UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Fabio André Barcelos

UM PROCESSO DE SUPORTE E TOMADA DE DECISÃO NO TRATAMENTO DE INCIDENTES DE SEGURANÇA

Santa Maria, RS
2020

Fabio André Barcelos

UM PROCESSO DE SUPORTE E TOMADA DE DECISÃO NO TRATAMENTO DE INCIDENTES DE SEGURANÇA

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação(PPGCC) da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Mestre em Ciência da Computação**.

Orientador: Prof. Dr. Raul Ceretta Nunes

Co-orientador: Prof. Dr. Luis Alvaro de Lima Silva

Santa Maria, RS

2020

Barcelos, Fabio André

Um Processo de Suporte e Tomada de Decisão no Tratamento de Incidentes de Segurança / por Fabio André Barcelos. – 2020.
88 f.: il.; 30 cm.

Orientador: Raul Ceretta Nunes
Co-orientador: Luis Alvaro de Lima Silva
Dissertação (Mestrado) - Universidade Federal de Santa Maria, Centro de Tecnologia, Pós-Graduação em Ciência da Computação, RS, 2020.

1. Tratamento de Incidentes. 2. IODEF. 3. STIX. 4. CBR. I. Nunes, Raul Ceretta. II. Silva, Luis Alvaro de Lima. III. Título.

E-mail: fabio@cpd.ufsm.br

Fabio André Barcelos

UM PROCESSO DE SUPORTE E TOMADA DE DECISÃO NO TRATAMENTO DE INCIDENTES DE SEGURANÇA

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação(PPGCC) da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Mestre em Ciência da Computação**.

Aprovado em 27 de Novembro de 2020:

Raul Ceretta Nunes, Dr. (UFSM)
(Presidente/Orientador)

Carlos Raniery Paula dos Santos, Dr. (UFSM)

Eduardo Luzeiro Feitosa, Dr. (UFAM)

Santa Maria, RS

2020

DEDICATÓRIA

À minha amada esposa Lilian e à minha filha (princesa) Maria Fernanda, por todo amor, incentivo, apoio e compreensão. Nada disso teria sentido se vocês não existissem na minha vida.
À minha mãe, Cleci, por sempre acreditar em mim e por ter abdicado de sua vida em prol das realizações e da felicidade de seus filhos.

AGRADECIMENTOS

A Deus por me proporcionar perseverança em todos os momentos da minha vida.

Ao Prof. Raul, pela orientação, competência, profissionalismo, dedicação e por todos os valiosos apoios e incentivos durante o período do mestrado. Obrigado por acreditar em mim e pelos tantos incentivos. Os seus ensinamentos foram imprescindíveis para o alcance do objetivo final, a conclusão do mestrado.

A minha amada filha, princesa e amiga ***Maria Fernanda Barcelos*** *por ter paciência e estar ao meu lado durante toda esta etapa.*

A minha esposa, amor e melhor amiga ***Lilian Barcelos*** *por estar ao meu lado durante esta caminhada, sempre solícita e carinhosa, presente em todos os momentos.*

A minha mãe, ***Cleci Ilha Barcelos****, pelo amor, carinho e incentivo incondicional.* E a minha irmã querida, sempre pronta a me apoiar em tudo nesta vida.

À minha família, e aos meus sogros, por apoiarem e compreenderem o meu isolamento em inúmeros finais de semana.

Aos amigos e colegas de trabalho que me ajudaram nesta etapa.

A todos os ***professores*** *que compartilharam seus conhecimentos comigo.*

À ***Universidade Federal de Santa Maria*** *por proporcionar um estudo gratuito de qualidade e excelência aos estudantes.*

Por fim, a todos aqueles que contribuíram, direta ou indiretamente, para a realização desta dissertação, o meu sincero agradecimento.

“A dor é passageira, mas a glória é para sempre!”

(CIAAR – CENTRO DE INSTRUÇÃO E ADAPTAÇÃO DA AERONÁUTICA)

RESUMO

UM PROCESSO DE SUPORTE E TOMADA DE DECISÃO NO TRATAMENTO DE INCIDENTES DE SEGURANÇA

AUTOR: FABIO ANDRÉ BARCELOS
ORIENTADOR: RAUL CERETTA NUNES
CO-ORIENTADOR: LUIS ALVARO DE LIMA SILVA

Muitas organizações mantêm uma equipe de resposta a incidentes para mitigar os danos causados por incidentes e restaurar imediatamente os serviços digitais. Contudo, poucas delas aprendem com as experiências passadas de uma maneira sistemática que lhes permitam não apenas responder a incidentes de segurança na organização, mas gerir este conhecimento. Além disso, existe uma deficiência de profissionais experientes na área de segurança. Neste sentido, a técnica de raciocínio baseado em casos tem sido aplicada na recuperação de planos de tratamento de incidentes. Este trabalho revisita esta abordagem e propõe um processo com melhorias para sua melhor eficiência: uma nova maneira de categorizar incidentes com base em categorias internacionais e nos padrões IODEF e STIX, o que contribui no mapeamento de incidentes para ferramentas de tratamento de incidentes; e o uso de diferentes funções de similaridade para aumentar a precisão de recuperação de casos, potencializando o reuso das experiências passadas na resolução de novos incidentes de segurança. Um protótipo de ferramenta que inclui as melhorias foi desenvolvido. Os experimentos demonstraram altos níveis de precisão na reutilização de casos, aumentando a qualidade no tratamento de incidentes, bem como comprovam a capacidade de gestão sistemática do conhecimento.

Palavras-chave: Tratamento de Incidentes. IODEF. STIX. CBR.

ABSTRACT

AUTHOR: FABIO ANDRÉ BARCELOS
ADVISOR: RAUL CERETTA NUNES
COADVISOR: LUIS ALVARO DE LIMA SILVA

Many organizations maintain an incident response team to mitigate the damage caused by incidents and immediately restore digital services. However, few of them learn from past experiences in a systematic way that allows them not only to respond to security incidents in the organization, but to manage this knowledge. In addition, there is a shortage of experienced security professionals. In this sense, the case-based reasoning technique has been applied in the recovery of incident handling plans. This paper revisits this approach and proposes a process with improvements for its better efficiency: a new way to categorize incidents based on international categories and the IODEF and STIX standards, which contributes to the mapping of incidents to incident handling tools; and the use of more then one similarity function to increase the accuracy of case recovery, enhancing the reuse of past experiences in resolving new security incidents. A tool prototype that includes the improvements was developed. The experiments demonstrated high levels of precision in the reuse of cases, increasing the quality in the handling of incidents, as well as demonstrating the capacity for systematic knowledge management.

Keywords: Incident Handling. IODEF. STIX. CBR.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interface*
CBR	*Case-based Reasoning*
CERT	*Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança*
CERT.BR	*Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil*
CMS	*Content Management System*
CIDR	*Classless Inter-Domain Routing*
CIRC	*Computer Incident Response Capability*
CIRT	*Cyber Incident Response Team*
CSIRT	*Computer Security Incident Response Team*
CTI	*Cyber Threat Intelligence*
CTIR.GOV	*Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo*
DDoS	*Distributed Denial of Service*
DNS	*Domain Name System*
DoS	*Denial of Service*
IANA	*Internet Assigned Numbers Authority*
ICMP	*Internet Control Message Protocol*
ID	*Unique Identifier*
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
IPv4	*IP Version 4*
IODEF	*Incident Object Description Exchange Format*
KNN	*k-Nearest Neighbours Algorithm*
LOOCV	*Leave-one-out Cross Validation*
JSON	*JavaScript Object Notation*
Malware	*Malicious software*
NAT	*Network Address Translation*
NIST	*National Institute of Standards and Technology*
RFC	*Request for Comments*
RID	*Real-time Internetworking Defense*
SQL	*Standard Query Language*
SMTP	*Simple Mail Transfer Protocol*
SSH	*Secure Socket Shell*

SOC	*Security Operations Center*
STIX	*Structured Threat Information Expression*
URL	*Uniform Resource Locator*
US-CERT	*United States Computer Emergency Readiness Team*
XML	*Extensible Markup Language*
XSS	*Cross-Site Scripting*

SUMÁRIO

1 INTRODUÇÃO

Com a segurança cibernética ganhando reconhecimento cada vez maior como uma preocupação fundamental nas organizações, há uma percepção associada de que habilidades especializadas são necessárias para apoiá-la. No entanto, isso criou desafios para as organizações na busca de talentos associados, pois existe escassez de pessoal qualificado. Essa escassez está se intensificando devido à crescente necessidade de profissionais nesta área (STRATEGIES FOR BUILDING AND GROWING STRONG CYBERSECURITY TEAMS, 2019).

A demanda por profissionais na área de segurança cibernética está aumentando e diversos conjuntos de habilidades são necessários para acompanhar o cenário de ameaças em constante mudança, o que aumenta ainda mais o problema. Neste sentido, tal como destacado em (Sohime et al., 2020), é preocupante que na situação atual não tenha esse tipo de profissional qualificado para lidar com um número crescente de ataques.

A escassez global de profissionais com boas habilidades em segurança cibernética está afetando a capacidade das organizações para abordar adequadamente esse tema de grande relevância. A pesquisa publicada pela *Enterprise Strategy Group* em conjunto com a *Information Systems Security Association International* (ISSA) relatou que 70% dos membros da ISSA entrevistados no relatório acreditam que sua organização foi duramente atingida pela já proeminente escassez de habilidades em segurança cibernética global (OLTSIK, 2020). Ela revela, ainda, que pode levar anos para se tornar um profissional proficiente em segurança cibernética. É apontado que 39% acreditam que leva de 2 a 5 anos para desenvolver esse conhecimento e 18% disseram que pode demorar ainda mais. Esse tempo é esperado, considerando a taxa na qual a tecnologia evolui e as ameaças são desenvolvidas e disseminadas a nível mundial. Essa escassez acaba sendo uma grande preocupação para as empresas e um problema de pesquisa a ser resolvido.

Para atacar esse problema e mitigar potenciais prejuízos, este trabalho assume como hipótese que a solução passa por um processo de retençao do conhecimento de especialistas em segurança. Baseado na retenção das experiências de especialistas, o processo deve potencializar que profissionais com menos experiência possam realizar o tratamento de incidentes de maneira rápida e eficaz.

No contexto do problema, a gestão do conhecimento do especialista em segurança cibernética é necessária, principalmente, para o tratamento de incidentes. É essencial o arma-

zenamento deste conhecimento para ser reutilizado por outros profissionais. Para armazenar e reutilizar essa experiência acumulada, a técnica de Raciocínio Baseado em Casos (*Case-based Reasoning* - CBR) vem sendo explorada (NUNES; AL., 2019). Porém, observa-se que fatores chave neste processo de gestão de conhecimento, como a categorização dos incidentes, sua descrição por atributos padronizados, a escolha adequada da função de similaridade e a possibilidade de ponderação de atributos, não foram exaustivamente explorados.

Na área de software, segundo (BJØRNSON; DINGSØYR, 2008) a gestão do conhecimento é um processo de identificação, captura, avaliação, recuperação, compartilhamento e uso efetivo da informação na organização. Neste sentido, o processo proposto para gestão do conhecimento permite reduzir as lacunas do conhecimento em segurança e aumentar a eficiência do processo de tratamento de incidentes.

