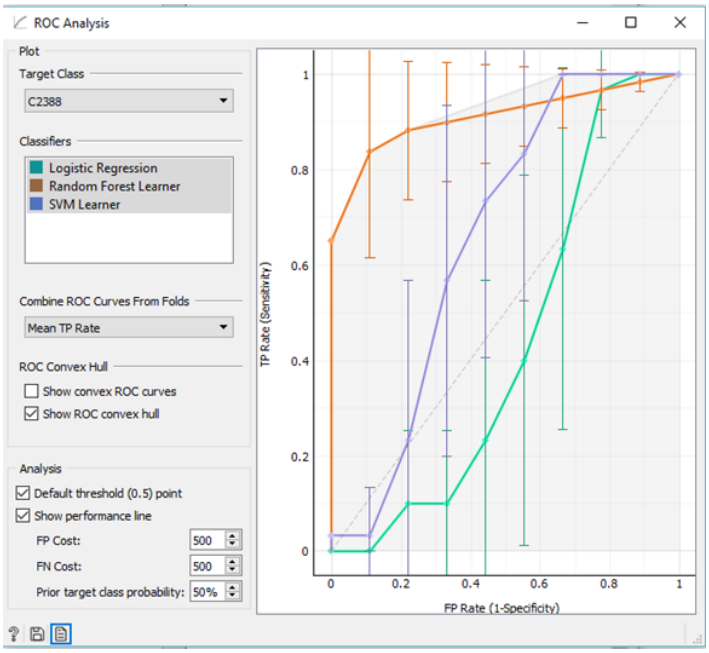


Ilustração 18- AUC dos diferentes modelos para o C2388

4.2. Dados do LANL

Foram recolhidos e utilizados um conjunto de dados de eventos de segurança disponibilizados pelo *Los Alamos National Laboratory* [41], e que representam 58 dias consecutivos de eventos, anonimizados e recolhidos na rede interna dos Laboratórios.

Estão incluídos ainda no conjunto de dados disponibilizados os dados de eventos realizados por um *RedTeam* que são apresentados num ficheiro independente.

A primeira dificuldade em trabalhar com os dados referidos foi relacionada com a dimensão dos ficheiros dos mesmos que no caso mais critico correspondiam a 72Gb, tornando muito difícil o seu manuseamento.

Foram também realizadas operações, código disponível no Capítulo 9 – Anexos) que permitiu dividir os diferentes conjuntos de dados em partes mais facilmente trabalháveis (~200kb).

Os dados referidos bem como outros gerados e recolhidos para a realização do trabalho serão analisados nos pontos seguintes.

4.3. Dados *RedTeam*

A informação disponível originada nos eventos gerados pelo *RedTeam* é apresentada no formato seguinte. Está disponível a informação temporal em que o evento ocorre, o utilizador e o domínio que realizou a transação, computador de origem da transação e computador destino da mesma.

```
In [10]:  1 dfRed = pd.read_csv("C:\datasets\LANL\datafiles\outputRed.csv")
          2 dfRed.head()
```

Out[10]:

	time	user@domain	sourceC	destinationC
0	150885	U620@DOM1	C17693	C1003
1	151036	U748@DOM1	C17693	C305
2	151648	U748@DOM1	C17693	C728
3	151993	U6115@DOM1	C17693	C1173
4	153792	U636@DOM1	C17693	C294

Ilustração 19- Estrutura dos dados gerados pelos eventos do RedTeam.

[41] A. D. Kent, "Comprehensive, Multi-Source Cybersecurity Events," Los Alamos National Laboratory, http://dx.doi.org/10.17021/1179829, 2015.

4.4. *Conjunto de dados* adicionais

Para a elaboração do presente trabalho foram criados os *conjuntos de dados* adicionais descritos seguidamente.

O *conjunto de dados* adicional *cvss.csv* foi produzido para este trabalho a partir de uma amostra aleatória das vulnerabilidades identificadas em *"https://nvd.nist.gov/vuln/full-listing"* para as quias os dados estivessem disponíveis na versão 3.0 da mesma classificação, que estivessem no estado *Analysed*, ou seja aquelas cuja análise se encontrava completa, com todas as associações de dados e que tivessem sofrido atualizações no decurso do ano de 2018. Foram assim ignoradas todas as vulnerabilidades que se encontravam, à data da recolha, em todos os outros estados.

Esta recolha foi feita de forma automática com recurso a um script desenvolvido em *python*, disponível no anexo 9.1, e a figura seguinte apresenta uma amostra do *conjunto de dados*

```
In [10]:
1 from numpy import isnan
2 from numpy import count_nonzero
3 from pandas import read_csv
4 import seaborn as sns
5 assets = read_csv('C:/datasets/LANL/tese/cvss.csv', header=0)
6 assets.head()
```

Out[10]:

	CVE-ID	Ver	BaseS	ImpactS	ExploitabilityS	AV	AC	PR	UI	S	C	I	A
0	CVE-2018-0235	3	7.4	4.0	2.8	A	L	N	N	C	N	N	H
1	CVE-2018-0258	3	9.8	5.9	3.9	N	L	N	N	U	H	H	H
2	CVE-2018-0252	3	8.6	4.0	3.9	N	L	N	N	C	N	N	H
3	CVE-2018-0226	3	7.5	5.9	1.6	N	H	L	N	U	H	H	H
4	CVE-2017-4952	3	7.5	3.6	3.9	N	L	N	N	U	H	N	N

Ilustração 20- Registos das métricas de vulnerabilidades disponíveis no *conjunto de dados* cvss.csv

Cada vulnerabilidade tem, de acordo com as especificações publicadas (FIRST, 2015) um conjunto de três grupos de métricas, o grupo de métricas base, o grupo de métricas temporais e o grupo de métricas ambientais.

O grupo de métricas *Base Score* é um grupo de métricas de base, que representam as caraterísticas intrínsecas da vulnerabilidade e que por isso mesmo são constantes ao longo do tempo e independentes do ambiente onde a vulnerabilidade vier a ser detetada.

O grupo de métricas temporais, *Temporal Score*, reflete o conjunto de caraterísticas da vulnerabilidade que são passíveis de ser afetadas pelo tempo, como sejam o aparecimento de *exploits* que explorem as mesmas ou a disponibilização de um *patch, que*

permita implementar controlos que as anulem ou que minimizem o seu impacto ou possibilidade de exploração e portanto o respetivo score..

O grupo de métricas ambientais, *Environmental Score*, representa as características de uma vulnerabilidade que são dependentes do ambiente onde a mesma se encontra, como sejam por exemplo a arquitetura das redes, duplicação de sistemas ou caraterísticas especificas associadas ao risco do negócio do nó, ativo ou sistema onde a mesma se encontra.

Assim e para cada vulnerabilidade identificada de acordo com os critérios referidos anteriormente, foram recolhidas as seguintes métricas: *Base Score (BaseS)*, *Impact Score (ImpactS)*, *Exploitability Score (ExploitabilityS)*, *Attack Vector (AV)*, *Attack Complexity, (AC)*, *Previleges Required (PR)*, *User Inteaction (UI)*, *Scope (S)*, e impacto nos atributos *Confidentiality*, *Integrity* e *Availability (A)*,

Foi criado um segundo *conjunto de dados*, designado *assets*, preenchido, de acordo com uma distribuição normal dos valores definidos em sede de *BIA*, correspondentes ao valor do ativo, apetite de risco, objetivo de risco, e os valores dos diferentes objetivos de recuperação, *RPO*, *RTO* e tempo máximo de indisponibilidade, *MTO*, também de acordo com uma distribuição normal dos diferentes valores, pelos hosts constituintes da rede do *LANL*, utilizando um script em *python*, com uma restrição adicional, que decorre da própria definição dos objetivos de risco e que recomenda que o *Risk Appetite* seja maior ou igual ao *Risk Objective*, pelas razões aduzidas no capítulo relativo ao *BIA*.

```
In [9]:
1 from numpy import isnan
2 from numpy import count_nonzero
3 from pandas import read_csv
4 import seaborn as sns
5 assets = read_csv('C:/datasets/LANL/tese/Assets.csv', header=0)
6 assets.head()
```

Out[9]:

	destinationC	AssetV	RiskApp	RiskObj	RPO	RTO	MTO
0	C2388	5.5	9.4	7.8	13.7	17.5	13.4
1	C754	4.7	4.3.6	13.3	9.4	13.1	NaN
2	C2519	4.9	6.8	6.7	9.1	14.9	12.8
3	C395	8.0	7.0	4.6	10.8	14.0	11.4
4	C1015	3.6	7.4	2.9	14.7	11.7	13.6

Ilustração 21- Registos das métricas do conjunto de dados assets.csv

Foi ainda criado um terceiro *conjunto de dados*, incidentes,csv, integrando e atribuindo a cada um dos computadores de destino (*destinationC*) dos eventos *redteam* as métricas resultantes do *conjunto de dados* cvss.

```
import numpy as np
import matplotlib.pyplot as plt
import skfuzzy as fuzz
import skfuzzy.control as ctrl
import skfuzzy as fuzz
import seaborn as sns
import pandas as pd
%matplotlib inline
incidents = pd.read_csv("C:/datasets/LANL/tese/incidents.csv")
incidents.head()
```

	Unnamed: 0	time	user@domain	sourceC	destinationC	AssetV	RiskApp	RiskObj	RPO	RTO	...	ImpactS	ExploitabilityS	AV	AC	PR	UI	S	C	I	A
0	0	153792	U636@DOM1	C17693	C294	4.9	6.4	4.9	16.7	8.8	...	4.0	2.8	A	L	N	N	C	N	N	H
1	1	483455	U1723@DOM1	C17693	C294	4.9	6.4	4.9	16.7	8.8	...	5.9	3.9	N	L	N	N	U	H	H	H
2	2	483981	U1723@DOM1	C17693	C294	4.9	6.4	4.9	16.7	8.8	...	4.0	3.9	N	L	N	N	C	N	N	H
3	3	485925	U1723@DOM1	C17693	C294	4.9	6.4	4.9	16.7	8.8	...	5.9	1.6	N	H	L	N	U	H	H	H
4	4	486443	U636@DOM1	C17693	C294	4.9	6.4	4.9	16.7	8.8	...	3.6	3.9	N	L	N	N	U	H	N	N

Ilustração 22- Primeiros registos das métricas completas das vulnerabilidades disponíveis no ***conjunto de dados*** cvss.csv

Capítulo 5
Plataforma de processamento dos dados

Neste capítulo descreve se a metodologia e critérios utilizados para a seleção da plataforma e livrarias a que foi necessário recorrer ou implementar para desenvolver os trabalhos que permitissem suportar a presente investigação.

5.1. Critérios de seleção

Na elaboração do presente trabalho foram avaliadas diversas plataformas passíveis de serem utilizadas para suportar a realização do mesmo. Assim e após pesquisas foram identificadas algumas *frameworks* e definidos os requisitos mínimos que se entendeu as mesmas deveriam possuir, considerando os recursos tecnológicos disponíveis para a realização dos trabalhos de investigação (PC Portátil, i7, 16G RAM, 250G Disco). e que se podem resumir na figura seguinte:

Requisito	Matlab	Anaconda	Tensorflow	Orange3	ELK Stack
Open source	Não	Sim	Sim	Sim	Sim(ver opções gráficas)
Linguagem(es)	Própria	Python	Pyhon/outras	Python	Várias
Dinâmica de suporte (Actividade nos grupos de utilizadores, actualizações,..)	Alta	M. Alta	Media	Media	Media
Ferramentas de análise disponiveis	M.Alta	Bom	Bom	Bom	Bom
Gestão do ambiente utilizado	Media	M. Alta	Media	Alta	Baixa
Opções Gráficas	Alta	Alta	Alta	Alta	Média(Licença)
Capacidade de deployment para produção	Media(Nota 1)	Alta	Alta	Alta	Dependente de recursos da infraestrutura
Suporte Industrial	Proprietário-Matlab	Opensource	Opensource - Google	Opensource	Proprietário-RedHat
Requisitos da infraestrutura de suporte	Alta	Media	Alta	Media	Alta
CPU	Alta	Media	Media	Media	Alta
Memória	Alta	Media	Media	Media	Alta
	Nota 1- A solução Matlab avaliada dependia de uma ova disponibilizada sobre uma VM, que dispunha de recursos limitados de CPU e disco	Nota 2- A solução Anaconda - interface gráfico da framework conda tem facilidades de gestão integradas do ambiente de todos os pacotes instalados			

Ilustração 23- Quadro dos parâmetros de avaliação das diferentes *frameworks* consideradas como passíveis de serem utilizadas para a realização do trabalho.

Considerando os fatores referidos na figura anterior decidiu-se optar pela plataforma *Anaconda*, de *data science* e *machine learning*, que reclama para ela própria uma comunidade de mais de seis milhões de utilizadores, de código aberto, baseada em *python* e R, com capacidade de gestão de diferentes ambientes de teste ou validação e com a possibilidade de utilização de componentes de análise gráfica.

Acresce que esta *framework* permite a utilização integrada do *Orange* e do *jupyter notebook* e a gestão do ambiente utilizado pelas diferentes livrarias de *python*.

Esta *framework* permite ainda a edição interativa de código, tendo sido inicialmente instalada a versão 1.7.0 da referida *framework*, e atualizada sucessivamente para a versão 1.9.2 com a qual foram realizados os últimos scripts que se referem neste trabalho.