Atualmente, quando ocorre um incidente de segurança, a resposta rápida e eficaz é fundamental. Por esse motivo, a Equipe de resposta a incidentes de segurança de computadores (CSIRT)(IOANNOU; STAVROU; BADA, 2019), deve ser capaz de detectar e mitigar incidentes, vulnerabilidades e riscos que possam surgir, e neste processo faz-se necessário uma plano de tratamento sólido para aumentar o nível de maturidade da equipe. Porém, com a quantidade de incidentes, sem um bom processo de gestão do conhecimento uma resposta rápida e eficaz é um desafio. Por exemplo, o relatório anual de incidentes reportados ao CERT.BR (CERT-BR, 2019a), publicado pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, indica que 875.327 incidentes foram reportados de janeiro a dezembro de 2019, sendo que 46% são de ataques do tipo *scan*, no qual é realizado varreduras em redes de computadores por atacantes para identificar serviços que estejam vulneráveis. Isso demonstra a necessidade de eficássia das equipes de segurança para correção de vulnerabilidades em servidores.

A descrição de incidentes, primeiro passo neste processo, ocorre por meio de modelos de representação de dados (MENGES; PERNUL, 2018). Porém, atualmente, estão disponíveis vários formatos de dados diferentes, tais como IODEF versão 1 (MEIJER; DANYLIW; DEMCHENKO, 2007), IODEF versão 2 (DANYLIW, 2016) e o STIX versão 1, STIX versão 2 (MITRE, 2019), com propriedades variadas, que permitem estruturar e descrever incidentes, incluindo informações de inteligência contra ameaças cibernéticas (CTI). Um incidente pode ser uma informação de inteligência que precisa ser tratada. As diferenças observadas nos formatos de dados padronizados implicam em problemas no que diz respeito à compreensão e compatibilidade consistentes.

O processo de resolução e tratamento do incidente, segundo passo, pode ser modelado computacionalmente por mecanismos de raciocínio baseado em casos. O raciocínio baseado em casos (CBR) (WATSON, 1999) é uma metodologia genérica para construir sistemas baseados em conhecimento voltados a resolver problemas em tarefas específicas, tal como no tratamento de incidentes. O CBR resolve os novos problemas (novos incidentes) adaptando as soluções bem-sucedidas de problemas semelhantes no passado (reúso de planos de tratamento) e possibilitando armazenar a solução como um novo caso (problema-solução).

No CBR, a suposição de similaridade afirma que problemas semelhantes têm soluções similares. O processo de solução de problemas de CBR é baseado nas etapas 4R conhecidas: Recuperar, Reutilizar, Revisar e Reter (AAMODT; PLAZA, 1994). Quanto mais válida for a suposição de similaridade, mais eficiente será o processo CBR, pois as soluções recuperadas (casos da base) são mais semelhantes ao caso da consulta (incidente que necessita uma solução, na consulta ainda desconhecida). A estratégia de recuperação mais comum é baseada nos algoritmos *k-Nearest Neighbour* (kNN), retornando as soluções dos k casos armazenados na base de casos que são mais semelhantes (do ponto de vista estrutural) à consulta. No entanto, nem sempre é garantido que a suposição de similaridade seja mantida (ABDEL-AZIZ; STRICKERT; HÜLLERMEIER, 2014).

Este trabalho revisita a abordagem baseada em CBR para a resolução de incidentes de segurança e propõe um processo para descrever e reter o conhecimento de informações sobre ameaças cibernéticas de maneira padronizada e estruturada.

1.1 OBJETIVOS E CONTRIBUIÇÕES

Este trabalho visa incrementar a capacidade do tratamento de incidentes de segurança cibernética através da implantação de um processo de gestão de conhecimento padronizado e estruturado baseado na técnica de raciocínio baseado em casos. Neste sentido visa promover melhorias para gestão de tratamento de incidentes via consolidação do conhecimento de especialistas numa base de casos de CBR.

As principais contribuições do trabalho são:

- uma categorização de incidentes, atualizada e alinhada a outras amplamente difundidas à nível mundial;
- a adoção de um grupo de atributos padronizados para descrever um incidente ajustado à

modelos de representação dados estruturados e padronizados;

- a exploração de funções de similaridade ajustadas ao tipo de dado do atributo, a fim de melhorar a recuperação e reutilização de casos para a resolução de novos incidentes de segurança;
- a exploração da ponderação de atributos na análise de similaridade realizada de acordo com a opinião de um grupo de especialistas de diferentes domínios; e
- o desenvolvimento de uma ferramenta de gestão de conhecimento para tratamento de incidentes de segurança da informação que implementa e valida a eficácia da solução e das melhorias propostos.

1.2 METODOLOGIA

Para contemplar as necessidades deste trabalho foi necessário uma fase de revisão bibliográfica para investigar a carência de profissionais de segurança nas organizações, demonstrando a real necessidade de criar um processo baseado em CBR para a retenção do conhecimento.

Foi pesquisado modelos de representações de dados que foram adequados para compor os incidentes cibernéticos. Foi necessário também fazer uma avaliação para criação de um modelo de categorias e atributos encontrados na literatura e que pudessem ser mapeados a modelos amplamente difundidos e relacionados a incidentes de segurança. Posteriomente foi realizado testes com funções algorítmicas utilizando o *framework jCOLIBRI* que fornece uma estrutura para a construção de sistemas CBR com base nas técnicas de engenharia de software desenvolvida pelo grupo GAIA(RECIO-GARCIA, 2008). A ponderação de atributos foi implementada por meio da avaliação de um grupo de especialistas, dada a devida importância de cada atributo de acordo com a categoria e com a experiência no tratamento de incidentes. A manutenção da base de casos foi tratada por meio de atualizações periódicas para geração de novos resultados.

Foi utilizado o formato IODEF e o STIX, pois são formatos para representar informações de segurança do computador e ameaças comumente trocadas entre Equipes de Resposta a Incidentes de Segurança de Computadores (CSIRTs) ou outras equipes de segurança operacional.

Para realização do processo de validação, ou seja, a realização de experimentos, foi implementado um protótipo com a finalidade de gerenciamento da base de casos, na qual é

possível realizar a consulta de casos, ações, categorias de incidentes, *hosts* de uma determinada organização e os tipos de *malwares*. A consulta de casos similares pode ser realizada por todos os atributos disponíveis para execução das funções de similariade de acordo com o tipo de atributo, levando em consideração um conjunto de pesos pré definidos por um grupo de especialistas. Com a funcionalidade de importação de casos no formato IODEF e STIX.

Nesse contexto a pesquisa se classifica como exploratória que adota um estudo de caso como centro de seu processo de avaliação e validação.

1.3 ORGANIZAÇÃO DE TEXTO

Este trabalho está organizado como segue. O capítulo 2 apresenta os conceitos importantes para a compreensão do texto da dissertação. O capítulo 3 apresenta uma revisão dos trabalhos relacionados encontrados na literatura. O capítulo 4 apresenta a arquitetura da solução proposta baseada em CBR e detalha como ela recupera, adapta e reutiliza experiências anteriores na resolução de incidentes de segurança. O capítulo 5 apresenta os experimentos e resultados. Por fim, o capítulo 6 traz as conclusões finais e trabalhos futuros.

2 REVISÃO BIBLIOGRÁFICA

Neste capítulo são apresentados os principais conceitos para a compreensão deste trabalho. A Seção 2.1 conceitua Gestão do Conhecimento (GC), a Seção 2.2 define incidentes de segurança cibernética, a Seção 2.3 denomina e descreve Tratamento e Resposta a Incidentes de Segurança e suas fases, a Seção 2.4 destaca a Representação de Dados, e, por fim, a Seção 2.5 apresenta a técnica de Raciocínio Baseado em Casos.

2.1 GESTÃO DO CONHECIMENTO

A Gestão do Conhecimento (GC) é definida como "a capacidade pela qual as comunidades capturam o conhecimento crítico para o seu sucesso, aprimoram-no constantemente e o tornam disponível da maneira mais eficaz para aqueles que precisam" (BIRKENKRAHE, 2002). Também é uma combinação "de informação, entendimento, capacidade, experiência, habilidades e valores" (ROWLEY, 2007). O conhecimento em si é um ativo intelectual, e a ciência o vê como multidisciplinar. Grande parte da vantagem competitiva de uma organização reside na formação, armazenamento e uso do conhecimento adquirido ao longo do tempo. A GC é um modelo de negócios interdisciplinar emergente que tem como foco o conhecimento na estrutura de uma organização. É um processo contínuo sistemático de criação, aplicação, disseminação, renovação e atualização do conhecimento para obter objetivos organizacionais (GHAZIRI; AWAD, 2005).

O contexto é um componente crucial da compreensão completa do conhecimento (JAFARI et al., 2008), que promove uma compreensão mais eficaz de uma determinada situação no trabalho colaborativo, caracterizado pelo compartilhamento de ideias e informações.

O contexto a ser aplicado está relacionado ao plano de tratamento de incidentes de segurança, no qual será armazenado o conhecimento e a experiência de especialistas. As lições aprendidas de uma investigação de segurança podem incluir informações sobre aprimoramentos dos controles de segurança existentes, além de analisar a necessidade de alterações nos processos e procedimentos de resposta a incidentes de segurança existentes (GRISPOS, 2016).

2.2 INCIDENTES DE SEGURANÇA CIBERNÉTICA

Existem muitas definições do termo “incidente de segurança cibernética” na literatura. As definições na revisão de literatura são as seguintes: (1) um incidente de segurança cibernética pode ser “qualquer evento adverso real ou suspeito em relação à segurança de sistemas ou redes de computadores” (CERT/CC, 2017); (2) o Instituto SANS (KRAL, 2011) descreveu em seus guias de resposta a incidentes um incidente como “um evento adverso em um sistema de informação e/ou rede, ou a ameaça da ocorrência de tal evento”; (3) em (KILLCRECE et al., 2003) um incidente é definido como uma “atividade não autorizada contra um computador ou rede que resulta em violação de uma política de segurança”. Com base nas definições, pode-se concluir que, embora existam muitas definições de “incidentes”, todas elas mostram um conteúdo substancial de semelhanças. Portanto, neste trabalho, assume-se que um incidente de segurança cibernética corresponde a ações/eventos/situações/coleta de dados com más intenções que levam a ameaças ou danos à segurança cibernética.

Um exemplo de incidente é um invasor que comanda uma *botnet* para enviar grandes volumes de solicitações de conexão a um servidor da *Web*, causando a falha. Negação de serviço, compartilhamento não autorizado de informações confidenciais, um ataque mal-intencionado a um sistema ou rede de computação e a exclusão inadvertida de um documento importante são todos considerados incidentes.

O NIST identifica vários benefícios de ter uma capacidade de resposta a incidentes (CICHONSKI et al., 2012). Um benefício importante é que essa capacidade ajuda a responder aos incidentes de maneira sistemática (isto é, seguindo uma metodologia consistente de tratamento). Isso ajuda a maximizar a chance de tomar as ações apropriadas para tratá-los. Além disso, a capacidade de resposta ajuda as organizações a minimizar as conseqüências. Ainda, outro benefício é a capacidade de aprender com incidentes. Ao usar as informações obtidas durante o tratamento, uma organização pode construir uma proteção mais forte contra intrusões futuras e, ao mesmo tempo, estar mais bem preparada para lidar com incidentes futuros por meio de planos de tratamento armazenados.

2.3 TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA

Nas organizações, uma equipe de tratamento a incidentes possui diferentes denominações (HERNANDEZ, 2018), mas corresponde a uma equipe de pessoas qualificadas que

operam sob processos definidos e são suportadas por tecnologias integradas de inteligência de segurança, operando sob o guarda-chuva do seu ambiente geral de operações de segurança. Essa equipe concentra-se em ameaças cibernéticas, monitoramento, investigação forense, gerenciamento de incidentes e relatórios (PODZINS; ROMANOVS, 2019), sendo denominada de Equipe de resposta a incidentes de segurança de computadores (CSIRT), Equipe de resposta a incidentes de computadores (CIRT), Centro de resposta a incidentes de computadores (CIRC), Centro de resposta a incidentes de segurança de computadores (CSIRC), Centro de operações de segurança cibernética (CSOC) ou Centro de Defesa cibernética.