5.2. Condicionantes

Um dos parâmetros de avaliação (Dinâmica de suporte), tal como representado na figura anterior, e que pretende avaliar o numero e a frequência de interações da comunidade envolvida no desenvolvimento das componentes de código aberto[42][43], apesar de ser de facto muito alta, na *framework* escolhida, Anaconda, veio a revelar-se como relativamente contraproducente e demasiado volátil (nomeadamente na componente de atualizações e dependências), o que, devido ao elevado número de pacotes e livrarias envolvidas no ambiente utilizado provocou demasiada entropia durante a elaboração do trabalho.

O conjunto dos dados recolhidos do LANL, é um conjunto muito vasto de dados, tendo alguns dos ficheiros mais de 70G, o que dificulta a sua utilização e manuseamento, com os recursos disponíveis para a realização do trabalho.

5.3. Solução adotada

Assim foi instalada e mantida a plataforma *Anaconda* (v1.9.2) de gestão do ambiente e pacotes que compõem as diferentes aplicações e a própria *framework*, e as aplicações: *Orange3*, uma aplicação que integra com esta plataforma e que é um conjunto

[42] https://github.com/matplotlib/matplotlib/graphs/code-frequency
[43] https://github.com/numpy/numpy/graphs/code-frequency

de ferramentas de programação visual para *machine learning, data mining e data visualization*, a aplicação *web Jupyter Notebook* (v5.7.0), que permite criar e partilhar documentos com código, visualizações com funcionalidades de limpeza e transformação de dados, simulação numérica, modelação estatística, visualização de dados, *machine learning*, *data mining* e análise de dados com vários *workflows* interativos, *QTConsole* (v4.4.2) um interface gráfico baseado em *PyQt*, *Spyder* (v3.3.1) um ambiente de desenvolvimento integrado para *Python.*

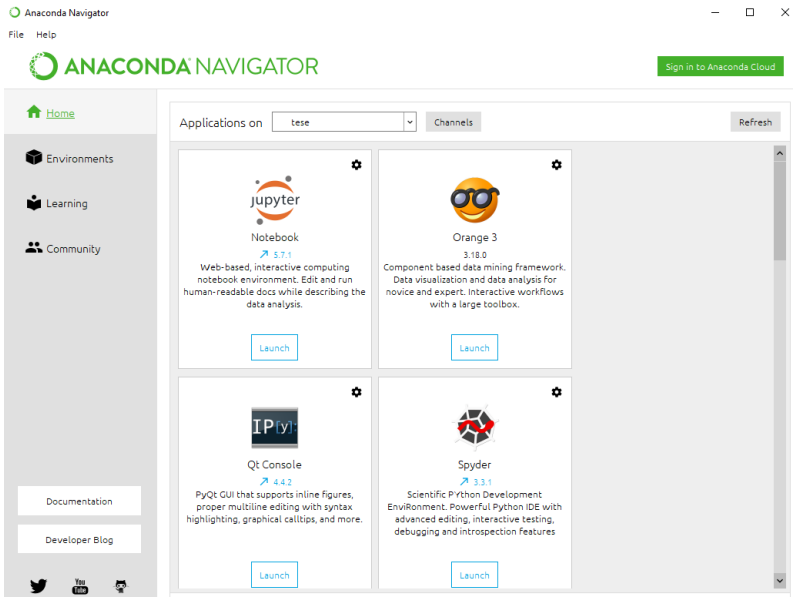


Ilustração 24- Interface de gestão da aplicação *Anaconda* com as aplicações instaladas no ambiente tese configurada para suportar a implementação da solução.

5.4. Anaconda

A figura seguinte apresenta o painel de controlo da *framework Anaconda* com os diferentes ambientes e pacotes aplicacionais instalados (227).

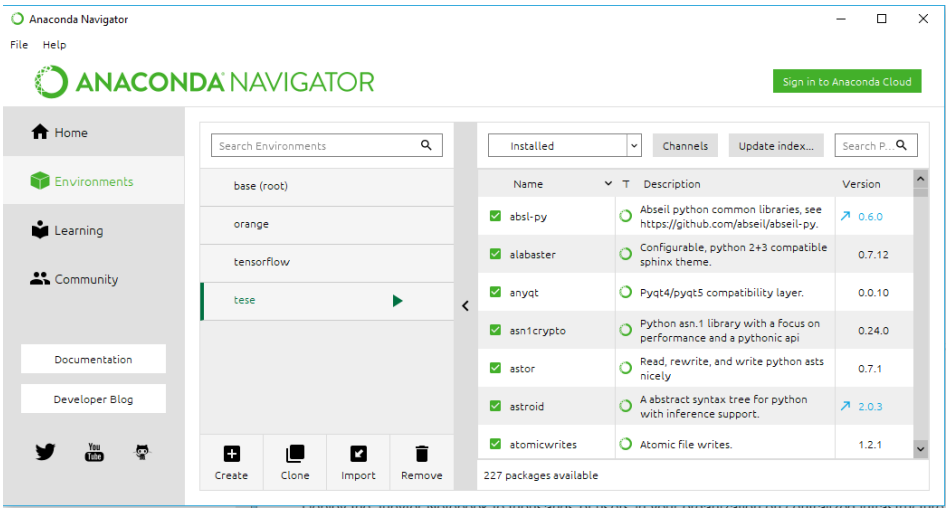


Ilustração 25- Interface de gestão da aplicação Anaconda Navigator do ambiente tese configurada para suportar a implementação da solução.

Cada um dos pacotes instalados permite ou implementa um determinado conjunto de funcionalidades utilizáveis no desenvolvimento de scripts, controlos e simuladores.

Os pacotes mais relevantes para os trabalhos realizados foram:

- *skfuzzy* – uma *toolbox* que implementa as funções de logica de *fuzzy*;

- *pandas*- uma livraria de código aberto de alta performance para análise de estruturas de dados;

- *numpy* – computação científica em *python;*

- *matplotlib*- livraria gráfica;

- *seaborn* -livraria gráfica baseada no *matplotlib* de visualização de dados;

5.5. Orange

Orange é uma solução *opensource* para visualização interativa de dados e análise dos mesmos, através de uma interface gráfica ou de *python scripting*. Tem diversos

componentes para *machine learning*, pesquisa de texto e recentemente incorpora também componentes para bioinformática e séries temporais.

Os componentes mais importantes utilizados foram as funcionalidades de seleção e processamento de dados, avaliação de diferentes modelos preditivos e implementação dos *workflows*, elaboração das previsões e análise das mesmas.

5.6. Jupyter Notebook

É uma aplicação *web opensource* que permite criar e partilhar documentos que contêm código fonte, equações, visualizações e texto descritivo que pode ser utilizada para simulação numérica, modelação estatística, visualização e transformação de dados.

A figura seguinte mostra a interface da aplicação a correr no computador local. Neste trabalho foi utilizada para implementar, validar, executar e obter os resultados do código utilizado para implementar as componentes de lógica difusa e representação gráfica dos respetivos resultados.

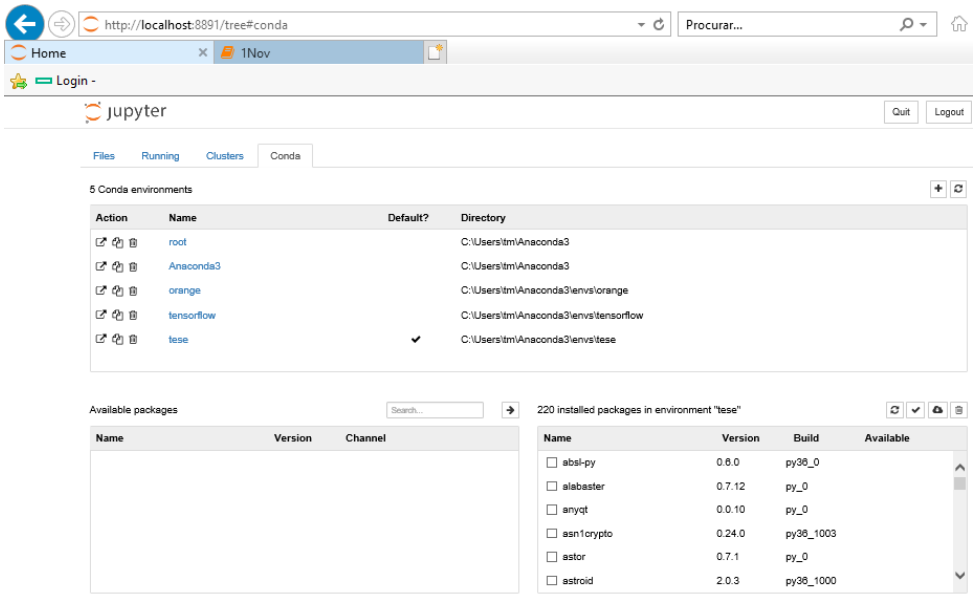


Ilustração 26- Interface de gestão da aplicação ***Jupyter Notebook*** que suportou os trabalhos realizados.

5.7. Sumário

A escolha da plataforma para realizar os trabalhos foi uma escolha importante e condicionada pelos recursos computacionais disponíveis, por uma solução que fosse de

código livre, e que portanto não onerasse nem o decurso dos trabalhos nem a solução a que os mesmos pudessem conduzir e que por outro lado dispusesse de todos os recursos necessários para atingir os objetivos propostos.

Sendo um dos parâmetros a considerar na escolha da linguagem/framework a utilizar a atividade registada pela mesma nas plataformas onde se encontra alojada, (ex. https://github.com/scikit-fuzzy/scikit-fuzzy/pulse) de modo a evitar a adoção de uma solução ou descontinuada ou com um baixo indice de atividade o facto é que a muito intensa atividade de atualização dos diferentes componentes da solução, bem como as dependências dos diferentes pacotes que compõem a solução escolhida provocou alguns problemas de estabilidade e incompatibilidade de módulos o que se veio a revelar como um desafio adicional.

Capítulo 6
Apresentação e discussão dos resultados

Neste capítulo são apresentados os resultados obtidos durante a realização do presente trabalho. Começamos por descrever o modelo e os diferentes componentes que o constituem e posteriormente apresentamos os resultados obtidos com a utilização do mesmo, na gestão das vulnerabilidades e risco. Terminaremos com a informação pertinente obtida e com as diferentes possibilidades da sua utilização num sistema de suporte à decisão.

6.1. Modelo de gestão de vulnerabilidades e risco

A ilustração seguinte representa o modelo utilizado no decurso dos trabalhos e o fluxo de dados entre os diferentes componentes do mesmo.

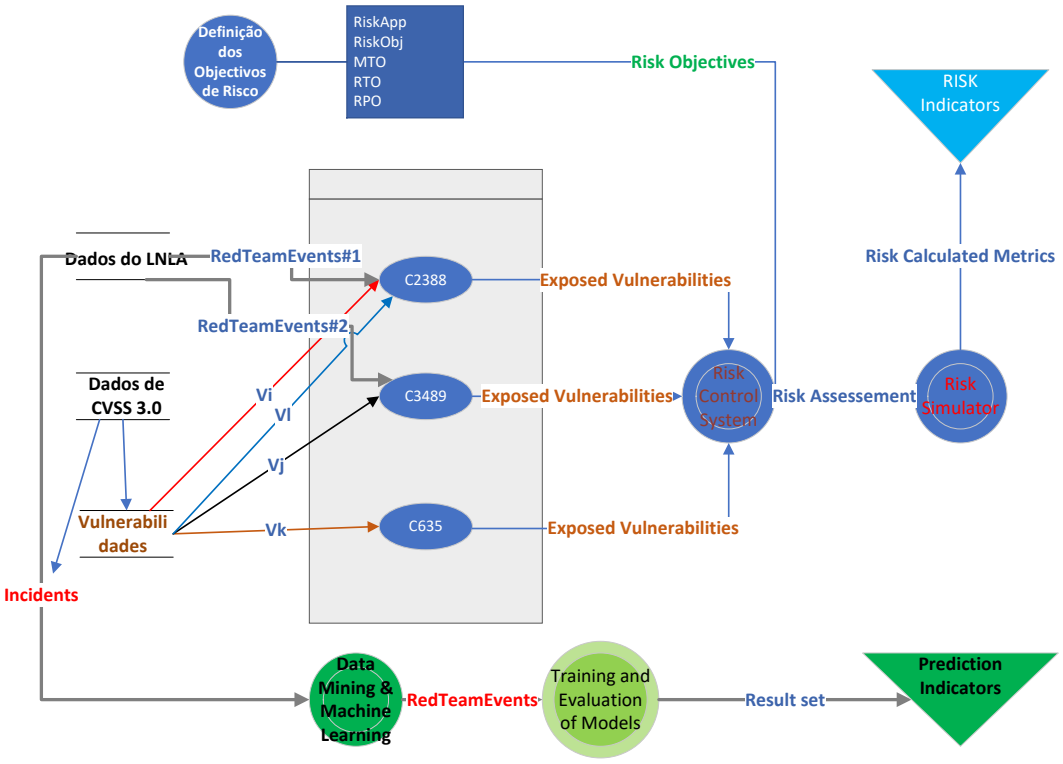


Ilustração 27- Modelo de gestão de Vulnerabilidades e Risco.

6.1.1. Componentes e descrição do Modelo

Os trabalhos realizados tiveram como objetivo permitir quer a avaliação das vulnerabilidades e do nível de exposição ao risco, decorrente das mesmas, a que os diferentes ativos (*hosts*) estavam expostos, quer a avaliação e treino de um conjunto de modelos preditivos, a identificação de quais destes modelos se revelavam mais precisos face aos dados existentes e a produção de indicadores preditivos relativamente ao conjunto de *hosts*.dos potenciais alvos dos próximos ataques considerando os dados disponíveis do conjunto de ações realizadas por um *RedTeam*. .

Os *workflows* utilizados para produzir as diferentes avaliações que a seguir se descrevem com mais pormenor estão representados na figura seguinte.

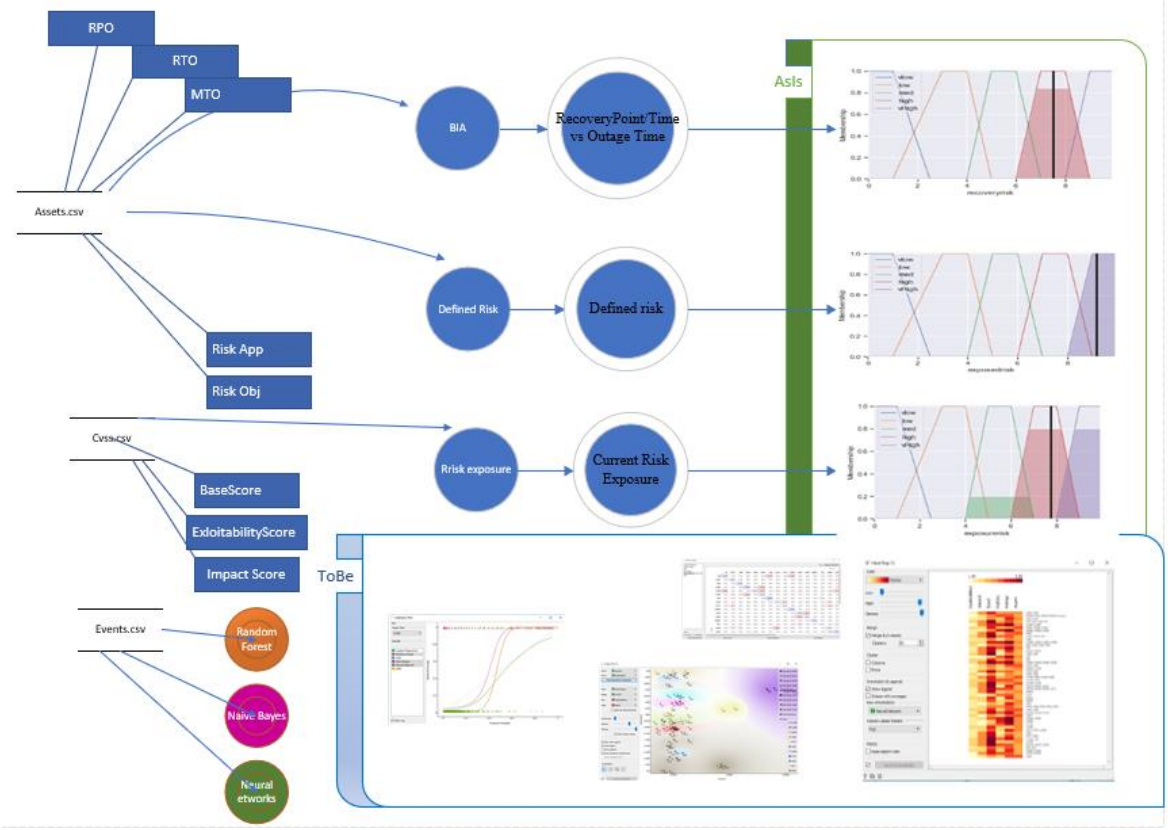


Ilustração 28- Diagramas do fluxo de dados utilizados para produzir os resultados

Assim os parâmetros RPO, RTO e MTO foram utilizados para a avaliação do impacto no negócio, os parâmetros *risk appetite* e *risk objective* para a risco definido,

Para a exposição atual ao risco foram utilizados os valores do *base score*, *exploitbility score* e *impact score* de todas as vulnerabilidades que afetavam um determinado ativo.

6.1.2. Avaliação do Impacto nas variáveis diretamente ligadas ao BIA[44]

Para permitir a avaliação do impacto nas variáveis diretamente ligadas ao negócio e nomeadamente para permitir avaliar qual o impacto nos objetivos definidos para qualquer ativo em sede de impacto no negócio, que como referido anteriormente, eram os valores correspondentes aos *RPO*[45], *RTO*[46] e *MTO*[47], utilizou-se um modelo de controlo e simulação baseado na logica difusa implementado com o pacote *skfuzzy*.

Definiram-se as três variáveis, `PObj = TObj = MTObj = universe`, respetivo universo e as respetivas funções de pertença de que se dá seguidamente um exemplo.

```
PObj_vHigh = fuzz.trapmf(universe, [0, 0, 2, 3])
PObj_high= fuzz.trapmf(universe, [2, 3, 4 , 5])
PObj_med= fuzz.trapmf(universe, [4, 5 , 6, 11])
PObj_low= fuzz.trapmf(universe, [6, 11, 12, 24])
PObj_vlow = fuzz.trimf(universe, [12, 24, 24])
```

Considerou-se como razoável que os objetivos nesta área pudessem situar-se num universo linear entre 0 e 24 horas `universe = np.arange(0, 24, 0.1)` (altura a partir da qual se considerou que estaríamos perante a necessidade de acionar ou planos de contingência ou mecanismos de recuperação de desastre). A figura seguinte apresenta de modo gráfico a função de pertença relativamente a uma dessas variáveis sendo as outras de grafismo semelhante.

Ilustração 29- Função de pertença da variável RTObj

[44] *BIA- Business Impact Analysis*
[45] *RPO- Recovery Point Objective*
[46] *RTO- Recovery Time Objective*
[47] *MTO-Maximum Time of Outage*

A *defuzzyficação* da referida função permitiu obter os valores que se observam na figura seguinte.

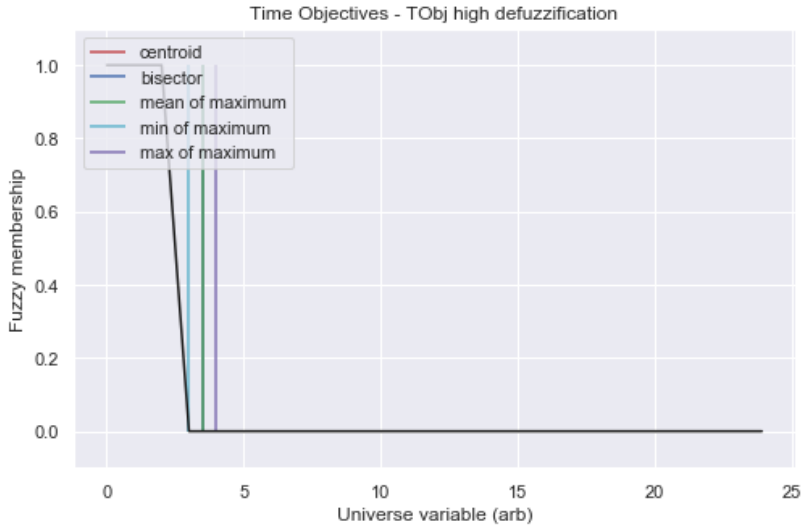


Ilustração 30- Defuzzificação da variável RTObj para o nível médio.

Para efeitos da simulação considerou-se como crítico o período inferior às 6 horas razão pelo qual se definiu, para esse caso, um universo específico com um ponto critico com o valor de 5.9.

```
universe = np.linspace(0, 5.9, 24)
```

Para o simulador foram definidas três variáveis fuzzy, respetivamente,

```
RecoveryPointTimeObj = ctrl.Antecedent(universe, 'RecoveryPointTimeObj')
```

para os objetivos de recuperação do RTO e RPO e

```
MaxOutage = ctrl.Antecedent(universe, 'MaxOutage')
```

e a do universo dos resultados,

```
output = ctrl.Consequent(universe, 'output')
```

Estas três variáveis foram preenchidas com os diferentes níveis

```
names = ['vlow', 'low', 'med', 'high', 'vHigh']
```

correspondentes à valoração respetiva,

```
MaxOutage.automf(names=names)
```

Seguidamente foram criadas as rules que permitiam a gestão do sistema de controlo e de simulação de que se mostra um dos exemplos:

```
rule4 = ctrl.Rule(antecedent=((RecoveryPointTimeObj['high'] & MaxOutage['vHigh']) |
                              (RecoveryPointTimeObj['vHigh'] & MaxOutage['vHigh']) |
                              (RecoveryPointTimeObj['vHigh'] & MaxOutage['high'])),
                  consequent=output['vHigh'], label='rule vHigh')
```

O sistema de controlo foi iniciado com todas as rules criadas previamente e validar que as mesmas cobrem todo o universo de estados possíveis.

```
system = ctrl.ControlSystem(rules=[rule0, rule1, rule2, rule3, rule4])
```

e seguidamente inicializado o sistema de simulação

```
sim = ctrl.ControlSystemSimulation(system, flush_after_run=24 * 24 + 1)
```

O simulador permite que definido qualquer valor de entradas seja determinado o resultado da aplicação a essas mesmas entradas do conjunto de regras definido e gerar o resultado correspondente. A aplicação da simulação à totalidade do universo de entradas permite gerar o espaço de resultados que está representado na figura seguinte para este conjunto de variáveis.

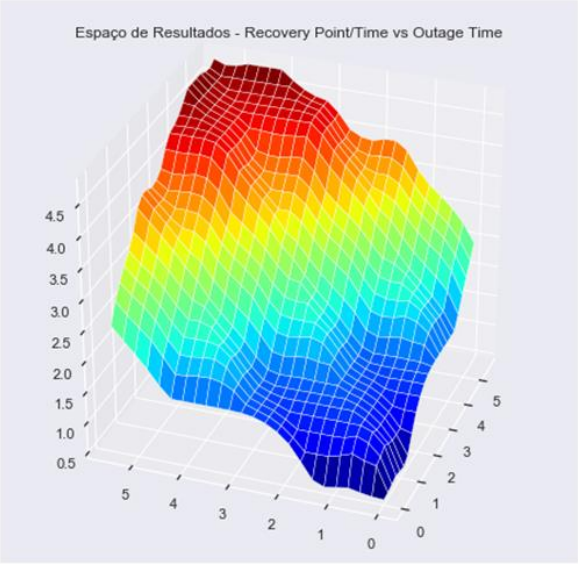


Ilustração 31- Espaço de resultados RecoveryPoint/Time vs Outage Time.

São visíveis na figura as zonas do espaço de resultados correspondentes aos níveis mais altos representados pela cor vermelho escuro. De forma semelhante será também possível avaliar o risco relativo aos tempos e ponto de recuperação bem como ao tempo máximo de indisponibilidade de um determinado ativo como se descreve seguidamente.

Definidos o universo temporal considerado, para os parâmetros baseados no tempo, *RPO*, e *RTO*

```
timespace = np.arange(0, 24, 0.1)
```

e o universo de risco em que estes mesmos parâmetros produziriam resultados,

```
riskspace = np.arange(0, 10, 0.1)
```

foram definidas as funções de controlo respetivas

```
OutTime = ctrl.Antecedent(timespace,'outtime')
```

```
Recovery = ctrl.Antecedent(timespace, 'recovery')
```

e as respetivas funções de pertença seguintes, onde se consideram os intervalos de recuperação de ativos até 3 horas correspondentes a riscos muito altos, e assim sucessivamente até um limite de 24 horas para ativos de risco muito baixos.

```
Recovery['vHigh'] = fuzz.trapmf(timespace, [0, 0, 3, 4])
Recovery['high'] = fuzz.trapmf(timespace, [3, 4, 5 , 6])
Recovery['med'] = fuzz.trapmf(timespace, [5, 6 , 8, 12])
Recovery['low'] = fuzz.trapmf(timespace, [8, 12, 14, 24])
Recovery['vlow'] = fuzz.trimf(timespace, [14, 24, 24])
```

```
OutTime['vHigh'] = fuzz.trapmf(timespace, [0, 0, 2, 3])
OutTime['high'] = fuzz.trapmf(timespace, [2, 3, 4 , 5])
OutTime['med'] = fuzz.trapmf(timespace, [4, 5 , 6, 11])
OutTime['low'] = fuzz.trapmf(timespace, [6, 11, 12, 24])
OutTime['vlow'] = fuzz.trimf(timespace, [12, 24, 24])
```

Definida a função de pertença do universo de resultados possíveis e representada graficamente na figura seguinte é possível verificar que se consideraram riscos de recuperação altos para valores inferiores a 2,5 horas, uma vez que se assumiu que se um determinado ativo tem um tempo de recuperação máximo desta ordem de grandeza será um ativo critico para o negócio.

```
recoveryRisk['vlow'] = fuzz.trapmf(riskspace, [0, 0, 1, 2.5])
recoveryRisk['low'] = fuzz.trapmf(riskspace, [1, 2.5, 4 , 5])
recoveryRisk['med'] = fuzz.trapmf(riskspace, [4, 5 , 6, 7])
recoveryRisk['high'] = fuzz.trapmf(riskspace, [6, 7 , 8, 9])
recoveryRisk['vHigh'] = fuzz.trapmf(riskspace, [8, 9 , 10, 10])
```

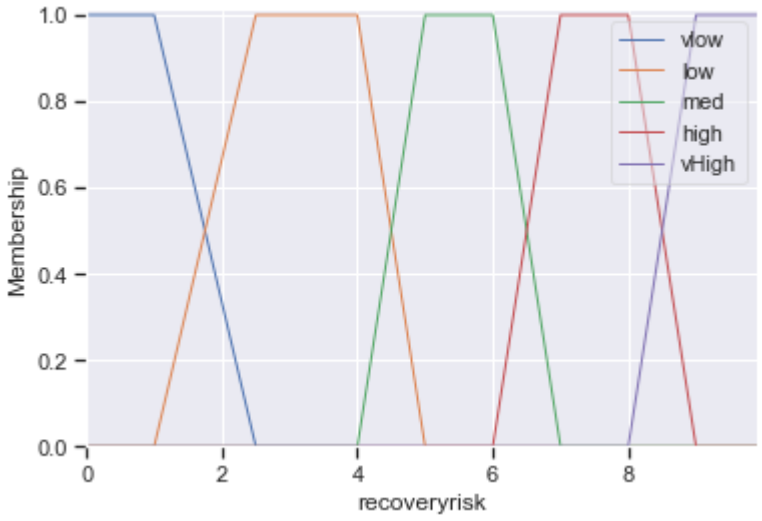


Ilustração 32- Função de pertença dos riscos de recuperação de um ativo.