A manipulação de incidentes consiste na realização de relatórios de incidentes, análise de incidentes e resposta a incidentes (KILLCRECE et al., 2003). A resposta a incidentes refere-se às ações tomadas para resolver ou mitigar um incidente, coordenar e disseminar informações e implementar estratégias de acompanhamento para impedir futuros incidentes semelhantes, uma vez que um incidente foi detectado, uma reação de resposta eficaz deve ser realizada. Em (BASKERVILLE; SPAGNOLETTI; KIM, 2014), a resposta geralmente é uma reação rápida e eficaz a um evento para mitigar seus impactos que causem dano. A vantagem de ter uma capacidade de resposta é minimizar a perda de informações e a interrupção de serviços e estar em conformidade com normas e políticas legais.

A resposta a incidentes coordena abordagens para gerenciar incidentes cibernéticos e precipitação para limitar as consequências. As estruturas de resposta a incidentes orientam a direção e a definição de preparação, planejamento e execução de respostas, descrevendo e detalhando seus elementos, etapas e estágios (CICHONSKI et al., 2012).

Um plano de tratamento tem como objetivo fornecer uma resposta eficaz a incidentes e detalha os processos necessários para lidar com incidentes de segurança de computadores, inclusive os recursos necessários para a execução do plano. O tratamento deve permitir que os analistas afastem os atacantes, analisem os resultados de suas respostas e apliquem as lições aprendidas para evitar ameaças repetidas.

As quatro fases do ciclo de vida de resposta a incidentes do NIST (STANDARD, 2002)(CICHONSKI et al., 2012) são: preparação; detecção e análise; contenção, erradicação e recuperação; e atividade pós-incidente. A seguir cada fase é detalhada.

- Fase 1 - Preparação

  A qualidade da resposta a incidentes depende em grande parte da preparação da resposta. Nesta fase de preparação do ciclo de vida, todos os componentes necessários para respon-

der efetivamente a um incidente de segurança de computador são identificados, criados ou adquiridos. A preparação inclui o seguinte:

  - Estabelecer uma capacidade, processo e plano de gerenciamento de incidentes;
  - Criação de políticas e procedimentos de resposta a incidentes;
  - Aquisição e treinamento de equipe de resposta a incidentes;
  - Aquisição de ferramentas e treinamento para tratamento de incidentes;
  - Construir um sistema de rastreamento de incidentes; e
  - Criação de políticas e processos de relatório de incidentes.

- Fase 2 - Detecção e análise

  Embora a capacidade de detectar incidentes esteja configurada como parte da fase de preparação, a detecção inicia o processo de resposta a incidentes. Eles não podem ser respondidos até que a detecção ocorra. Métodos de detecção comumente usados são:

  - *firewalls*;
  - sistemas de detecção / prevenção de intrusão;
  - sistemas de análise de tráfego de rede; e
  - sistemas de gerenciamento de informações de eventos de segurança.

- Fase 3: Contenção, erradicação e recuperação

  A contenção segue a detecção e validação de um incidente de segurança. Os objetivos da contenção são:

  - Parar o problema, ou seja, limitar o dano; e
  - Recupere o controle dos sistemas e da rede.

  Erradicação é a eliminação dos componentes de um incidente, como remover *malware*, eliminar contas de usuário mal-intencionadas e identificar vulnerabilidades que foram exploradas como parte do incidente de segurança.

  Recuperação é a restauração dos sistemas para a operação normal após um incidente de segurança. As tarefas de recuperação incluem restaurar arquivos de backups, mitigar vulnerabilidades identificadas na fase de erradicação e corrigí-las e alterar senhas.

- Fase 4: Atividade pós-incidente

  A atividade pós-incidente concentra-se nas lições aprendidas para melhorar a capacidade de resposta a incidentes e impedir que o incidente se repita. Os tipos de perguntas feitas durante a fase pós-incidente incluem o seguinte:

  - O que aconteceu exatamente? (linha do tempo do incidente para determinar eventos de interesse)
  - O que funcionou bem? O que não funcionou tão bem?
  - Quais procedimentos falharam na escala para responder ao incidente?
  - Quais funções da equipe funcionaram e foram desempenhadas adequadamente?
  - Foram cometidos erros que impediam a recuperação?
  - Quais ações da equipe poderiam ser melhoradas?
  - Quais políticas e procedimentos podem ser aprimorados?
  - Como esse incidente pode ter sido evitado?

Em síntese, as equipes de Resposta a Incidentes de Segurança de Computadores (CSIRTs) são responsáveis por gerenciar ameaças e vulnerabilidades de segurança cibernética para serem pró-ativas contra crimes cibernéticos. Além disso, os papéis e responsabilidades de uma CSIRT estão centrados na resposta a incidentes cibernéticos e no consequente reúso do conhecimento adquirido.

2.4 REPRESENTAÇÃO DE DADOS

Com os ataques cibernéticos em rápida evolução, os especialistas em segurança cibernética estão usando ativamente a inteligência de ameaças cibernéticas para identificar e responder a ataques cibernéticos em tempo hábil. A representação de dados é um elemento-chave no processo de troca de inteligência de ameaças, porque as informações são pré-definidas. A literatura fornece vários formatos que suportam a estruturação de informações de inteligência de ameaças. Exemplos para esses formatos são IODEF (DANYLIW, 2016) e STIX (MITRE, 2019). O foco principal do IODEF é a troca de informações sobre incidentes entre as Equipes de Resposta a Incidentes (CERTs). O STIX 2 não está vinculado a um caso de uso específico e fornece um

conjunto abrangente de ferramentas para a representação de várias informações sobre incidentes. Como são formatos com amplas possibilidades de aplicação (MENGES; PERNUL, 2018), na proposta deste trabalho o foco será nestas duas representações. Essa escolha é confirmada pelo fato de o IODEF e o STIX serem o formato padrão para a troca de informações sobre inteligência de ameaças mais utilizada atualmente (SHACKLEFORD, 2015) (SAUERWEIN et al., 2017). O STIX fornece as mais extensas estruturas de dados entre os formatos disponíveis (ASGARLI; BURGER, 2016) (MENGES; PERNUL, 2018). Isso permite uma ampla integração de conhecimentos especializados no processo de análise. A seguir o IODEF e o STIX são apresentados em mais detalhes.

2.4.1 IODEF

O IODEF *(Incident Object Description Exchange Format)* (MEIJER; DANYLIW; DEMCHENKO, 2007) define uma representação de dados e fornece uma estrutura de compartilhamento sobre incidentes de segurança de ativos computacionais com o objetivo de trocar essas informações entre as Equipes de Resposta a Incidentes de Segurança de Computadores (CSIRTs). O foco do IODEF é o transporte de informações sobre incidentes e não de armazenamento ou processamento. E para a transmissão destas informações é usado uma representação XML e para o transporte é utilizado o protocolo *Real-time Internetworking Defense* (RID) (MORIARTY, 2012).

Para poder atender a demandas não previstas no IODEF, foi criado a extensão IODEF-SCI e incorporado informações de segurança cibernética (SCI), no qual foi mantido a estrutura base do IODEF e foi adicionado campos para referência externa. Esta extensão inclui as seguintes informações: padrão de ataque, informações de plataforma, vulnerabilidade e fraqueza, instruções de contramedida, logs de eventos de computador e avaliações de severidade (TAKAHASHI; LANDFIELD; KADOBAYASHI, 2014).

Com o surgimento do IODEF versão 2 (DANYLIW, 2016), foi introduzido estruturas de dados para indicadores, atacantes e medidas defensivas e tornou obsoleta a RFC 5070. Além disso, a versão 2 adota as capacidades para o referenciamento externo que fazem parte do IODEF-SCI.

Na sua última versão ele fornece 250 propriedades de objetos e tipos de dados. Isso mostra um enorme aumento na cobertura de conteúdo em comparação com a primeira versão. Esse aumento pode ser parcialmente explicado pela introdução de entidades de eventos muito

específicas, como representações de assinaturas digitais. Em contraste com a versão 1, a versão 2 preenche a maior parte dos critérios de avaliação estrutural. Mostra apenas fraquezas nos critérios legibilidade humana, documentação e aplicação prática (MENGES; PERNUL, 2018).

O IODEF é atualmente usado por várias organizações para troca de incidentes de segurança (KAMPANAKIS; SUZUKI, 2017). São elas: o *Anti-Phishing Working Group* (APWG), um consórcio internacional que reúne empresas afetadas por ataques de *phishing*, que fornece uma ferramenta de relatório de *phishing* e cibercrime; o Centro Avançado de Defesa Cibernética (ACDC), atuante a nível europeu, que provê soluções para atenuar os ataques em andamento relacionados a *botnets*; dentre outros.

O esquema desta representação de dados foi projetado para descrever todos os atributos possíveis necessários em uma troca de incidentes de segurança. Assim, o IODEF contém uma infinidade de construções de dados. Além disso, no esquema, existem vários atributos e classes que podem ser utilizados de acordo com a necessidade das organizações.

Portanto é um modelo que se destaca entre os melhores, pois é utilizado por várias organizações, possui um *framework* com inúmeros atributos e classes e foi verificado em (MENGES; PERNUL, 2018) que atende a vários critérios avaliados tornando eficiente a sua usabilidade.

2.4.2 STIX

O STIX é um esforço baseado na comunidade, desenvolvido para padronizar a comunicação e a representação das instâncias de ameaças cibernéticas compartilhadas por diferentes nós de colaboração. Fornece uma licença permissiva, esforços de manutenção, e uma documentação abrangente. É um gráfico de nós e arestas e possui Objetos de Domínio STIX (SDO) e Objetos de Relacionamento STIX (SRO) (MITRE, 2019). Os SDO são nós, enquanto os SRO são arestas do gráfico. Além disso, o STIX fornece uma arquitetura unificada que une um conjunto diversificado de informações sobre ameaças cibernéticas (MENGES; PERNUL, 2018), incluindo:

- Observáveis cibernéticos (por exemplo, uma chave de registro é criada, o tráfego de rede ocorre para endereços IP específicos, *e-mails* de endereços específicos são observados);
- Indicadores: possíveis observáveis com significado e contexto anexados;
- Incidentes: são as ocorrências de ações adversárias específicas;

- Táticas Adversárias, Técnicas e Procedimentos-TTP: fornecem a possibilidade de capturar padrões, exploits ou *malware*, recursos como pessoas, ferramentas e infraestrutura utilizada pelo atacante e o efeito pretendido o ataque;
- Alvos de exploração (por exemplo, vulnerabilidades, fraquezas ou configurações);
- Cursos de Ação: fornece recursos para capturar contramedidas tomadas pelo defensor, bem como informações sobre o provável impacto causado pelo incidente, por exemplo, resposta a incidentes ou vulnerabilidade / soluções de fraqueza;
- Campanhas de ataque cibernético: são os conjuntos de incidentes e / ou TTP com intenção compartilhada;
- Atores de ameaças cibernéticas: identificação e / ou caracterização do adversário;

Este padrão possui doze objetos de domínio STIX (SDOs) e dois objetos de relacionamento STIX (SRO) para categorizar cada informação com os atributos específicos de cada objeto relacionado-os de acordo com as ameaças.