Seguidamente apresenta-se um exemplo de uma das regras utilizadas no sistema de controlo e na simulação do mesmo.

```
rule2 = ctrl.Rule( Recovery['low'] & OutTime['low'] |
                   Recovery['vlow'] & OutTime['med'] |
                   Recovery['med'] & OutTime['vlow'] |
                   Recovery['low'] & OutTime['med'] |
                   Recovery['med'] & OutTime['low']
                   , recoveryRisk['low'])
```

Como se pode verificar considerou-se que para tempos de recuperação muito baixos (entre 14 e 24 horas), baixos (entre as 8 e as 14 horas) e as combinações destes com um, e apenas um, nível de risco médio estaríamos perante uma situação em que o risco de recuperação seria baixo. Esta regra é visualizável na figura seguinte.

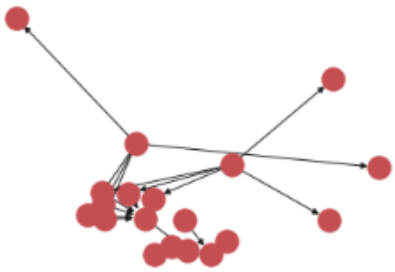


Ilustração 33- Representação gráfica da *rule2* do sistema de controlo do risco de recuperação de um ativo.

A inicialização do sistema de controlo foi feita com a totalidade das regras aplicáveis de acordo com a expressão seguinte:

```
recovery_ctrl = ctrl.ControlSystem([rule1, rule2, rule3, rule4, rule5])
```

e a activação do simulador com

```
recovery_calc = ctrl.ControlSystemSimulation(recovery_ctrl)
```

.

A estimulação deste mesmo simulador com tempos de resposta de 4.7 horas e tempos máximos de indisponibilidade de 6.8 horas permitiu obter os seguintes gráficos de exposição ao risco e de recuperação do ativo.

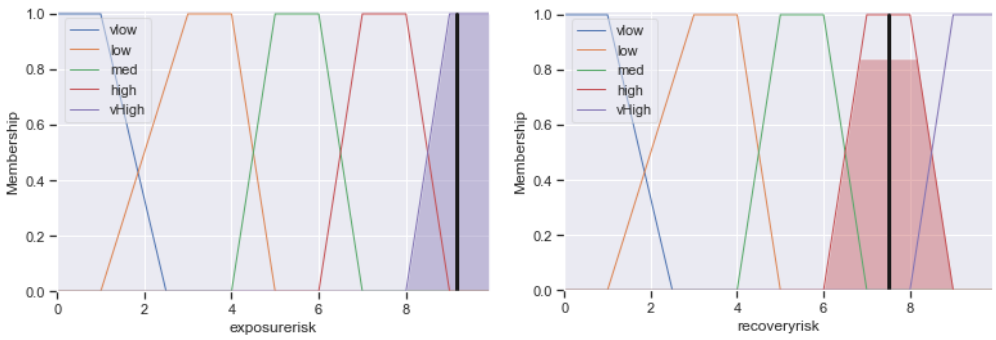


Ilustração 34- Nível de exposição ao risco e de recuperação de um ativo.

6.1.3. Gestão de vulnerabilidades e risco

A função m*embership* da exposição ao risco, de cada um dos ativos, entendida como o resultado das funções dos scores, das CVSS, que afetam um determinado ativo nas suas componentes de *base score* e *exploitability score*, foi definida depois de extraídos os scores das vulnerabilidades que afetam esse mesmo ativo.

Para cada uma das variáveis e para o conjunto de resultados foi utilizado um modelo com cinco níveis de pertença estando discriminadas seguidamente as funções que suportam o universo dos resultados.

```
ExposureRisk['vlow'] = fuzz.trapmf(riskspace, [0, 0, 1, 3])
ExposureRisk ['low'] = fuzz.trapmf (riskspace, [1, 3, 4, 5])
ExposureRisk ['med'] = fuzz.trapmf (riskspace, [4, 5, 6, 7])
ExposureRisk ['high'] = fuzz.trapmf (riskspace, [6, 7, 8, 9])
ExposureRisk ['vHigh'] = fuzz.trapmf (riskspace, [8, 9, 10, 10])
```

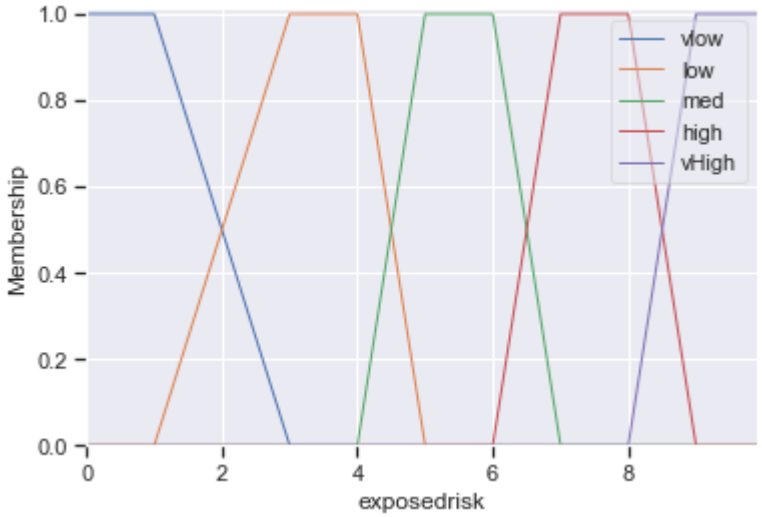


Ilustração 35- Função de pertença da exposição ao risco para diferentes níveis do mesmo.

Foram também construídos os conjuntos de regras que possibilitariam a ativação do modelo do sistema de controlo e do simulador do mesmo modelo. A título de exemplo apresenta-se o conjunto de regras que suporta a *rule1, do referido modelo*, bem como o respetivo modelo tal como representado graficamente pela aplicação.

```
rule1 = ctrl.Rule (ExploitScore ['vlow'] & BaseScore ['vlow'] |
                   ExploitScore ['vlow'] & BaseScore ['low'] |
                   ExploitScore ['low'] & BaseScore ['vlow']
                    ExposureRisk['vlow'])
```

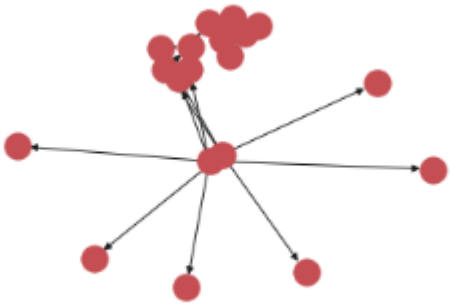


Ilustração 36- Visualização do ruleset da rule1 – Risco muito baixo (vlow)

As funções de criação do modelo e de simulação do mesmo são referenciadas de seguida, sendo ativadas com os dados dos ativos cuja análise se pretende. Importa ainda referir que o modelo de simulação tem mecanismos de verificação que permitem garantir se o universo de todos os casos possíveis está coberto, não realizando a avaliação e respetiva simulação se tal não acontecer.

```
risk_ctrl = ctrl.ControlSystem ([rule1, rule2, rule3, rule4, rule5])
risk_calc = ctrl.ControlSystemSimulation (risk_ctrl)
risk_calc.compute ()
ExposureRisk.view (sim=risk_calc)
```

A aplicação do sistema de controlo e do simulador a um dos computadores referenciados como originadores dos eventos do *RedTeam*, supostamente sofrendo de uma vulnerabilidade conhecida permitiu apurar os seguintes resultados.

```
Current Risk Exposure:
Host: C17693
 CVE: CVE-ID-11595
 CVE vector: CVE-2018-11595,3,7.8 ,5.9,1.8,L,L,N,R,U,H,H,H
 Current Risk Score: 7.740728831725619
```

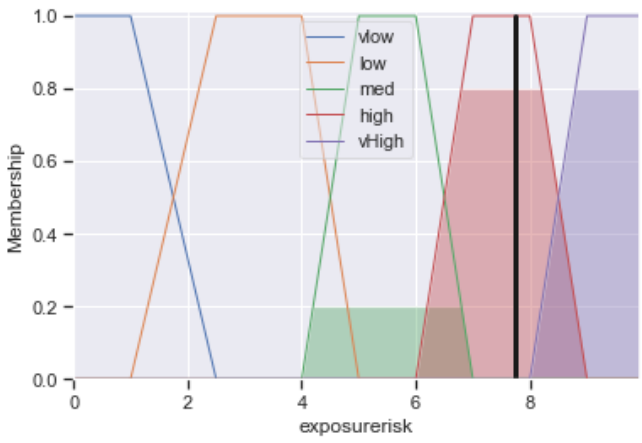


Ilustração 37- Visualização do nível de exposição ao risco do host C17693, gerado pelo simulador.

Como se constada da figura, é possível perceber as diferentes componentes de risco em cada um dos seus níveis, no caso nível médio com a componente mais baixa e risco alto e muito alto com as componentes maiores, bem como a representação do nível global calculado de exposição ao risco para este ativo.

Para a avaliação das componentes de apetite de risco e objetivos de risco dos ativos utilizou-se uma metodologia semelhante para se tentar obter indicadores que possibilitassem a tomada de decisão.

Assim definiu-se um universo para estas variáveis

```
riskspace = np.arange(0, 10, 0.1)
```

e as respetivas funções de pertença de que se dá seguidamente um exemplo.

```
RiskObj['vlow'] = fuzz.trapmf(riskspace, [0, 0, 1, 3])
RiskObj['low'] = fuzz.trapmf(riskspace, [1, 3, 4 , 5])
RiskObj['med'] = fuzz.trapmf(riskspace, [4, 5 , 6, 7])
RiskObj['high'] = fuzz.trapmf(riskspace, [6, 7 , 8, 9])
RiskObj['vHigh'] = fuzz.trapmf(riskspace, [8, 9 , 10, 10])
```

As variáveis de controlo criadas foram as seguintes:

```
RiskApp = ctrl.Antecedent(riskspace, 'riskappetite')
RiskObj = ctrl.Antecedent(riskspace, 'riskobjective')
DefinedRisk = ctrl.Consequent(riskspace, 'definedrisk')
```

As regras correspondentes à totalidade dos casos possíveis, de que também se dá apenas um exemplo e o respetivo gráfico:

```
rule2 = ctrl.Rule( RiskObj['low'] & RiskApp['low'] |
                   RiskObj['vlow'] & RiskApp['med'] |
                   RiskObj['low'] & RiskApp['med']
                   , DefinedRisk['low'])
```

Ilustração 38- Visualização do *ruleset* da rule2 – Risco baixo (*low*).

A ativação do sistema de controlo e do simulador com valores representativos do Objetivo e Apetite de risco correspondentes a um dos ativos do universo com respetivamente, Apetite de Risco de 9.4 e Objetivo de Risco de 7.8, permitiu a obtenção da figura seguinte onde se pode constatar que o modelo considera uma situação deste tipo

como de risco muito elevado o que é evidenciado de forma cabal no gráfico resultante, pela colocação da barra vertical negra resultante da simulação na zona correspondente a esse risco.

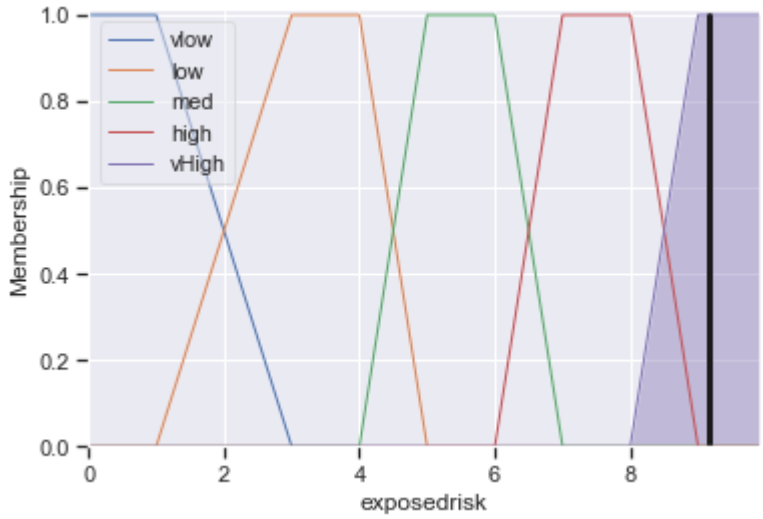


Ilustração 39- Resultado da simulação para um ativo com RiskApp=9.4 e RiskObj=7.8

Se considerarmos que as vulnerabilidades de cada um dos ativos que compõem um sistema de informação afetam esse mesmo ativo de acordo com o referido no início deste trabalho, e se considerarmos que a generalidade da informação disponibilizada relativamente às vulnerabilidades existentes permite obter a informação relativa ao *base score* $\overrightarrow{Vbs_i}$ e à *exploitability* $\overrightarrow{Ves_j}$, podemos considerar que o nível de exposição ao risco de um determinado ativo dum sistema de informação será constituído pelo somatório do máximo de cada um destes componentes, aplicados ao simulador que se apresentou e materializado na operação seguinte que mais não é que a operação *max* do conjunto de operadores lógicos sobre conjuntos difusos:

$$ExposedRisk_{\ asset\ k} = \sum_{i}^{j} (\overrightarrow{Vbs_{ij}}) \vee\ (\overrightarrow{Ves_{ij}})$$

Ou seja, o conjunto dos vetores componentes das vulnerabilidades existentes em cada um dos ativos permite determinar o nível de exposição e exploração de que esse mesmo ativo sofre em cada instante, sendo este nível equivalente aos máximos do conjunto de vulnerabilidades que afetam o ativo num determinado instante no tempo.

A eliminação de uma das vulnerabilidades de que sofre um determinado ativo determinará que o nível de exposição e exploração desse mesmo ativo será subtraído dos vetores correspondentes à vulnerabilidade eliminada.

A aplicação dos dois simuladores a um determinado de ativo permite obter de forma gráfica os níveis de exposição ao risco que afetam esse mesmo ativo representados nas figuras seguintes para o *host* C2388, alvo de maior numero de interações por parte do *redteam*.permite obter uma de forma gráfica os níveis de risco associados a esse mesmo ativo.

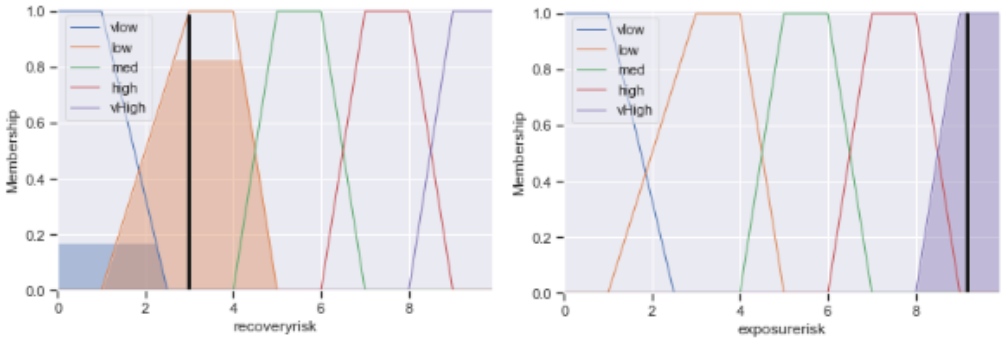


Ilustração 40- Recovery Risk e Exposure risk para o C2388

Assim podemos concluir que a utilização de modelos e simuladores com recurso à lógica de *fuzzy* é passível de ser utilizada para a obtenção de indicadores que permitam suportar a decisão, avaliar o nível de exposição ao risco dos sistemas de informação e determinar os níveis de impacto no negócio considerando o conjunto de vulnerabilidades que afetam cada um dos seus ativos, os objetivos corporativos de risco e o impacto no negócio da potencial falha de cada um desses ativos.

6.2. Análise baseada em *Data Mining* e *Machine Learning*

A disponibilidade de conjuntos abundantes de dados e a necessidade de transformar esse conjunto de dados em informação e essa informação em conhecimento é um dos princípios básicos para adquirir e manter a superioridade da informação.

Numa área onde a produção de dados é massiva e predominante e caracteristicamente *VUCA*[48] a utilização de ferramentas e técnicas que permitam ou possam

[48] *VUCA- Volatile, Uncertain, Complex and Ambiguous*

contribuir para adquirir e manter essa mesma superioridade de informação podem ser vantagens competitivas, neste caso particular, vantagens defensivas que permitam à organização proteger mais eficazmente os seus ativos.

A disponibilidade dos dados e das ferramentas que permitem suportar as análises e eventualmente extrair informação e conhecimento, podendo este último revestir-se das características preditivas e de *leading*[49] e *lagging indicators*[50] sobre os dados e os sistemas em que os mesmos são processados e o ambiente em que se efetuam as transações pode ajudar a suportar a vantagem competitiva que esta informação ou conhecimento permite.

Acresce que as metodologias e as ferramentas que permitem este tipo de análise estão, devido ao progressivo aumento das capacidades de processamento e ao menor custo da sua aquisição estão cada vez mais acessíveis.

Neste sentido foram realizadas várias análises sobre os dados disponíveis, utilizando a aplicação *Orange3*, disponível na *framework Anaconda* instalada para suportar o presente trabalho, para tentar obter, numa primeira fase quais as melhores metodologias que permitiam realizar este tipo de operações e depois quais os métodos que se poderiam considerar mais suscetíveis de produzir informação pertinente considerando o tipo de dados disponíveis.

O conjunto de dados disponível, considerando que era composto por dados numéricos e classes (ex. C2388, CVE-2018-11501) presta-se à utilização de métodos de classificação.

A *framework* implementa funções que permitem a construção de modelos de classificação, a sua avaliação e a classificação da precisão de cada um dos modelos. Estão disponíveis vários modelos tendo face ao conjunto e tipo de dados sido avaliados os seguintes: regressão logística, *k-nearest neighbors*, *support vector machines*, e *random forest.*

[49] *Leading Indicators* – indicadores que sinalizam eventos futuros
[50] Lagging indicators – indicadores que confirmam a existência de um padrão

Test & Score

Settings

Sampling type: Shuffle split, 10 random samples with 66% data
Target class: Average over classes

Scores

Method	AUC	CA	F1	Precision	Recall
Logistic Regression	0.776	0.186	0.106	0.105	0.186
Random Forest	0.984	0.848	0.838	0.848	0.848
SVM	0.902	0.564	0.526	0.629	0.564
Naive Bayes	0.997	0.715	0.745	0.883	0.715
Neural Network	0.922	0.559	0.529	0.548	0.559
kNN	0.809	0.444	0.419	0.424	0.444

Ilustração 41- Teste e classificação média dos diferentes modelos.

Os resultados da avaliação de performance de cada um dos classificadores, tal como se pode inferir da figura anterior é que os modelos com melhor desempenho, tendo em conta a média das diferentes classes, para este conjunto e tipo de dados foram: a rede neuronal, a *naive bayes* e a *random forest*.

Foram utilizados cinco parâmetros para esta avaliação, a saber: o AUC comparando as predições gravadas e os dados existentes no modelo de teste, o CA (*Accuracy Classification Score*) que permite determinar a precisão do subset de classes previsto numa predição o qual deve corresponder exatamente ao *subset* da amostragem, o F1 média ponderada da precisão e do *recall.*

A Precisão é definida como o rácio entre as identificações positivas e o somatório do total das identificações (positivas e falsas positivas). Permite determinar que percentagem das identificações positivas está de facto correta.

Recall ou Revisão é definida como o rácio entre as identificações positivas e o somatório do total das identificações positivas com os casos de falsos negativos

Todas estas métricas têm um intervalo entre zero e um e como melhor valor o um.

Para cada uma destas métricas é possível obter e selecionar os valores corretos e rejeitar os incorretos da matriz de confusão, que na imagem seguinte é representada pela matriz de confusão resultante da rede neuronal.

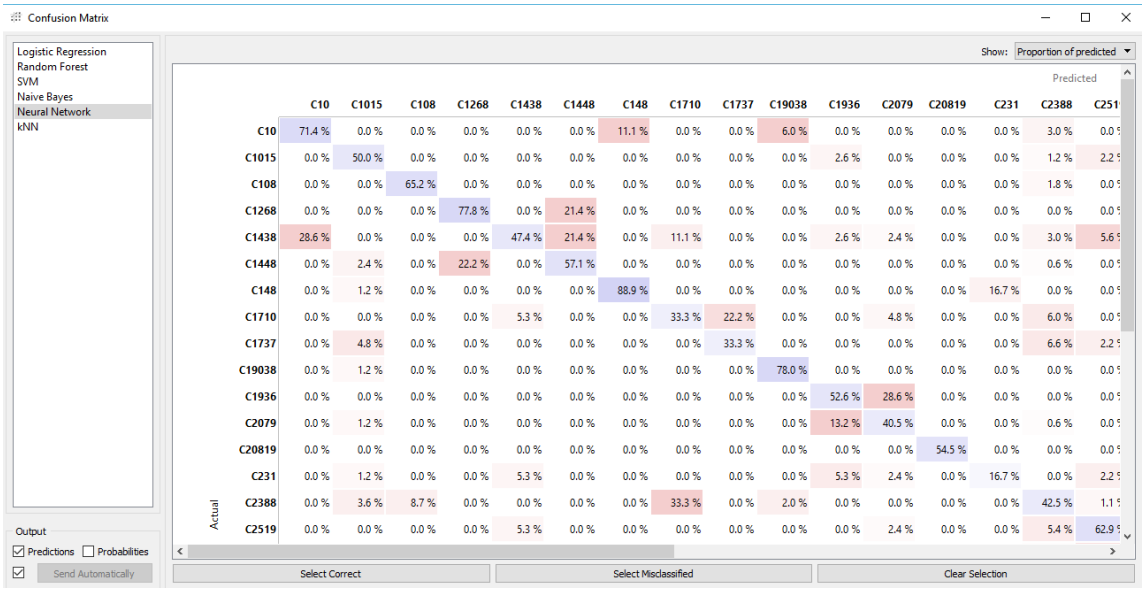


Ilustração 42- Matriz de confusão da neural network.

Realizada a análise das curvas *ROC* (*Receiver Operating Curve*) obtidas para cada um dos modelos foi possível apurar a imagem da figura seguinte.

Com referido anteriormente as curvas ROC podem ser usadas para avaliar classificadores devendo, contudo, ser usadas com parcimónia quando se pretende tirar conclusões sobre a superioridade de um classificador face a outro. Esta análise simplista pode ser enganadora pois sem a informação da variância não se poderá fazer essa comparação (Fawcett, 2003).

A imagem abaixo mostra que o modelo *random forest* é aquele que neste caso, tem melhor desempenho face respetivamente à rede neuronal e ao *naive bayes*, estando representada a análise para o C2388.

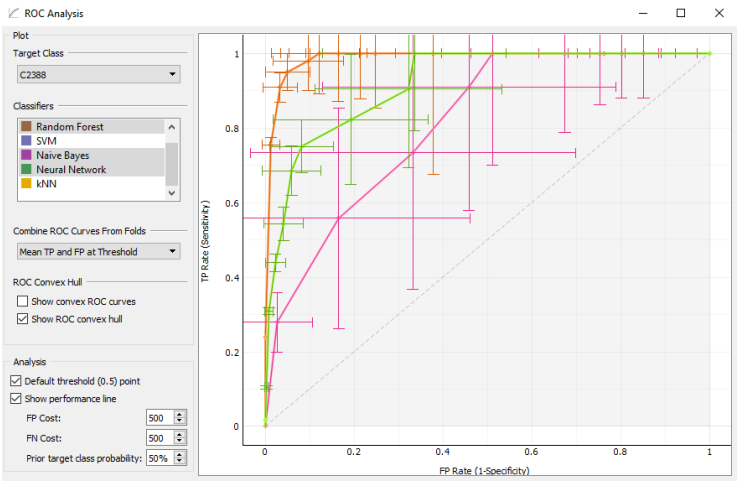


Ilustração 43- Análise comparada do ROC para o computador C2388

A curva *lift* mostra a relação entre o número de instâncias que foram preditas positivamente e aquelas que eram efetivamente positivas, medindo assim diretamente a performance dum classificador face a um classificador *random.*

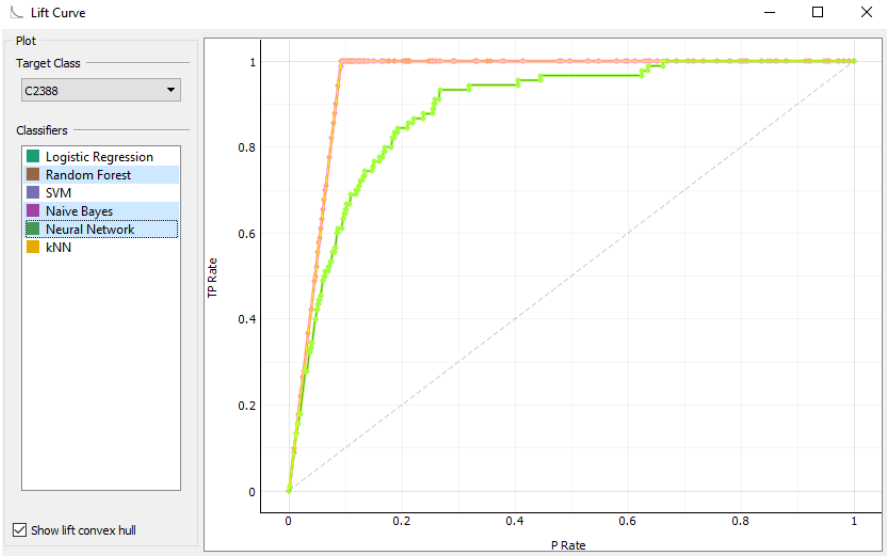


Ilustração 44- Análise comparada da curva *Lift* para os diferentes modelos para o computador C2388.