São objetos de domínio STIX:

- Padrão de ataque: Um tipo de Táticas, Técnicas e Procedimentos (TTP) que descreve maneiras pelas quais os agentes de ameaças tentam comprometer os alvos;
- Campanha: Um agrupamento de comportamentos de adversários que descreve um conjunto de atividades ou ataques maliciosos que ocorrem durante um período de tempo em relação a um conjunto específico de destinos;
- Curso de Ação: Uma ação tomada para evitar um ataque ou responder a um ataque;
- Identidade: Indivíduos, organizações ou grupos, bem como classes de indivíduos, organizações ou grupos;
- Indicador: Contém um padrão que pode ser usado para detectar atividades cibernéticas suspeitas ou mal-intencionadas;
- Conjunto de Intrusão: Um conjunto agrupado de comportamentos e recursos adversários com propriedades comuns que se acredita serem orquestrados por um único ator de ameaça;

- *Malware*: Um tipo de TTP, também conhecido como código malicioso e software mal-intencionado, pode comprometer a confidencialidade, integridade ou disponibilidade dos dados ou sistema da vítima;
- Dados Observados: Transmite informações observadas em um sistema ou rede (por exemplo, um endereço IP);
- Relatório: Coleções de informações sobre ameaças centradas em um ou mais tópicos, como a descrição de um agente de ameaça, *malware* ou técnica de ataque, incluindo detalhes contextuais;
- Ator de Ameaças: Indivíduos, grupos ou organizações que se acredita estarem operando com intenção maliciosa;
- Ferramenta: Software legítimo que pode ser usado por agentes de ameaças para realizar ataques;
- Vulnerabilidade: Um erro no software ou na configuração que pode ser usado diretamente por um hacker para obter acesso a um sistema ou rede.

São objeto de Relacionamento STIX:

- Relação: Usado para vincular dois SDOs e descrever como eles estão relacionados uns aos outros.
- Visualização: Denota a crença de que um elemento de *cyber threat intelligence-CTI* foi visto (por exemplo, indicador, *malware*).

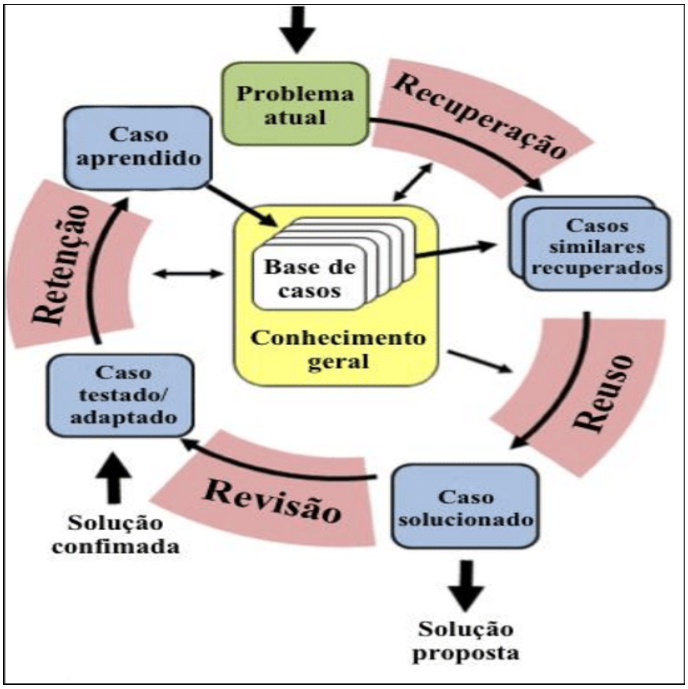
Atualmente, STIX é o padrão mais utilizado (SHACKLEFORD, 2015), embora seja muito complexo de implementar (KAMPANAKIS, 2014). Ele é modular e pode incorporar outros padrões com eficiência (BURGER et al., 2014). O STIX fornece um mecanismo comum para tratar de informações estruturadas sobre ameaças cibernéticas, melhorando a consistência, eficiência, interoperabilidade e conhecimento geral da situação (MENGES; PERNUL, 2018). Além disso, é um excelente padrão que tem a vantagem de transportar vários tipos de dados representados em cada intercâmbio, inclusive incluindo o padrão de dados pré-normalizados (MITRE, 2019). Cabe ressaltar que é um dos padrões mais abrangentes para unificar o compartilhamento de informações de segurança cibernética.

2.5 RACIOCÍNIO BASEADO EM CASOS

O CBR é uma metodologia (WATSON, 1999) para resolução de problemas, baseada no uso de experiências passadas para resolver um novo problema. O ciclo de resolução no CBR pode ser descrito por quatro etapas, conforme Figura 1 : Recuperar-Reutilizar-Revisar-Reter.

1. Recuperar da base de casos o caso mais similar (ou casos) para o novo problema a ser resolvido.
2. Reutilizar informações e conhecimento do caso ou casos recuperados para resolver o problema.
3. Revisar a solução proposta.
4. Manter as partes provavelmente úteis da experiência para a resolução de problemas futuros.

Figura 1 – Ciclo do Raciocínio Baseado em Casos



Fonte: (VON WANGENHEIM; VON WANGENHEIM, 2003)

Um caso consiste em uma descrição do problema que na abordagem deste trabalho é um incidente de segurança e uma solução, um plano de tratamento para solucionar o incidente. Uma base de caso (CB) é composta por casos armazenados anteriormente. A metodologia de

raciocínio baseado em casos *(Case Based Reasoning - CBR)* é o processo de resolver um novo problema usando soluções de problemas passados. Por isso, também é chamado de método de solução de problemas baseado na experiência (DE; CHAKRABORTY, 2018). O núcleo do CBR é o princípio de busca dos K-vizinhos mais próximos (KNN), que mede a similaridade de uma nova instância com os exemplos anteriores, usando uma função de kernel adequadamente definida.

No gerenciamento de tratamento de incidentes de segurança, o CBR é uma abordagem adequada para gerir planos de tratamento, com o suporte de uma base de dados de planos atualizados. Um plano de tratamento começa na avaliação do ativo que identifica o cenário em potencial, e cria um plano de tratamento para solucionar o incidente. Um modelo baseado em CBR foi utilizado para oferecer as recomendações ao analista de segurança. O CBR evita a complicada fase de treinamento do modelo e é aplicável a uma variedade de tipos de dados.

Para desenvolver métodos baseados no CBR diferentes *frameworks* podem ser utilizados. Dentre eles o *framework jCOLIBRI* (RECIO-GARCÍA; GONZÁLEZ-CALERO; DÍAZ-AGUDO, 2014) foi criado para servir de referência no desenvolvimento de aplicações CBR e projetado para ser extensível e reutilizável. Possui links para material de apoio como: documentação, tutoriais e exemplos. Esta ferramenta foi desenvolvida em JAVA, como plugin do Eclipse, sua primeira versão foi disponibilizada em 2005 e o desenvolvimento continua ativo, o que proporciona experiência na área de CBR. Todas as etapas do Ciclo CBR estão implementadas neste *framework*.

O estudo comparativo de (ELKAFRAWY; MOHAMED, 2015) aplicou a mesma base de casos em diferentes ferramentas e concluíu que os *frameworks* myCBR (BACH; ALTHOFF, 2012) e *jCOLIBRI* são mais avançados por implementarem todas as etapas do Ciclo CBR. Já as outras focam apenas na etapa de recuperação de casos similares. Uma das vantagens do *jCOLIBRI* sobre os demais é a capacidade de se conectar com bases de dados externas, o que possibilita o uso de SQL *Query's* facilitando a seleção de dados e aproveitando o poder do SGBD (Sistema Gerenciador de Banco de Dados), enquanto os demais utilizam arquivos texto ou XML.

3 TRABALHOS RELACIONADOS

Na revisão sistemátca da literatura foram selecionados os trabalhos apresentados neste capítulo. Na pesquisa foi utilizado um conjunto de palavras chaves, tais como: *Lack of cybersecurity manager*, *Lack of cybersecurity professionals*, *An Exploration of the Cybersecurity Workforce Shortage*, *survey Shortage of cybersecurity professionals*, *cyber-security skills*, *data representation for security incident reports*, *knowledge management implementation of incident security*, *taxonomy of security incidents*, *Cyber Attacks*, *Case-Based Reasoning* - CBR, *incident response plan*, *Incident response - playbooks*, *Application of Case Based Reasoning in IT Security Incident Response*. As fontes de pesquisa utilizadas neste trabalho foram: *Association for Computing Machinery* (ACM), *Advanced Computing: An International Journal (ACIJ)*, *Google Scholar*, *Scopus*, *IEEE Explore*, Portal de Periódicos CAPES/MEC e *ScienceDirect*.

Em (AJJOURI; BENHADOU; MEDROMI, 2019), uma solução para detecção de intrusão baseada na arquitetura de um sistema multiagente foi proposta. Para apoiar as decisões que esses agentes devem tomar, a técnica CBR foi explorada na recuperação, reutilização e revisão do conhecimento de caso. Os casos foram representados por um conjunto de características: protocolo, endereço IP de origem, porta de origem, endereço IP de destino, porta de destino e conteúdo do pacote. Embora esse tipo de solução baseada em vários agentes seja relevante neste cenário adverso em relação à detecção de intrusão por diferentes razões, os autores não exploraram os padrões de representação de dados e não foi identifcado experimentos e validações no artigo. Assim, é um desafio usar a solução proposta em conjunto com outros sistemas de segurança da informação que visam resolver problemas causados por diferentes tipos de incidentes. A partir da revisão dos padrões de trocas de dados de segurança (MENGES; PERNUL, 2018) (TAKAHASHI; MIYAMOTO, 2016), este trabalho investiga uma solução para este problema.

Em (COLOMÉ; NUNES; SILVA, 2019) foi proposto reter a experiência de um especialista em segurança da informação em uma base de conhecimento, a qual utiliza a técnica de Raciocínio Baseado em Casos tendo como objetivo automatizar a recomendação de planos de respostas a novos incidentes. No trabalho foi utilizado o IODEF versão 1 para a modelagem de casos, selecionando os atributos nos quais foram julgados coerentes pelos autores para a representação das informações contidas nos incidentes de segurança. Foram elencados os tipos de incidentes mais comuns e utilizado a ponderação de atributos estática. Porém não foi tratado pelos autores as representações do modelo STIX, IODEF versão 2, e a ponderação de atributos

dinâmica, o que tornaria a recuperação do plano de tratamento mais eficaz. O autor empregou a distância euclidiana para os cálculos de similaridade, no entanto, verificou-se que não é adequado calcular a similaridade entre alguns atributos utilizando essa função. Por exemplo, o atributo categoria, definido como númerico, não poderia ter seu valor analisado por esta função de distância, pois dado um incidente com este atributo com valor "dois" *(Defacement)* e o outro com valor "três" (DDoS), pela distância euclidiana seriam classificados como próximos, apesar de serem categorias completamente diferentes. O adequado seria aplicar uma função de similaridade de igualdade. O mesmo acontece com outros atributos, tal como Protocolo e *NomeMalware*. Funções de similaridade que são ajustadas com o uso de pesos de atributos baseados em especialistas de domínio também não foram exploradas na recuperação e reutilização de planos de tratamento de incidentes de segurança, mecanismos explorados neste trabalho.