Por último foi feita a análise dos *calibration plots* dos três classificadores, os quais permitem aferir as probabilidades das diferentes classes face aquelas que foram objeto de predição pelos classificadores.

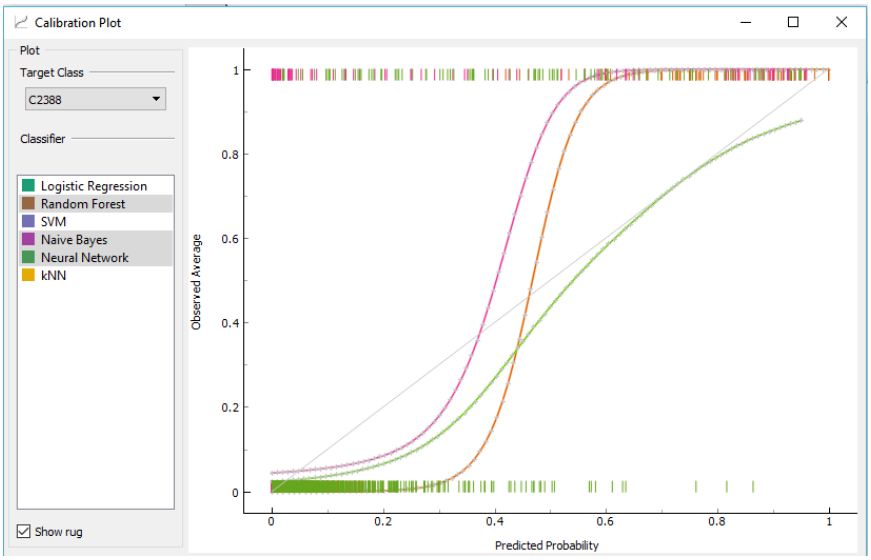


Ilustração 45- Resultados dos *Calibration plots* para o computador C2388 dos diferentes modelos.

Considerando os dados disponíveis foi gerado um *heatmap*, com a distribuição dos diferentes ativos e os respetivos scores permitindo visualizar de forma intuitiva as características mais relevantes destes ativos, associar-lhes uma imagem e um gradiente de

cor e assim permitir facilmente identificar quais os que do ponto de vista da decisão poderiam requerer uma intervenção mais imediata.

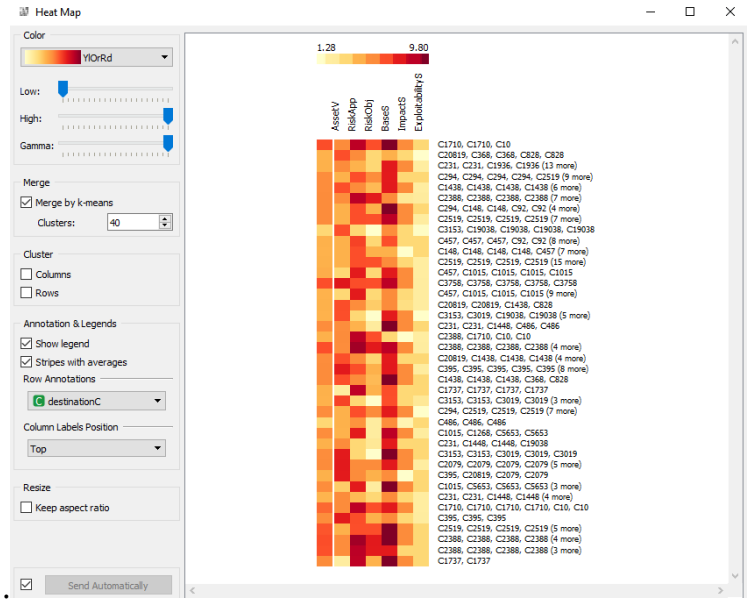


Ilustração 46- *Heatmap* dos ativos, com representação em gradiente de cor dos valores da exposição dos ativos e respetivas características *AssetV, RiskApp, RiskObj, BaseS, ImpactS e ExploitabilityS.*

Implementado o *workflow* seguinte foi possível comparar os resultados das predições dos três modelos selecionados, análise esta que é como sabemos, condicionada pelo tipo de dados que estamos a analisar, sendo que no caso presente foram utilizados aqueles que depois da análise realizada anteriormente obtiveram melhor performance face ao conjunto e tipos e dados a tratar.

Assim utilizando um *data sampler*, sobre o conjunto de dados disponíveis, com um tipo de amostragem de proporção de dados fixa no valor de 66% submeteram-se os mesmos aos três diferentes modelos preditivos, que obtiveram melhores resultados, tal como descrito anteriormente.

Naive Bayes:

Rede neuronal:

Nós nos níveis escondidos:100;

Activation: ReLu

Solver:Adam;

Regularização:0,0001;

Numero máximo de Iterações:200;

Random Forest:

Numero de arvores:100;

Numero de atributos considerados em cada split:5;

Fixed seed for random generator:1;

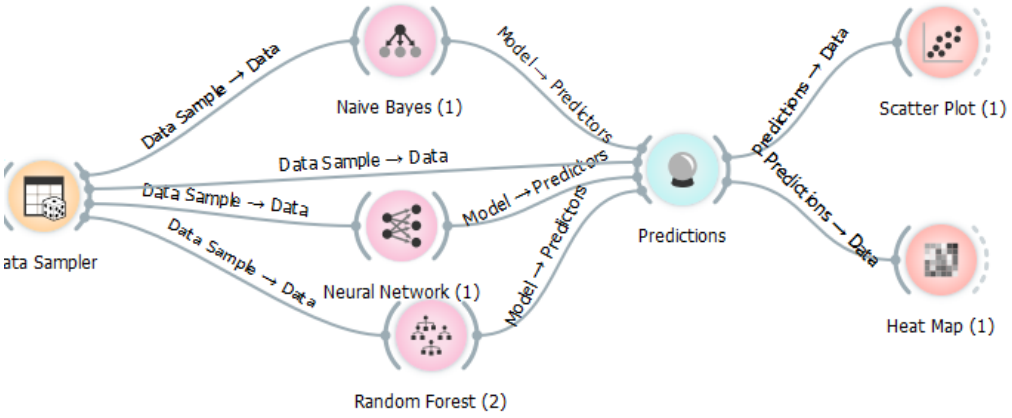
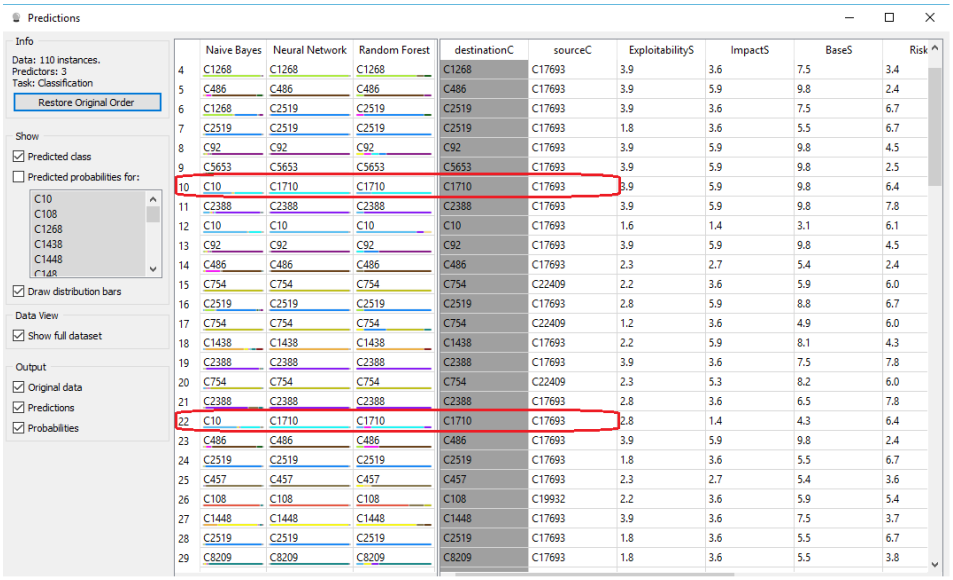


Ilustração 47- *Workflow* utilizado para a predição utilizando os três algoritmos avaliados com melhor performance.

Os resultados previstos pelos três algoritmos foram os representados (parcialmente) na imagem seguinte, tendo apenas em dois casos as predições divergido e apenas nos resultados fornecidos pelo modelo *Naive Bayes*, relativamente ao *host* c1710.



	Naive Bayes	Neural Network	Random Forest	destinationC	sourceC	ExploitabilityS	ImpactS	BaseS	Risk
4	C1268	C1268	C1268	C1268	C17693	3.9	3.6	7.5	3.4
5	C486	C486	C486	C486	C17693	3.9	5.9	9.8	2.4
6	C1268	C2519	C2519	C2519	C17693	3.9	3.6	7.5	6.7
7	C2519	C2519	C2519	C2519	C17693	1.8	3.6	5.5	6.7
8	C92	C92	C92	C92	C17693	3.9	5.9	9.8	4.5
9	C5653	C5653	C5653	C5653	C17693	3.9	5.9	9.8	2.5
10	C10	C1710	C1710	C1710	C17693	3.9	5.9	9.8	6.4
11	C2388	C2388	C2388	C2388	C17693	3.9	5.9	9.8	7.8
12	C10	C10	C10	C10	C17693	1.6	1.4	3.1	6.1
13	C92	C92	C92	C92	C17693	3.9	5.9	9.8	4.5
14	C486	C486	C486	C486	C17693	2.3	2.7	5.4	2.4
15	C754	C754	C754	C754	C22409	2.2	3.6	5.9	6.0
16	C2519	C2519	C2519	C2519	C17693	2.8	5.9	8.8	6.7
17	C754	C754	C754	C754	C22409	1.2	3.6	4.9	6.0
18	C1438	C1438	C1438	C1438	C17693	2.2	5.9	8.1	4.3
19	C2388	C2388	C2388	C2388	C17693	3.9	3.6	7.5	7.8
20	C754	C754	C754	C754	C22409	2.3	5.3	8.2	6.0
21	C2388	C2388	C2388	C2388	C17693	2.8	3.6	6.5	7.8
22	C10	C1710	C1710	C1710	C17693	2.8	1.4	4.3	6.4
23	C486	C486	C486	C486	C17693	3.9	5.9	9.8	2.4
24	C2519	C2519	C2519	C2519	C17693	1.8	3.6	5.5	6.7
25	C457	C457	C457	C457	C17693	2.3	2.7	5.4	3.6
26	C108	C108	C108	C108	C19932	2.2	3.6	5.9	5.4
27	C1448	C1448	C1448	C1448	C17693	3.9	3.6	7.5	3.7
28	C2519	C2519	C2519	C2519	C17693	1.8	3.6	5.5	6.7
29	C8209	C8209	C8209	C8209	C17693	1.8	3.6	5.5	3.8

Ilustração 48- Resultados das predições dos três algoritmos.

O *scatter plot* da figura seguinte representa as previsões geradas pelo modelo *Naive Bayes* onde se pode constatar que a generalidade dos ataques é desenvolvida a partir do

host C17693 tendo como alvos os *hosts* representados no canto inferior direito e sendo as principais vulnerabilidades exploradas as constantes da legenda no canto superior direito.

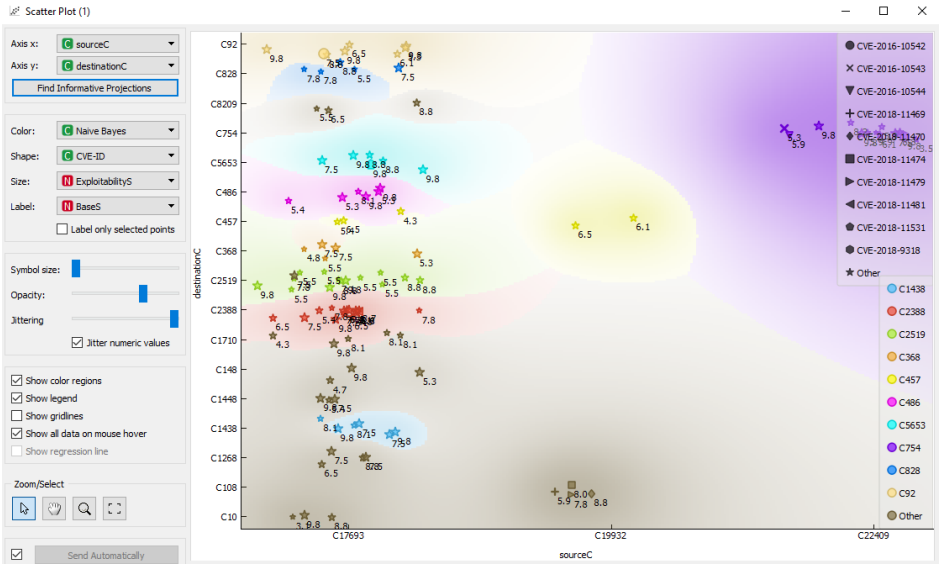


Ilustração 49- *Scatter plot* de predições do algoritmo *Naive Bayes*

O *heatmap* seguinte mostra os ativos com ataques previstos como consequência das análises anteriores e os respetivos scores.