Em (ZAKARIA, 2015) foi proposto um sistema CBR para auxiliar os analistas de segurança no tratamento e resposta a incidentes de segurança cibernética por meio de experiências que são armazenadas em uma base casos de uso. As funcionalidades principais são: o armazenamento de caso que contém uma lista de experiências passadas, que são representadas na forma de casos, que consiste em dois segmentos: o problema e a solução. O sistema proposto é capaz de raciocinar e tomar decisões no domínio da resposta a incidentes de segurança. No entanto os atributos são limitados, pois não são considerados: o impacto, o sistema operacional do *host* afetado, a vulnerabilidade, o título no caso de uma violação de *copyright* e a porta lógica utilizada para se comunicar com a *botnet*. Não foi identifcado experimentos e validações neste artigo. Foi analisado que não foi adotada nenhuma representação de dados padrão e não foi abordada nenhum conjunto de categorias de incidentes. Neste trabalho são explorados categorias e atributos que não foram considerados, bem como as representações padronizadas de dados.

Em (SANTOS; NOBRE, 2019) foi empregado a técnica de CBR para aprimorar ferramentas que auxiliam profissionais inexperientes na resolução de atividades de identificação de vulnerabilidades em sistemas operacionais linux. A finalidade é fazer com que profissionais inexperientes obtenham resultados semelhantes ao de profissionais experientes. Foi implementado um protótipo que possui a capacidade de cadastrar novos casos, identificar vulnerabilidades a partir da recuperação de casos com aplicação de algoritmos de similaridade, sugerir soluções, permitir avaliação da solução proposta, a adaptação da solução em situações onde existe a necessidade de complemento e o aprendizado de novas experiências, de acordo com a metodolo-

gia CBR. Foram utilizados as funções de similaridade baseadas em cosseno e Levenshtein pois apresentaram resultados satisfatórios nos testes realizados. Para o algoritmo de recuperação foi utilizado o *Nearest Neighbor Matching*, ou algoritmo de vizinhança por sua vasta documentação, simplicidade, eficiência e ser comum entre as aplicações CBR. Não foi adotada nenhuma representação de dados padrão. Neste trabalho são explorados representações padronizadas de dados.

Na tabela 1 foi realizado um comparativo dos trabalhos relacionados. Nota-se que apenas o trabalho (COLOMÉ; NUNES; SILVA, 2019) utiliza representação de dados e ponderação de atributos (estática). Porém, utilizou o IODEF versão 1, e ficou limitado a esse formato e versão, implementou a ponderação estática de atributos. Cabe ressaltar que a primeira versão do IODEF tornou-se obsoleta (MEIJER; DANYLIW; DEMCHENKO, 2007) dando lugar para outra versão (DANYLIW, 2016). No estudo comparativo de representação de incidentes (MENGES; PERNUL, 2018) é apontado as deficiências da versão, tais como representações de informações do atacante ou defensor e a integração de dependências externas.

Os outros trabalhos não relataram o uso de representação de dados, ponderação dinâmica de atributos e nem especialistas de domínio, apesar de todos empregarem o uso da técnica de CBR para recuperação de casos. A ponderação dinâmica é um facilitador para a recuperação dos casos, visto que diferentes combinações de valores para cada atributo podem resultar em melhores resultados. Isso reflete diretamente na solução do caso.

Na última coluna, especialistas de domínio, observou-se que nenhum dos trabalhos explorou visões de diferentes especialistas. Nenhum utiliza o conhecimento de um grupo de analistas de segurança seniores para ajustar dinamicamente o conjunto de pesos para as diferentes consultas CBR. A opinião deste grupo é um fator relevante devido a escassez de mão de obra especializada na área de cibersegurança, pois na falta de profissionais com experiência, esse conhecimento pode ser utilizado por uma equipe inexperiente.

Tabela 1 – Trabalhos relacionados

Trabalho	Formato de Representação de dados	Ponderação dinâmica de atributos	Especialistas de domínio
AJJOURI; BENHADOU; MEDROMI, 2019	Não relata o uso	Não utiliza	Não utiliza
M Colomé, RC Nunes, LA de Lima Silva, 2018	IODEF versão 1	Utiliza a ponderação de atributos de forma estática	Não utiliza
ZAKARIA, 2015	Não relata o uso	Não utiliza	Não utiliza
SANTOS; NOBRE, 2019	Não relata o uso	Não utiliza	Não utiliza
Este trabalho	IODEF versão 2 e STIX	Utiliza	Utiliza

Fonte: Autor.

4 PROCESSO PARA GESTÃO DE CONHECIMENTO NO TRATAMENTO DE INCIDENTES DE SEGURANÇA

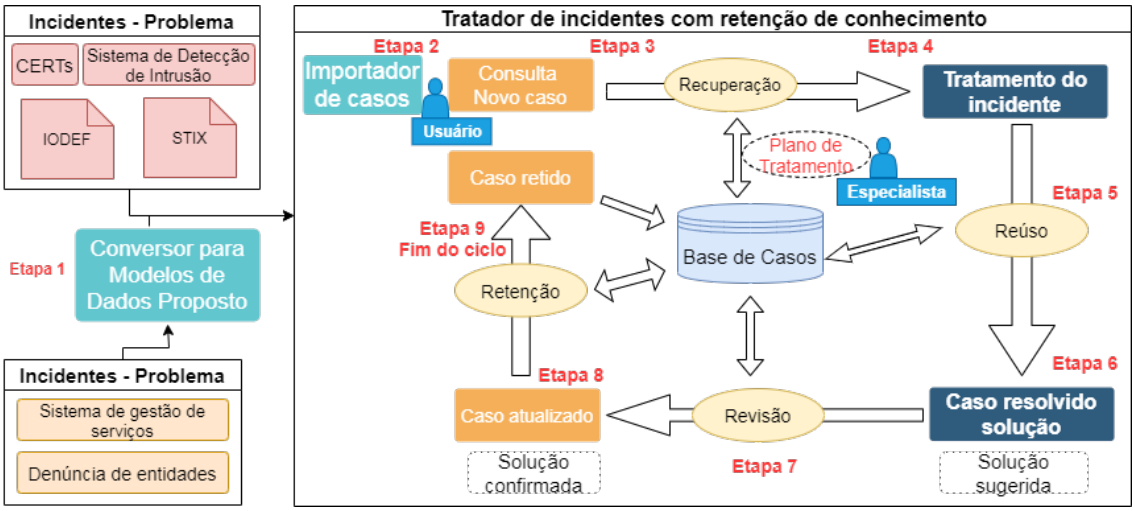
Neste capítulo é proposto o processo de tratamento de incidentes baseado na técnica de *Case-base Reasoning* (CBR), o qual permite sistematizar a gestão do conhecimento no processo de tratamento de incidentes de segurança da informação. A Seção 4.1 apresenta a abordagem geral do processo e as demais Seções detalham etapas inovadoras do processo.

4.1 ABORDAGEM PARA TRATAMENTO DE INCIDENTES BASEADO EM CBR

Este trabalho estende a dissertação apresentada em (COLOMÉ; NUNES; SILVA, 2019) e propõe melhorias para gestão de tratamento de incidentes via consolidação do conhecimento de especialistas numa base de casos de CBR. Para ter uma melhor organização deste conhecimento é proposto: 1) uma categorização atualizada, alinhada a outras amplamente difundidas à nível mundial, e com um grupo de atributos para descrever um incidente ajustado à modelos de dados estruturados e padronizados; 2) a exploração de funções de similaridade ajustadas a fim de melhorar a recuperação e reutilização de casos para a resolução de novos incidentes de segurança; ao fazer isso, é abordado o uso de conhecimento baseado em similaridade coletado no formato de atributos e pesos, onde tais ajustes são realizados e analisados de acordo com a opinião de quatro especialistas de domínios diferentes; e consequentemente 3) desenvolvimento de uma nova versão do sistema que implementa e valida a eficácia da solução e dos melhoramentos propostos.

Na Figura 2 é apresentado a arquitetura da solução, que começa na etapa 1 com a chegada de um incidente (problema) que foi detectado em algum ativo da infraestrutura computacional da organização. O incidente é mapeado para categorização adotada com um conjunto de atributos necessários para sua identificação na composição da base de casos. Esses atributos são alinhados por modelos de representação de dados amplamente difundidos, o IODEF V2 (DANYLIW, 2016) e o STIX V2 (MITRE, 2019), mas também podem ser preenchidos através de um sistema de gerenciamento de *service desk*.

Figura 2 – Arquitetura proposta para solução de gestão de conhecimento no tratamento de incidentes de segurança.



Fonte: Autor

O mapeamento do relato de um incidente para um caso de consulta é realizado por um conversor de modelos (incidente –> caso). Para fazer isso, os valores de cada atributo de um incidente descrito em IODEF V2 ou STIX V2 são analisados a fim de classificar o incidente de acordo com a categorização proposta neste trabalho. Esta análise faz uso da descrição do incidente, uma vez que ela detalha as informações que podem ser úteis na recuperação de planos de tratamento relevantes, como por exemplo o endereço IP associado a um servidor de aplicação da organização. Mas o tratamento de um incidente ocorrido em um servidor pode ser diferente de um tratamento do mesmo incidente em uma máquina cliente. Com uma categorização resultante dos atributos dos padrões IODEF e STIX, o processo de mapeamento descrito é facilitado, proporcionando um mapeamento automático para a categorização proposta sem a necessidade de intervenção humana.

Na Etapa 2, o incidente é considerado um caso de consulta que deve ser respondido pelo sistema. Os parâmetros de consulta são baseados nas informações registradas neste novo caso. Este processo de formação de consulta acontece sem a necessidade de ajustes humanos. Em algumas situações particulares, devido à falta de informações relevantes no incidente relatado, um analista de segurança pode ajustar os parâmetros de consulta de acordo com uma investigação rápida sobre os detalhes do incidente e sua experiência. Se o usuário for um analista de segurança júnior, ele pode simplesmente executar a consulta formada sem alterar nada. Isso significa que o sistema proposto deve recomendar medidas de tratamento de incidentes, mesmo em face de especificações de consulta incompletas (às vezes incorretas). Os parâmetros de pe-

sos dos atributos, usados nos cálculos de similaridade, também podem ser ajustados na consulta pelos analistas sêniores. Se um analista sem experiência tiver que lidar com a resolução do incidente, ele pode construir e executar consultas alternativas no sistema. Com isso, vai poder explorar os resultados obtidos na recuperação. Além disso, várias alternativas de esquemas de ponderação previamente coletados e testados com usuários especialistas no domínio também estão disponíveis no sistema. Portanto, analistas de segurança sem experiência podem reutilizar esse conhecimento de similaridade com base na opinião de analistas mais experientes para realizar suas consultas a fim de resolver os danos e as vulnerabilidades do incidente relatado.

Na Etapa 3, os casos mais semelhantes contidos na base de caso são retornados como resultado das execuções da consulta. Essa recuperação também é guiada pela categorização do incidente. Os casos recuperados representam os detalhes da resolução do incidente de segurança anterior. Isso é registrado principalmente nos casos recuperados na forma de um plano de tratamento de incidentes. Os planos recuperados detalham uma sequência minuciosamente descrita de etapas que devem ser seguidas pelos analistas de segurança para responder ao tipo de incidente indicado no caso recuperado. A reutilização de tal conhecimento de resolução de incidente de segurança pode ser desenvolvida com a execução do plano de tratamento recuperado. No entanto, tais planos podem estar sujeitos a pequenas modificações, uma vez que esses planos corretivos podem ser executados em diferentes infraestruturas computacionais na organização. Em qualquer caso, a recuperação da informação de tratamento anterior registrada em casos concretos de resolução de problemas permite um tratamento mais eficaz do incidente, não só permitindo reduzir o tempo de tratamento, mas também garantindo uma resolução adequada.

Na Etapa 4, é analisado o plano de tratamento recomendado (associado aos casos recuperados mais semelhantes). Se o analista entender que o plano permite que o incidente seja mitigado, ele passa para a Etapa 5, para reutilizar as informações de tratamento recuperadas da base de casos. Se forem necessários ajustes nos planos de resolução de incidentes recuperados, então serão feitos pelo analista de segurança antes da reutilização das informações do plano. Isso significa que a reutilização do conhecimento de resolução de incidentes pode ser parcial, sempre que necessário, pois o conhecimento recuperado pode ser utilizado para posteriormente gerar novos planos.

Na Etapa 6, é consolidada as informações resultantes do processo de reutilização de experiências anteriores de resolução de incidentes, indicando que o plano de tratamento recuperado mitigou o incidente. Ao fazer isso, esses usuários também podem sugerir o registro de

possíveis variações nos planos de tratamento de incidentes recuperados e reutilizados. Em um processo contínuo de atualização e aprendizado direcionado à captura e representação de novos conhecimentos de resolução de incidentes, este usuário também pode sugerir o registro de um novo plano de tratamento para um incidente específico. É importante notar que essa solução sugerida pode não ser ideal ou mesmo apropriada por muitos motivos. Neste caso, deve ser submetido a uma revisão por especialistas em segurança da organização, onde esta revisão é desenvolvida antes que o novo caso seja registrado na base de casos. Também é importante observar que, dada a dinâmica das situações de ataque cibernético, novos casos de resolução de ataque são continuamente registrados na base de casos. Além disso, os usuários também podem recomendar procedimentos de solução para casos existentes, que podem precisar ser ajustados de diferentes formas. Assim, o sistema proposto é direcionado para um cenário no qual o conhecimento da resolução de incidentes é constantemente revisitado e revisado, não apenas como uma resposta às medidas de ataque e defesa que se desafiam, mas também como uma resposta às mudanças da infraestrutura computacional subjacente.

Na Etapa 7, uma solução sugerida pelo analista júnior passa por uma revisão desenvolvida pelo analista sênior. Para isso, esses especialistas podem consultar a base de caso para analisar outros casos registrados. Como parte de tais atividades de manutenção, os usuários mais experientes também revisam e atualizam planos que podem ser semelhantes em muitos aspectos. O objetivo é detectar as necessidades de revisão efetivas às quais os casos registrados na base de casos devem ser submetidos.

Na Etapa 8, uma equipe sênior analisa o relatório construído e decide se armazena ou não novas soluções (novas experiências). Finalmente, na Etapa 9, os novos planos são consolidados e mantidos na base de caso (aprendizagem).

A solução proposta torna dinâmico o processo de tratamento de incidentes de segurança da informação, permitindo o aprendizado constante de novos casos e, consequentemente, a retenção do conhecimento de resolução de problemas. Com a solução proposta, a capacidade de resolução é aumentada, com particular atenção para fornecer o suporte de resolução de problemas necessário para permitir que profissionais de segurança juniores desenvolvam melhor esse trabalho. As próximas seções detalham as etapas da solução proposta.

4.2 CATEGORIZAÇÃO DE INCIDENTES

Com o aumento do crime cibernético, ameaçando indivíduos, empresas e governos, tornou-se essencial para o setor de segurança estabelecer uma maneira comum de falar sobre o problema. A maioria das empresas experimenta uma série de incidentes de segurança que ocorrem com certa frequência e intensidade (KUYPERS; MAILLART; PATÉ-CORNELL, 2016). Logo, faz-se necessário categorizar estes incidentes para que seja apresentado um plano que obtenha êxito no seu tratamento. Neste sentido, esta seção busca categorizar os tipos de incidentes mais relevantes de segurança cibernética para estabelecer uma forma de padronização e aplicabilidade nas ações de planos de tratamento.

A categorização proposta nesta seção deriva de categorias variadas apresentadas na literatura e padrões de representação amplamente difundidos, utilizados e aceitos. A seguir, inicialmente apresenta-se o resultado de estudos e análises de categorizações encontradas e, posteriormente, apresenta-se a categorização proposta.

Em (HUMAYUN et al., 2020) foi realizado um estudo de mapeamento sistemático para identificar e analisar os incidentes comuns de segurança cibernética, a fim de categorizá-los. No estudo, foram identificadas sete categorias, tal como ilustra a Figura 2. Porém percebeu-se a falta de alguns tipos de incidentes comuns que não foram mapeados, como *botnet* e violação de *copyright*, os quais possuem grande relevância em ataques cibernéticos. A Tabela 2 apresenta também a frequência e o percentual de ocorrência de ameaças. Observa-se uma concentração significativa não classificada (no tipo "Outros"), o que torna difícil a sistematização do tratamento a partir da categorização proposta por estes autores.

Tabela 2 – Tipos de Incidentes

Tipo de Incidente	Frequência	Porcentagem(%)
Reutilização de credenciais	1	1
Script entre sites(XSS)	1	1
Denial of Service(DoS)	29	37
Malware	16	21
Phishing	7	9
Seguestro de sessões e ataques *man-in-the-middle*	2	3
Ataque de injeção SQL	3	4
Outros	19	24

Fonte: (HUMAYUN et al., 2020)

Em (SCHMITT et al., 2018) foi publicado um estudo sobre as soluções utilizadas na União Europeia e as orientações para o desenvolvimento de uma taxonomia de referência. O estudo baseia-se na taxonomia do CSIRT europeu (CERT-PT, 2012) e na taxonomia comum da Europol para centros de aplicação da lei e de segurança cibernética (EUROPOL, 2017). O Grupo de Governança de Taxonomia, formado pela Enisa, Europol e o CERT europeu, foi estabelecido para a manutenção e atualização dessa taxonomia para maximizar a colaboração entre as forças policiais e os CSIRTs. Neste sentido, os autores fornecem uma taxonomia mais completa e detalhada do que em (HUMAYUN et al., 2020). Ela foi separada por classes e tipos, conforme ilustra a Tabela 3. Porém, o tipo "Comando e controle (C&C)", conhecido como *botnet*, foi classificado na classe *"Malware"*. As ações de uma *botnet* fornecem uma plataforma para diferentes ataques, que podem ser a distribuição de spam, infecções por *malware* e, o mais comum, DDoS. Logo, devido a sua amplitude de ataques, entende-se que *botnet* deveria ser uma categoria separada.

Tabela 3 – Classificação Européia

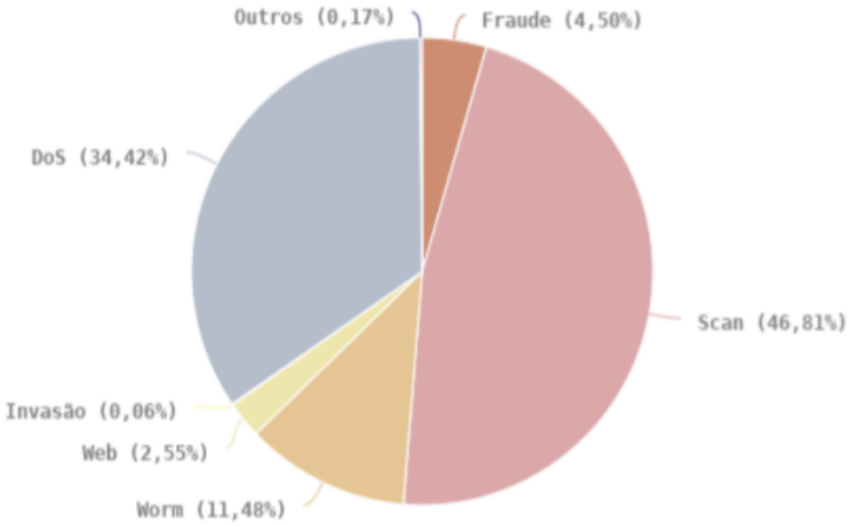
Classe de incidentes	Tipo de incidente
Malware	• Infecção • Distribuição • Comando e controle(CC) • Conexão maliciosa
Disponibilidade	• *Denial of Service(DoS)* • *Distributed Denial of Service(DDoS)* • Sabotagem
Obtenção de informações	• *Scan* • *Sniffing* • *Phishing*
Tentativa de intrusão	• Exploração de tentativa de vulnerabilidade • Tentativa de login
Intrusão	• (Bem-sucedida) Exploração de vulnerabilidade • Contas comprometidas
Segurança de Informação	• Acesso não autorizado • Modificação/exclusão não autorizada
Fraude	• Uso indevido ou não autorizado de recursos • Falsificação de identidade
Conteúdo abusivo	• *Spam* • *Copyright* • Exploração sexual infantil, racismo ou incitamento à violência
Outros	• Incidente não classificado/indeterminado

Fonte: (SCHMITT et al., 2018)

Em (US-CERT, 2017), o órgão responsável pelo tratamento de incidentes nos Estados Unidos da América - US-CERT - apresenta uma taxonomia única, diferente da utilizada pela agência europeia, porém muito semelhante em contextos descritivos. No entanto, a classificação é mais generalista em alguns incidentes, como o "Uso impróprio", o qual resulta de violações de políticas de uso aceitável e pode enquadrar as categorias "Tentativas de intrusão" e "Obtenção de informação". A categorização do US-CERT é apresentada na Tabela 4 com a descrição e os exemplos.

No contexto brasileiro não existe nenhuma taxonomia padrão de classificação de incidentes cibernéticos para troca de incidentes entre os CSIRTs. O CERT.BR disponibilizou as estatísticas sobre as notificações de incidentes que foram reportadas (CERT-BR, 2019b), e desta forma é possível identificar a classificação de incidentes utilizada pelo órgão. Entretanto, incidentes que ocorrem com certa frequência, como *phishing*, *botnet*, *spam*, tentativa de intrusão, não foram identificados. É apresentado na Figura 3 os tipos de incidentes que foram reportados ao CERT.BR de janeiro a dezembro de 2019, o que aponta os maiores percentuais (*Scan* com 46,81% e DoS com 34,42%) mas não uma categorização propriamente dita. A busca nos materiais do CERT.BR não resultou na identificação de uma categorização dos incidentes que poderia ser adotada pelo órgão.

Figura 3 – Incidentes reportados ao CERT.BR.