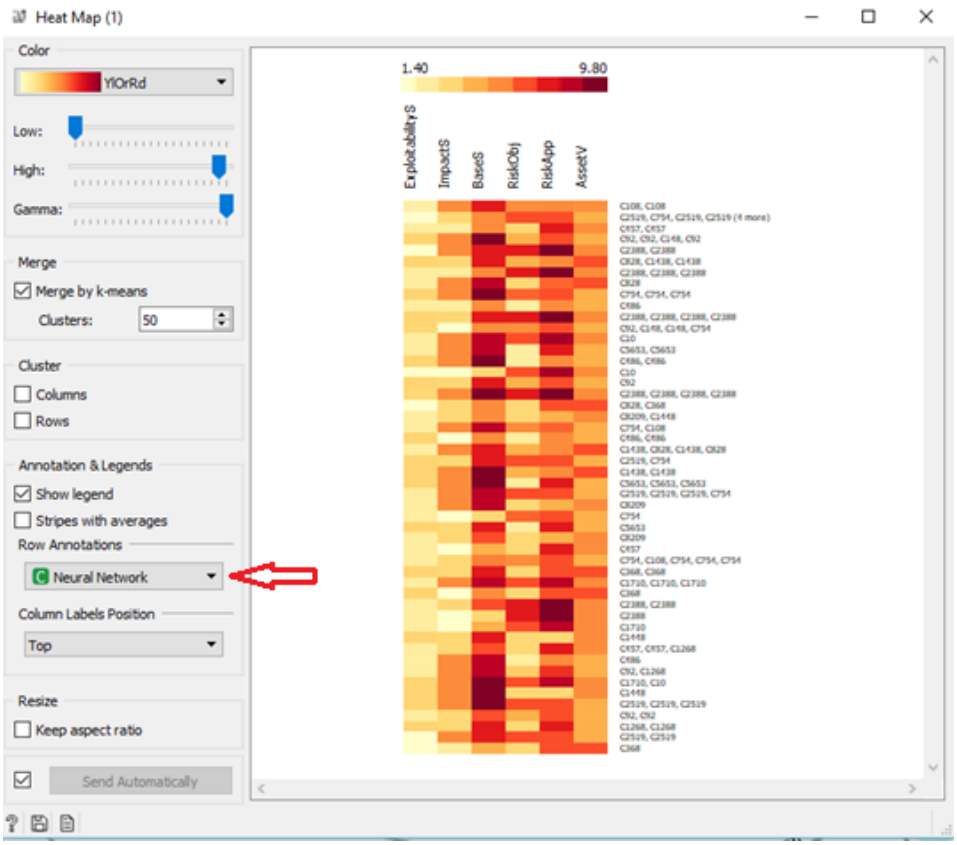


Ilustração 50- *Heatmap* dos ativos com os ataques previstos pela rede neuronal.

A intensidade cromática mais escura representa os ativos e as respetivas métricas resultantes das vulnerabilidades que os afetam (três primeiras colunas), dos níveis de objetivos de risco e apetite de risco (colunas quatro e cinco) e do valor do respetivo ativo (sexta coluna). Na legenda esquerda está representado o número de ataques previsto pela rede neuronal para cada ativo.

6.3. Resultados globais agregados

Os resultados dos *workflows* descritos anteriormente e o *workflow* global resultante estão representados na figura seguinte.

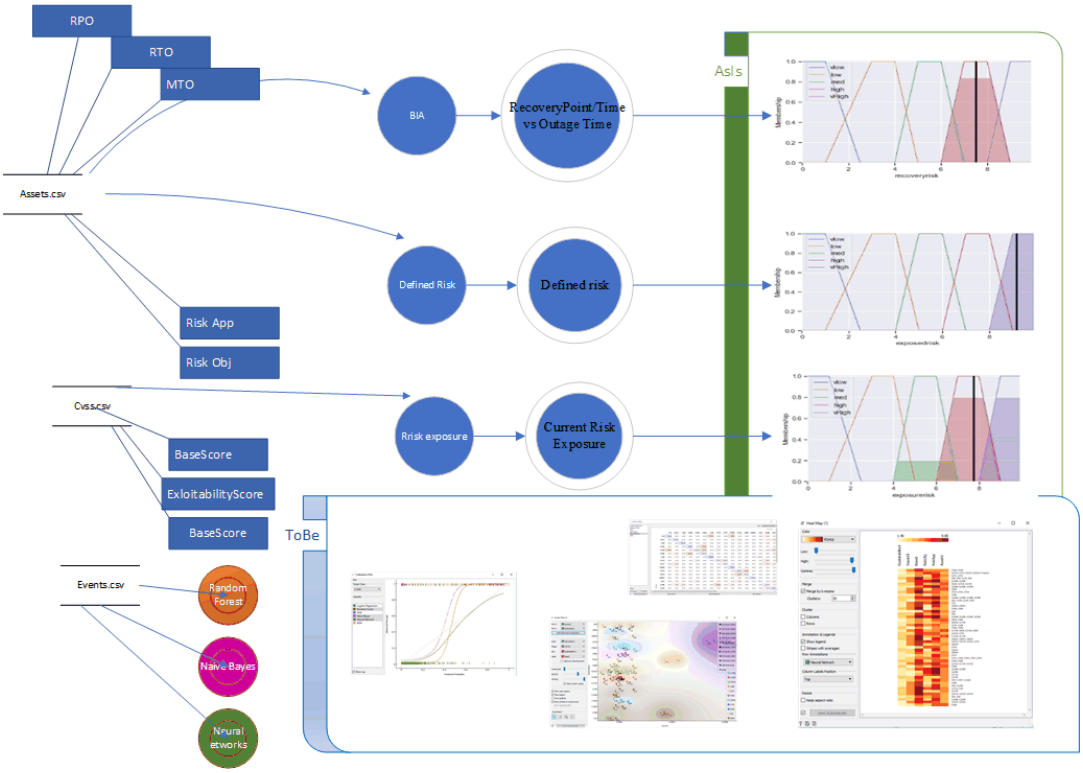


Ilustração 51- *Workflow* global agregado dos resultados do projeto.

Nesta figura é possível perceber os resultados obtidos que contribuem para o estado atual em termos de gestão de vulnerabilidades e risco, agregado na moldura verde com a designação de *AsIs (situação atual)*, onde é possível ter uma perceção dos diferentes níveis correntes de risco (*RecoveryRisk, DefinedRisk e ExposureRisk*).

Na moldura *ToBe* (situação futura) estão representados os resultados das análises resultantes dos diferentes classificadores com a representação da performance dos mesmos, matriz de confusão, *scatter plot* de predição de ataques e *heamap* com os ativos com ataques previstos em consequência das análises anteriores.

Capítulo 7
Conclusões e trabalho futuro

7.1. Conclusões decorrentes do trabalho realizado

Podemos afirmar que os resultados obtidos com o trabalho realizado permitiu concluir que a utilização de modelos e simuladores com recurso à lógica difusa é passível de ser utilizada para a obtenção de indicadores que permitam suportar a decisão, avaliar o nível de exposição ao risco dos sistemas de informação e determinar os níveis de impacto no negócio considerando o conjunto de vulnerabilidades que afetam cada um dos seus ativos, os objetivos corporativos de risco e o impacto no negócio da exploração das vulnerabilidades existentes em cada um desses ativos.

A informação produzida poderá também ser utilizada para a tomada de decisões relativamente a prioridades de intervenção nos ativos ou sistemas operacionais, possibilitando a comparação entre os níveis de exposição ao risco de cada um dos ativos e oferecendo ao decisor a informação pertinente para a atribuição de prioridades no processo de decisão, utilizando os dois tipos de interface disponibilizados, *heatmaps* e gráficos.

Foi possível categorizar diferentes níveis de exposição ao risco e de impacto no negócio e ainda obter indicadores comparativos desse mesmo nível de exposição com os objetivos de risco, dos diversos ativos corporativos, aferir a criticidade dos mesmos face aos objetivos corporativos de risco e contribuir desta forma para uma gestão proactiva do nível de exposição e da segurança de informação da organização.

Os modelos e simuladores utilizados, baseados em tecnologias não proprietárias e em linguagens de programação, populares, com desempenhos elevados, disponibilizando API´s[51] perfeitamente adaptadas à web, podem constituir uma *framework* que suportará uma solução deste tipo, permitindo implementá-la com uma amplitude *end to end*, Isto significa uma mesma linguagem e *framework* desde a recolha da informação, respetivo processamento, análise, classificação, produção de indicadores e apresentação dessa mesma informação e desses mesmos indicadores, com as inerentes economias de escala e permitindo disponibilizá-los nas mais diversas plataformas e formatos, incluindo interfaces web e mobile.

[51] *API-Aplication Programing Interface – conectores definidos e específicos que permitem conectar uma aplicação ou serviço a outras aplicações ou serviços.*

Tudo isto ainda com a vantagem de poderem ser facilmente autonomizados, serem não proprietários e poderem ser aplicados em contexto de situação real sem necessidade de grandes investimentos. No anexo 9§ 9.4 e 9.5 é possível ver uma *POC*[52] da visualização dos resultados respetivamente, embebido na *framework jupyter* e através de acesso web com recurso a uma *API* e à livraria *plotly.*

Foi também possível realizar através dum conjunto de ferramentas de análise gráfica, a modelação dos dados e avaliar que tipo de modelo preditivo melhor responderia ao conjunto de dados utilizados, atentas as características especificas dos mesmos. Foram treinados e avaliados os diferentes modelos, selecionados os que obtiveram melhores resultados na avaliação comparada e obtiveram-se modelos e indicadores preditivos relativamente às potenciais ameaças aos ativos da organização, considerando-se que nesta área se terá ainda de realizar trabalho adicional, nomeadamente o que inclua a alimentação de dados em tempo-real e eventualmente algum trabalho de afinação dos parâmetros dos diferentes modelos por forma a garantir que os mesmos conservam as capacidades de aprendizagem..

Ponto relevante é que estes modelos preditivos podem ser utilizados de forma dinâmica uma vez que as funcionalidades da *framework* permitem a seleção da propagação automática de eventos o que permite que o adicionar de um novo evento ao conjunto de dados reinicie o processo de recalculo automático de todos os nós/modelos do respetivo *workflow* e a propagação de resultados para as visualizações.

Como exemplo do referido teremos o caso em que o conjunto de dados de entrada esteja a ser atualizado com os dados provenientes do *tail* de um ficheiro de log, ou seja, com os eventos de sistema mais recentes

Por último refira-se que o modelo e os indicadores produzidos são autónomos e independentes e podem ser implementados de forma progressiva.

7.2. Linhas de Investigação futura

Os resultados conseguidos permitiram concluir que existe potencial na informação que foi possível gerar, na utilização da mesma para suportar decisões e que se entende que ainda será possível otimizar quer os modelos utilizados quer as potencialidades dos indicadores gerados, e de outros que se estima que também possam ser produzidos por

[52] *POC-Proof of Concept* -Prova de conceito

processo semelhantes e que permitam melhorar a qualidade da informação obtida, para o suporte ao processo de decisão.

Entende-se que foi possível gerar informação pertinente para o processo de decisão, no contexto particular da segurança da informação, gestão de vulnerabilidades e do risco e que a melhoria da mesma poderá contribuir para o suporte à decisão nesta área.

A otimização dos processos de avaliação, deteção e predição é uma linha de investigação a explorar.

Outra das áreas onde se poderá prosseguir o trabalho é o da integração dos diferentes indicadores produzidos, em *dashboards* únicos, melhorando a perceção situacional e do processo de decisão. Este objetivo apenas foi atingido parcialmente pois no decurso dos trabalhos realizados, não foi possível produzir um *dashboard* único que permitisse uma visão integrada dos diferentes indicadores produzidos. Estas visualizações poderão ser integradas num único *dashboard* num trabalho futuro.

Capítulo 8

Referências Bibliográficas

ABREU, Francisco - **Fundamentos de estratégia militar e empresarial**. [S.l.] : Edições Silabo, 2002. ISBN 9789726182757.

ALBERTS, David S.; GARSTKA, Jj; STEIN, Frederick P. - **Networking Centric Warfare -Developing Information Superiority**. ISBN 1-57906-019-6.

ALBERTS, David S.; HAYES, Richard E. - **Power to the Edge: Command..Control..in the Information Age**. ISBN 1893723135.

BORGES, José Alberto De Jesus - Metodologias e Técnicas de Apoio à Decisão. 2015).

BRANCH, Info Ops - **Concept of Operations Information Operations (Info Ops) in Support of Effects-Based Operations (EBO)**

BREIMAN, Leo (UC Berkeley) - Random forests. **Kluwer Academic Publishers**. . ISSN 1478-7954. 45:2001) 27. doi: 10.1186/1478-7954-9-29.

CANSO - CANSO Cyber Security and Risk Assessment Guide. **CANSO**. 2014).

CHEN, Tao *et al.* - Improving sentiment analysis via sentence type classification using BiLSTM-CRF and CNN. **Expert Systems with Applications**. . ISSN 09574174. 72:2017) 221–230. doi: 10.1016/j.eswa.2016.10.065.

CHENG, Y. *et al.* - Metrics of security. **Advances in Information Security**. . ISSN 15682633. 62:2014) 263–295. doi: 10.1007/978-3-319-11391-3_13.

CISSP - Business Continuity or Disaster Recovery Planning Domain. **CISSP Common Body of Knowledge**. 2012).

ENDSLEY, Mica R. - Theoretical Underpinnings of Situation Awareness: A Critical Review. **Situation Awareness Analysis and Measurement**. . ISSN 02726963. 2000) 3–32. doi: 10.1016/j.jom.2007.01.015.

ENISA - **ENISA Threat Landscape Report 2016: 15 Top Cyber-Threats And Trends** [Em linha] Disponível em WWW:<URL:https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2016-report-cyber-threats-becoming-top-priority%0Ahttps://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016%0A>. ISBN 9789292042028.