Fonte: (CERT-BR, 2019b)

Em (CTIR-GOV, 2020), o Centro de Tratamento e Resposta a Incidentes Cibernéticos

Tabela 4 – Vetores de Ataque

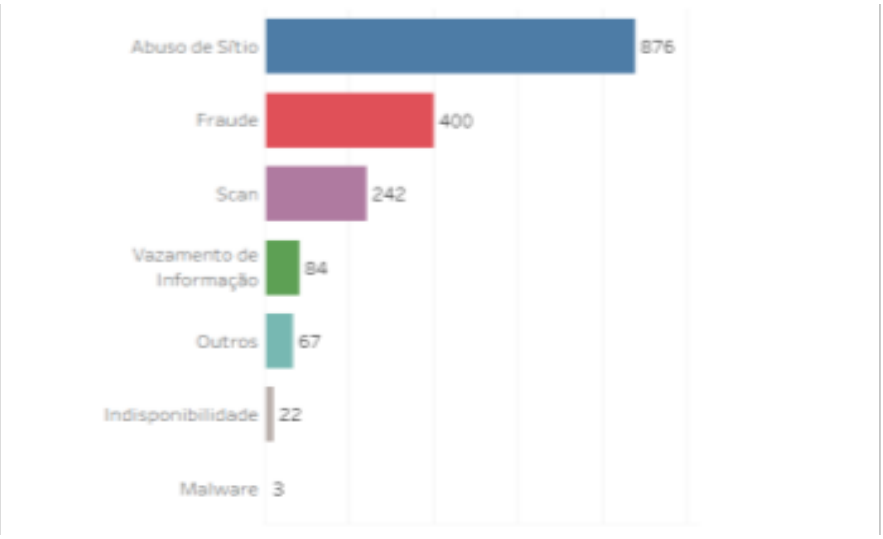
Vetor de Ataque	Descrição	Exemplo
Desconhecido		
Atrito	Um ataque que emprega métodos de força bruta para comprometer, degradar ou destruir sistemas, redes ou serviços.	Negação de serviço destinada a prejudicar ou negar o acesso a um aplicativo; um ataque de força bruta contra um mecanismo de autenticação, como senhas ou assinaturas digitais.
Web	Um ataque executado a partir de um site ou aplicativo baseado na Web.	Ataque de script entre sites usado para roubar credenciais ou redirecionar para um site que explora a vulnerabilidade do navegador e instala *malware*.
Email / *Phishing*	Um ataque executado por meio de uma mensagem ou anexo de email.	Explorar código disfarçado de documento anexado ou um link para um site mal-intencionado no corpo de uma mensagem de email.
Mídia externa/ removível	Um ataque executado a partir de mídia removível ou dispositivo periférico.	Código malicioso que se espalha para um sistema a partir de uma unidade de mídia infectada.
Falsificação de identidade/ falsificação	Um ataque envolvendo a substituição de conteúdo / serviços legítimos por um substituto malicioso.	Falsificações, ataques intermediários, pontos de acesso sem fio não autorizados e ataques de injeção estruturada de linguagem de consulta envolvem representação.
Uso impróprio	Qualquer incidente resultante da violação das políticas de uso aceitável de uma organização por um usuário autorizado, excluindo as categorias acima.	O usuário instala um software de compartilhamento de arquivos, levando à perda de dados confidenciais; ou um usuário executa atividades ilegais em um sistema.
Perda ou roubo de equipamento	A perda ou roubo de um dispositivo ou mídia de computação usado pela organização.	Um laptop ou dispositivo móvel extraviado.
Outro	Um método de ataque não se encaixa em nenhum outro vetor.	

Fonte: (US-CERT, 2017)

de Governo disponibiliza dados de incidentes e detalha sua distribuição dentro de categorias possivelmente utilizadas pela instituição. As categorias utilizadas na Figura 4, que descreve incidentes de janeiro até abril de 2020, permitem identificar os maiores números de casos de incidentes, que foram o abuso de sítio com 876 incidentes e fraude com 400 incidentes. Porém,

neste orgão percebe-se a semelhança de contexto de classificação de incidentes com o CERT.BR e a falta de categorias como *phishing*, *botnet* e tentativa de intrusão. Cabe salientar que não foi localizado uma proposição de categorização por esta instituição.

Figura 4 – Incidentes reportados ao CTIR.GOV.



Fonte: (CTIR-GOV, 2020)

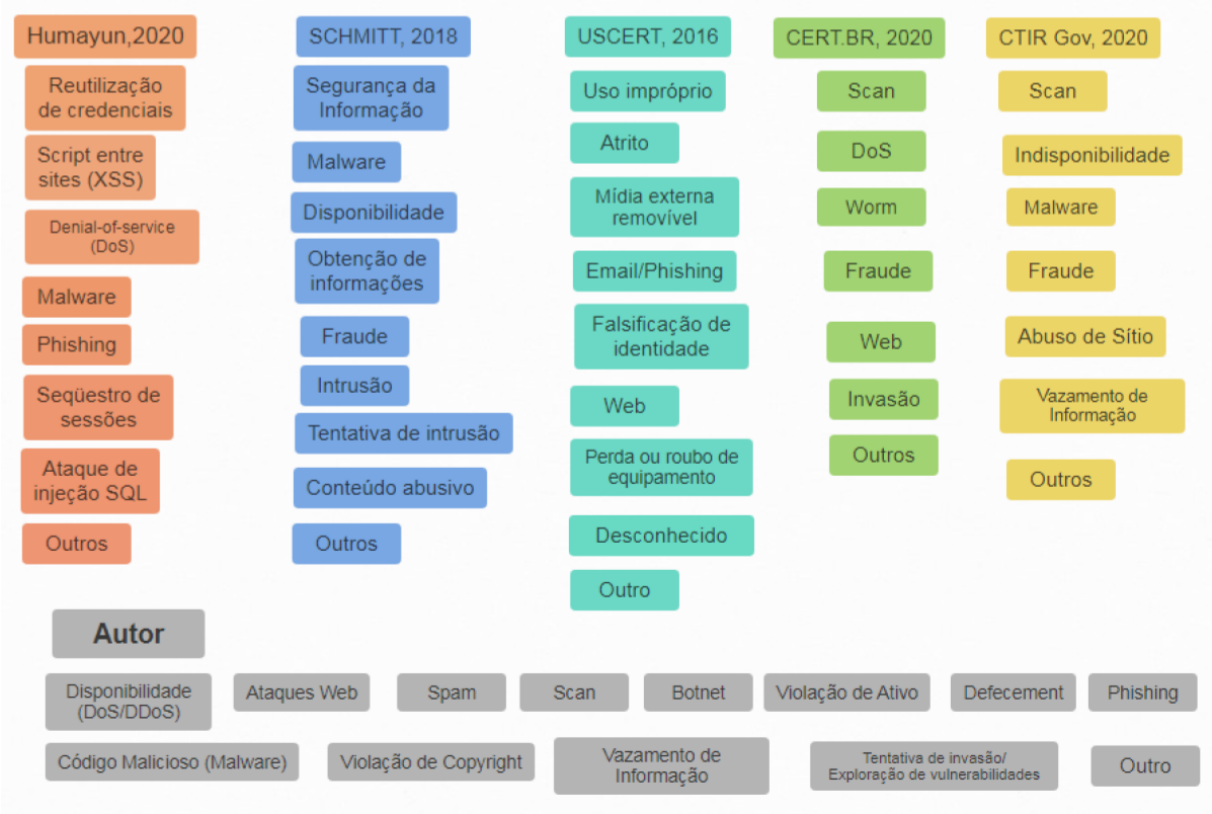
Em (PING; HAIFENG; GUOQING, 2010), foram avaliados um conjunto de tipos de incidentes semelhantes aos utilizados pelos CSIRTs, embora limitado, pois não foi identificado categorias que englobem *Copyright*, Ataques *Web*, *Spam*, *Botnet* na ontologia proposta por este autor.

(JIANG et al., 2014) mostrou um relacionamento hierárquico para diferentes tipos de incidentes de segurança, incluindo o relacionamento entre o vírus, o *worm* e o incidente de DDoS, porém ficou limitado em relação a outras categorias como Violação de*Copyright*, *Botnet* e Ataques *Web*.

Em síntese, foi observado nestes estudos e análises que na literatura há proposições de diferentes categorias e que destas pode-se extrair doze categorias/tipos mais comuns, formando assim uma nova categorização. São eles: Disponibilidade(DoS/DDoS), Ataques *Web*, *Spam*, *Scan*, Violação de *Copyright*, *Botnet*, Violação de Ativo, *Defacement*, *Phishing*, Tentativas de Invasão/Exploração de Vulnerabilidades, *Malware*, Vazamento de Informação e Outros, conforme ilustra a categorização cinza (parte de baixo) na Figura 5. Naturalmente, salienta-se que é necessário incluir a categoria "Outros"para atender a incidentes que eventualmente não sejam classificados em nenhuma categoria previamente conhecida. A Figura apresenta também, em cores distintas (colunas), as categorizações encontradas na literatura, a fim de facilitar a iden-

tificação de relacionamentos dos tipos presentes nas categorias previamente modeladas com os tipos presentes na nova categorização proposta. Cabe ressaltar que na modelagem de (SCHMITT et al., 2018), na categoria *malware*, o autor definiu comando e controle (*botnet*) como um tipo de incidente desta categoria e que na nova categorização o tipo *botnet* foi extraído da categoria *malware*. Considera-se importante esta separação por ser o tipo de incidente *botnet* base não só para incidentes do tipo *malware*.

Figura 5 – Categorias identificadas (colunas) e proposta (linhas em cinza).



Fonte: Autor.

A seguir, o detalhamento das categorias/tipos de incidentes selecionadas para a categorização de incidentes proposta.

• Disponibilidade (DoS/DDoS): Esse tipo corresponde a incidentes derivados de ataques que tornam uma máquina ou recurso de rede indisponível para os usuários legítimos, como interromper temporária ou indefinidamente os serviços de um *host* conectado à Internet (MALLIKARJUNAN; MUTHUPRIYA; SHALINIE, 2016). O ataque mais comum nesta categoria geralmente é baseado em ataques DDoS originados de *botnets*, mas também existem outros tipos que podem ser incluídos nesta categoria, como ataques de amplificação de DNS, dado que tornam indisponíveis recursos de rede. No entanto, a disponibilidade também pode ser afetada

por ações locais (destruição, interrupção do suprimento de energia, etc.) - ou por agravo, falhas espontâneas ou erro humano, sem malícia ou negligência.

• Código malicioso (*Malware*): Categoria que engloba identificação de software malicioso (*malware*) projetado para prejudicar os recursos do computador, roubando informações vitais, criptografando arquivos e obtendo acesso à máquina de destino remoto. Os *malwares* podem ter muitas formas (arquivos executáveis, scripts, dlls, macros etc.) operando em segundo plano no sistema (RANI; REEJA, 2019).

• Ataques *Web*: Esta categoria unifica duas sub-categorias, a *Web Based Attacks (Exploits)* e a *Web Application Attacks*. Os *Web Based Attacks* são ataques que usam sistemas e serviços da *Web* como o principal vetor para comprometer a vítima. Isso inclui explorações e injeções no nível do navegador (incluindo extensões), sites, exploração do Sistema de Gerenciamento de Conteúdo (CMS) e serviços da *Web*. Por exemplo, os ataques *drive-by*, *watering hole*, redirecionamento e *man-in-the-browser* são algumas sub-categorias conhecidas nesta categoria. Já os *Web Application Attacks* são considerados tentativas diretas ou indiretas de explorar uma vulnerabilidade ou fraqueza nos serviços e aplicativos na *Web*, abusando de suas APIs, ambientes de tempo de execução ou serviços, ou seja, o simples abuso de um componente ativo ou passivo de um software disponível via *web*. Esses ataques se sobrepõem aos baseados na *web* com bastante frequência devido aos serviços compartilhados no lado do aplicativo e na superfície de ataque no lado da ameaça. Os aplicativos da *Web* estão se tornando alvos mais interessantes para os adversários, à medida que mais empresas se tornam dependentes dos serviços da *Web*, tanto em receita quanto em reputação. Como exemplo, a injeção de *SQL*, *cross-site scripting* (XSS) e a inclusão de arquivos maliciosos em sites (SINGH et al., 2019) que pertencem a essa categoria.

• *Spam*: Corresponde ao uso abusivo de tecnologias de *e-mail* e mensagens para inundar usuários com mensagens não solicitadas. Embora esteja continuamente reduzindo em volume, o spam ainda é um dos principais vetores de ataque observados na internet (SFAKIANAKIS et al., 2019), devendo ser claramente classificado.

• *Scan*: Corresponde a ataques que enviam solicitações a um sistema para descobrir pontos fracos. Isso inclui também algum tipo de processo de teste para coletar informações sobre *hosts*, serviços e contas. Exemplos: fingerd, consulta DNS, ICMP, SMTP, varredura de portas (SFAKIANAKIS et al., 2019).

• *Botnet*: Corresponde a identificação de máquinas infectadas (computador ou redes de

computadores zumbis) derivadas da exploração de vulnerabilidades comuns, força bruta e outras técnicas comuns de infecção. Além disso, o "controlador de *botnets*" facilita e fornece uma plataforma para diferentes ataques maliciosos. Os exemplos vão desde a distribuição de spam, infecções por *malware*, reutilização de credenciais, mineração de bitcoins e, mais comumente, DDoS (DHAYAL; KUMAR, 2018).