FAWCETT, Tom - ROC Graphs - Notes and Pratical Considerations for Data Mining Researchers. **HP Laboratories Palo Alto**. 2003). doi: 10.1.1.10.9777.

FAYYAD, Usama; PIATETSKY-SHAPIRO, Gregory; SMYTH, Padhraic - From data

mining to knowledge discovery in databases. **Advances in Knowledge Discovery and Data Mining**. 17:3 (1996) 1–36.

FIRST - Common Vulnerability Scoring System v3.0: Specification Document. **Forum of Incident Response and Security Teams (FIRST)**. July (2015) 1–21.

GAI, Keke; QIU, Meikang; ELNAGDY, Sam Adam - Security-Aware Information Classifications Using Supervised Learning for Cloud-Based Cyber Risk Management in Financial Big Data. **Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and S**. 2016) 197–202. doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.66.

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aron - **Deep Learning**

HAN, Jiawei; KAMBER, Micheline; PEI, Jain - **Data Mining – Concepts & Techniques**. ISBN 9780123814791.

ISO/IEC 27000:2009 - Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. **ISO/IEC**. 2009).

ISO/IEC 27001:2013 - Information Technology — Security Techniques — Information Security Management Systems — Requirements. **ISO/IEC**. 2013).

ISO/IEC 27005:2011 - Information Tecnology - Security Techniques - Information Security Risk Management. **ISO/IEC**. 2011) 1–68.

JOH, HyunChul; MALAIYA, Yashwant K. - Defining and assessing quantitative security risk measures using vulnerability lifecycle and cvss metrics. **International conference on security and management (SAM)**. 1 (2011) 10–16.

KEEN, Peter G. W. - Decision Support Systems: A Research Perspective. 1980).

KEIM, Daniel A. *et al.* - Visual analytics: Scope and challenges. **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**. . ISSN 03029743. 4404 LNCS:4404 (2008) 76–90. doi: 10.1007/978-3-540-71080-6_6.

KINGMA, P. Diedrik; LEI BA, Jimmy - Adam - A method for Stochastic Optimization. **Energy Education Science and Technology Part B: Social and Educational Studies**. . ISSN 13087711. 5:2 (2013) 365–380. doi: 10.1063/1.4902458.

KOSUB, Thomas - Components and challenges of integrated cyber risk management. **Zeitschrift fur die gesamte Versicherungswissenschaft**. . ISSN 18659748. 104:5 (2015) 615–634. doi: 10.1007/s12297-015-0316-8.

MITRE - **CAPEC - About CAPEC** [Em linha] [Consult. 18 fev. 2018]. Disponível em WWW:<URL:https://capec.mitre.org/about/index.html>.

MITRE - **CVE - Common Vulnerabilities and Exposures** [Em linha], atual. 2016. [Consult. 18 fev. 2018]. Disponível em WWW:<URL:https://cve.mitre.org/>.

MOYLE, E.; LOEB, M. - State of cyber security 2017: Part 2 - current trends in the threat landscape. October 2016 (2017) 22.

NCSC - The cyber threat to UK business. **NCSC**. 2017) 24.

NCSC - The cyber threat to UK business. 2017) 24.

NOEL, Steven; JAJODIA, Sushil - Metrics suite for network attack graph analytics. **Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR '14**. 10:2014) 5–8. doi: 10.1145/2602087.2602117.

NVD - Vulnerability Metrics - [Em linha] [Consult. 18 fev. 2018]. Disponível em WWW:<URL:https://nvd.nist.gov/vuln-metrics>.

ÖĞÜT, Hulisi; RAGHUNATHAN, Srinivasan; MENON, Nirup - Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. **Risk Analysis**. . ISSN 02724332. 31:3 (2011) 497–512. doi: 10.1111/j.1539-6924.2010.01478.x.

OLSTIK, Jhon; ESG - the Big Data Security Analytics Era Is Here. **Enterprise Strategy Group**. 2013) 8–11.

ORTALO, Rodolphe; DESWARTE, Yves; KAâNICHE, Mohamed - Experimenting with quantitative evaluation tools for monitoring operational security. **IEEE Transactions on Software Engineering**. . ISSN 00985589. 25:5 (1999) 633–650. doi: 10.1109/32.815323.

PORTER, Michel E.; MILLAR, Victor E. - How Information Gives You Competitive Advantage. **Harvard Business Review**. 79201 (1985).

SHARP, Walter - Joint Publication 3-13 Information Operations. **US Department of Defense Joint Publication**. February (2006) 117.

SHUKLA, Anshu; CHATURVEDI, Shilpa; SIMMHAN, Yogesh - A Review on Internet of Things, Internet of Everything and Internet of Nano Things. **International Journal of Computer Applications (0975 8887)**. . ISSN 26269326. 113:1 (2017) 1–7. doi: 10.5120/19787-1571.

STANTON, N. A.; CHAMBERS, P. R. G.; PIGGOTT, J. - Situational awareness and safety. **Safety Science**. . ISSN 09257535. 39:3 (2001) 189–204. doi: 10.1016/S0925-7535(01)00010-8.

TAVANA, Madjid; TREVISANI, Dawn A.; KENNEDY, Dennis T. - A Fuzzy Cyber-Risk

Analysis Model for Assessing Attacks on the Availability and Integrity of the Military Command and Control Systems. **Research Methods**. 2015) 1231–1245. doi: 10.4018/978-1-4666-7456-1.ch053.

WALTZ, Edward **- Information warfare principles and operations**. ISBN 089006511X.

WANG, Lingyu; LIU, Anyi; JAJODIA, Sushil - Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts. **Computer Communications**. . ISSN 01403664. 29:15 (2006) 2917–2933. doi: 10.1016/j.comcom.2006.04.001.

WEBB, J. - Towards intelligence-driven information security risk management: an intelligent information security method. 2015) 0–3.

YARGER, Harry R. - **Strategic Theory for the 21st Century: The Little Book on big Strategy**. ISBN 1584872330.

ZHOU, Chenfeng Vincent; LECKIE, Christopher; KARUNASEKERA, Shanika - A survey of coordinated attacks and collaborative intrusion detection. **Computers and Security**. . ISSN 01674048. 29:1 (2010) 124–140. doi: 10.1016/j.cose.2009.06.008.

Capítulo 9

Anexos

9.1. Script para dividir os ficheiros em blocos mais facilmente acessíveis

Split huge dataframes (cont.)

In [24]:

```
import os
import csv

with open("C:\datasets\LANL\datafiles\outputAuth.csv") as f:
    buf = f.read() #.decoode('utf-8')
header, chunk = buf.split('\n', 1)

block_size = 200000
block_start = 0
counter = 0
while True:
    counter += 1
    filename = 'C:\datasets\LANL\datafiles\splits\outA\part_outA%03d.csv' % counter
    block_end = chunk.find('\n', block_start + block_size)
    print (filename, block_start, block_end)

    with open(filename, 'w') as f:
        f.write(header + '\n')
        if block_end == -1:
            f.write(chunk[block_start:]) #.encoode('utf-8'))

        else:
            f.write(chunk[block_start:block_end]) #.encode('utf-8'))
        f.write('\n')


    block_start = block_end + 1
    if block_end == -1: break
```

```
C:\datasets\LANL\datafiles\splits\outP\part_outP001.csv 0 200011
C:\datasets\LANL\datafiles\splits\outP\part_outP002.csv 200012 400028
C:\datasets\LANL\datafiles\splits\outP\part_outP003.csv 400029 600034
C:\datasets\LANL\datafiles\splits\outP\part_outP004.csv 600035 800063
C:\datasets\LANL\datafiles\splits\outP\part_outP005.csv 800064 1000079
C:\datasets\LANL\datafiles\splits\outP\part_outP006.csv 1000080 1200096
C:\datasets\LANL\datafiles\splits\outP\part_outP007.csv 1200097 1400104
C:\datasets\LANL\datafiles\splits\outP\part_outP008.csv 1400105 1600116
C:\datasets\LANL\datafiles\splits\outP\part_outP009.csv 1600117 1800122
C:\datasets\LANL\datafiles\splits\outP\part_outP010.csv 1800123 2000151
C:\datasets\LANL\datafiles\splits\outP\part_outP011.csv 2000152 2200152
C:\datasets\LANL\datafiles\splits\outP\part_outP012.csv 2200153 2400174
```

9.2. Dados recolhidos para o conjunto de dados adicional CVSS

CVE-2018-16429 Detail

Current Description

GNOME GLib 2.56.1 has an out-of-bounds read vulnerability in g_markup_parse_context_parse() in gmarkup.c, related utf8_str().

Source: MITRE
Description Last Modified: 09/03/2018
View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 7.5 HIGH
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H (V3 legend)
Impact Score: 3.6
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): None
Integrity (I): None
Availability (A): High

CVSS v2.0 Severity and Metrics:
Base Score: 5.0 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:P) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 10.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): None
Confidentiality (C): None
Integrity (I): None
Availability (A): Partial
Additional Information:
Allows disruption of service

9.3. Condicionantes decorrentes da volatilidade dos componentes da solução

```
IPython 7.1.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: import pandas_datareader
---------------------------------------------------------------------------
ImportError                               Traceback (most recent call last)
<ipython-input-1-a918617b42da> in <module>
----> 1 import pandas_datareader

~\Anaconda3\envs\tese\lib\site-packages\pandas_datareader\__init__.py in <module>
```

```
ImportError: cannot import name 'is_list_like'

In [2]: import pandas as pd

In [3]: pd.core.common.is_list_like = pd.api.types.is_list_like

In [4]: import pandas_datareader as pdreader
```

A solution **without** changing any files locally and **bypass** the version control of your package manager (pip) is to define *is_list_like* like this:

```
import pandas as pd
pd.core.common.is_list_like = pd.api.types.is_list_like
```

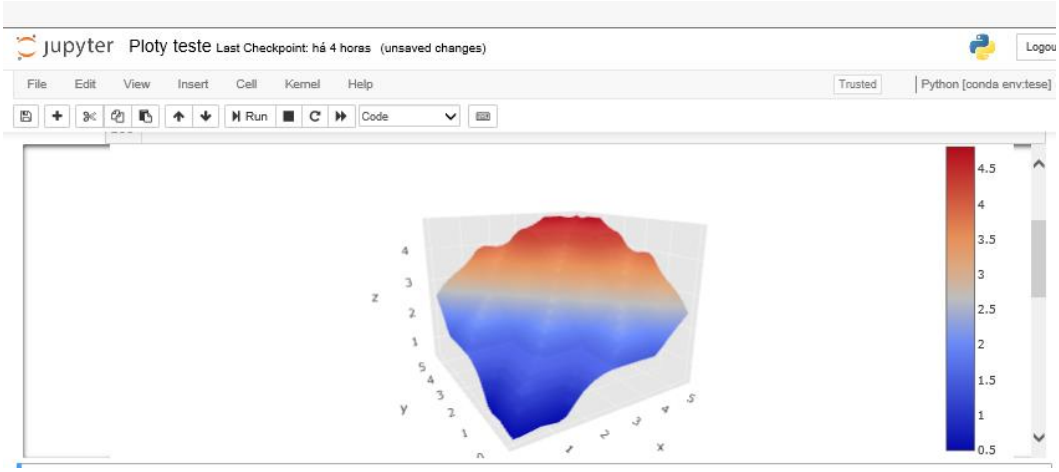
right before

```
import pandas_datareader as web
```

Furthermore this problem will be fixed in pandas_datareader version 0.7.0 release.

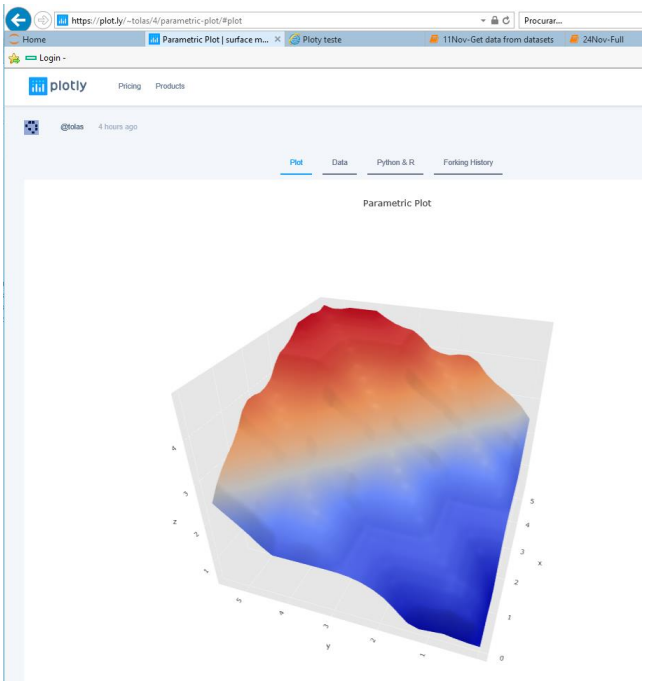
Name	T	Description	Version
pandas		High-performance, easy-to-use data structures and data analysis tools.	0.23.4
pandas-datareader		Up to date remote data access for pandas, works for multiple versions of pandas	0.7.0

9.4. API *plotly* embebida na *framework Jupyter*



Disponibilização embebida na *framework Jupyter* do espaço de resultados "*RecoveryTime*"

9.5. Interfaces web utilizando a API *plotly*



Disponibilização via web browser do espaço de resultados "*RecoveryTime*" em 'https://plot.ly/~tolas/4'