• Violação de Ativo: Corresponde a identificação de manipulação física/dano/roubo/-perda. Embora os ataques físicos não sejam uma ameaça cibernética real, eles ainda são possíveis nas empresas hoje em dia. Os ataques físicos podem não ser tão populares quanto outros tipos de ameaças cibernéticas, mas eles ainda podem levar a violações de dados ou sabotagem. O acesso físico a um dispositivo ainda dá a oportunidade aos invasores de realizar suas atividades maliciosas.

• Vazamento de Informação: Corresponde a identificação de ocorrências de violação de acesso, tal como a de informação que fica erroneamente acessível ao público, seja por ter sido mal protegida ou por algum hacker ter tido acesso a ela após explorar alguma falha de segurança. As empresas estão cada vez mais preocupadas com os dados que residem nos seus dispositivos e, mais especificamente, sobre a perda ou vazamento de dados e propriedade intelectual, especialmente na era da Lei Geral de Proteção de Dados (LEI, 2018), que menciona no seu artigo 46: "*Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.*".

• Tentativas de Invasão/Exploração de Vulnerabilidades: Corresponde a identificação de vulnerabilidades conhecidas ou tentativas de login. Inclui tentativas de comprometimento de um sistema ou de interrupção de qualquer serviço, explorando vulnerabilidades com um identificador padronizado. Exemplos: estouro de buffer, *backdoor*, script entre sites, tentativas de login por adivinhação, quebra de senhas e força bruta (SCHMITT et al., 2018).

• Violação de *Copyright*: Corresponde ao oferecimento cópias de software comercial não licenciado ou outros materiais protegidos por direitos autorais (SCHMITT et al., 2018).

• *Phishing*: Corresponde a identificação de mecanismos para criar mensagens que usam técnicas de engenharia social para que o destinatário seja atraído e "morda a isca". Comumente distribuição de mensagens de *e-mail* para abrir um arquivo anexo contendo software malicioso, clicar em um URL inseguro, entregar suas credenciais através de páginas de aparência legítima,

enviar dinheiro, dentre outros (GUPTA; SINGHAL; KAPOOR, 2016).

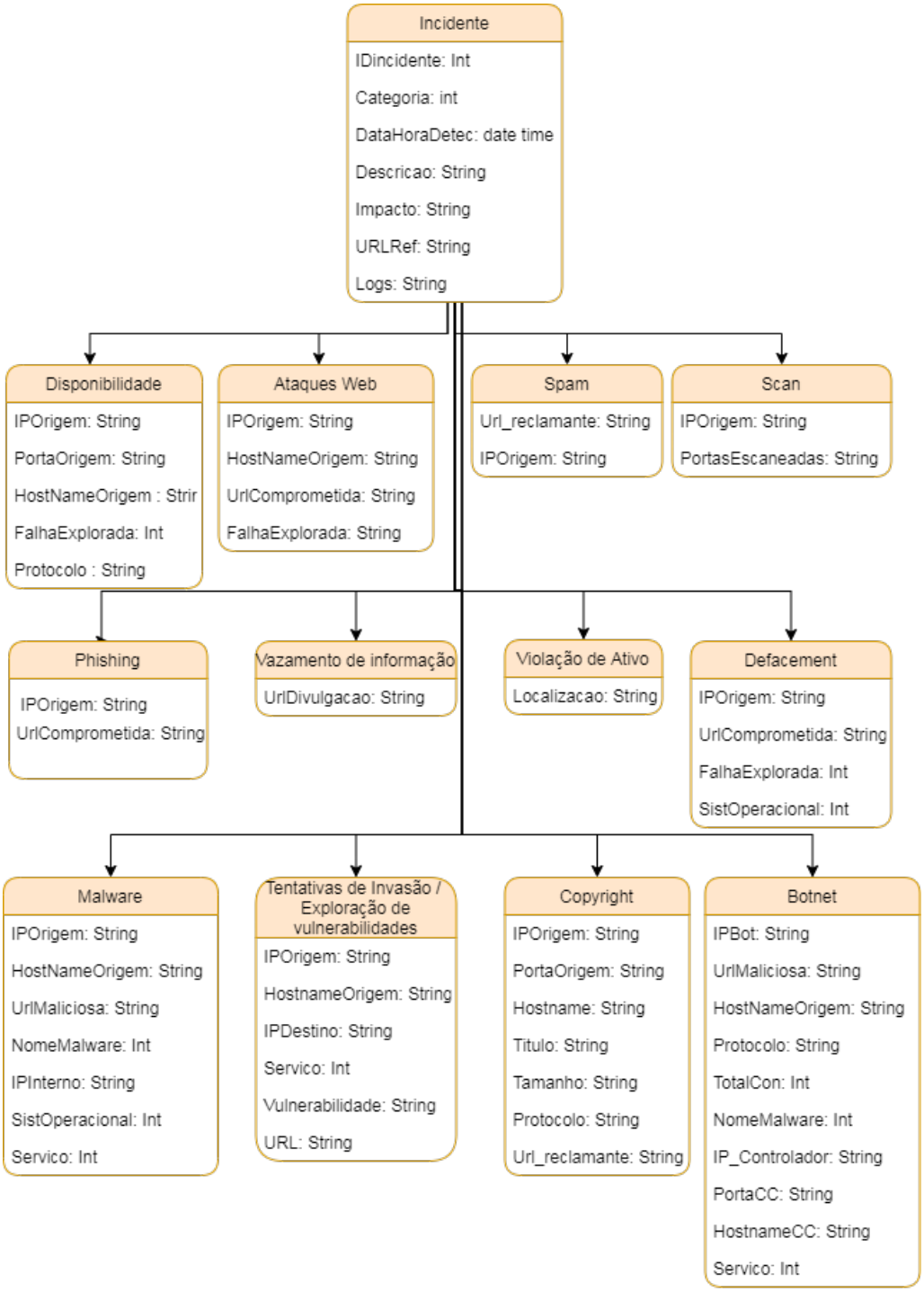
• *Defacement*: Corresponde a identificação de técnica de invasão que consiste em conseguir acesso a um site, no qual seja possível modificar a página inicial. Normalmente essa técnica é utilizada por hacktivistas para manifestar opiniões sobre um determinado assunto (CTIR-GOV, 2020).

4.3 SELEÇÃO DE ATRIBUTOS

Considerado uma dada categorização, tal como a proposta na seção 4.2, quando da ocorrência de incidentes, ações para a sua resolução são necessárias. Neste sentido, ter modelos estruturados e padronizados para descrever um incidente é uma necessidade. Considerando que um incidente pode ser definido tecnicamente como uma entidade com atributos, e que cada atributo é uma tupla <nome, valor>, esta seção apresenta uma proposta de conjunto de atributos para a identificação de incidentes que pertencem as categorias definidas na seção 4.2.

Inicialmente, foi realizado uma análise para definir os atributos necessários para compor uma base de casos. Para este trabalho foram analisados os atributos e propriedades indicados nos modelos de representação IODEF (DANYLIW, 2016) e STIX (MITRE, 2019), os quais possuem uma vasta aceitação no mercado e na academia. Como resultado, um novo modelo de representação de incidente, com atributos por categoria, é proposto. A Figura 6 ilustra esse novo modelo considerando as categorias propostas na seção 4.2 com o tipo de cada atributo. Destaca-se que as classes correspondentes a cada categoria possuem atributos que são herdados da classe principal Incidente, bem como atributos específicos que permitem caracterizar os tipos de incidente da classe. Destaca-se ainda, que diferente do modelo proposto em (COLOMÉ; NUNES; SILVA, 2019), este modelo foi construído a partir de uma nova categorização e seus atributos, que derivam de padrões de representação amplamente difundidos, utilizados e aceitos.

Figura 6 – Atributos por categoria de Incidentes.



Fonte: Autor.

A seguir apresenta-se a definição dos atributos por classe/categoria do modelo.

Os atributos da classe Incidente e que são herdados pelas demais classes são:

- *IDincidente*, identificador do incidente;
- Categoria, apresenta o tipo de incidente;

- *DataHoraDetec*, data e hora da detecção do incidente;
- Descricao, descrição do incidente;
- Impacto, define o impacto na organização (Alto, Médio, Baixo);
- *URLRef*, url de referência para o incidente;
- *Logs*, *log* com evidências do incidente.

Os demais atributos do modelo podem ser específicos ou comuns entre categorias.

A categoria Disponibilidade (DoS/DDoS) possui o *IPOrigem*, IP que realizou o ataque; *PortaOrigem*, Porta aberta no *host* de origem para realizar o ataque; *HostNameOrigem*, nome do *host* origem que executa o ataque; *FalhaExplorada*, são as vulnerabilidades exploradas pelo atacante; Protocolo, protocolo utilizado no ataque.

No caso da categoria Ataques *Web*, alguns atributos se repetem, tais como *IPOrigem*, *HostNameOrigem* e *FalhaExPlorada*, mantido as mesmas definições, e é incluído um novo, o atributo *UrlComprometida*, url do servidor *web* que foi invadido.

Na categoria *Malware* os atributos que se repetem são: *IPorigem* e *HostNameOrigem*. Os outros atributos dessa categoria são: *UrlMaliciosa*, url infectada que promove ataques, golpes e fraudes; *NomeMalware*, referência ao *malware* ou falha que está presente no *host* infectado; *IPInterno*, endereço IP do *host* infectado; *SistOperacional*, sistema operacional do *host* infectado; *Servico*, identificação do principal serviço em execução no *host* servidor, ou apenas *host* cliente.

A categoria *Spam* apresenta o *IPOrigem* que se repete e o atributo *Url_reclamante*, URL do site oficial da instituição reclamante da fraude. A categoria *Scan* apresenta o *IPOrigem* que já foi mencionado e *PortasEscaneadas*, são as portas de conexão/serviço escaneadas pelo atacantes.

A categoria *Botnet* apresenta como atributos comuns a outras categorias: *UrlMaliciosa*, *HostNameOrigem*, Protocolo, *NomeMalware* e *Servico*. As restantes são *IPBot*, endereço IP que está realizando o ataque; *TotalCon*, total de conexões do *host* infectado; *IP_Controlador*, endereço IP da *botnet* com quem o *IPBot* está se comunicando para receber e enviar instruções; *PortaCC*, porta utilizada para se comunicar com a *botnet*; *HostnameCC*, nome do *host* controlador.

A categoria Violação de Ativo apresenta o atributo *Localizacao*, local físico que está o ativo de rede.

A categoria *Phishing* apresenta os atributos que já foram mencionados: *IPOrigem* e *UrlComprometida*.

A categoria Vazamento de Informação possui o atributo *UrlDivulgacao*, URL que foi divuldado o vazamento de informações.

A categoria Tentativas de Invasão / Exploração de Vulnerabilidades possui os atributos *IPOrigem*, *HostNameOrigem* e *Servico* comuns a outras categorias. Vulnerabilidade, Vulnerabilidades presentes no *host*; URL, URL do servidor alvo.

A categoria Violação de *Copyright* possui os seguintes atributos comuns: *IPOrigem*, *PortaOrigem*, *Hostname*, Protocolo e *Url_reclamante*. E também os seguintes atributos específicos: Titulo, título do arquivo da violação de *copyright*; Tamanho, tamanho do arquivo em bytes.

A categoria *(Defacement)* possui os atributos *IPOrigem*, *URLComprometida*, *FalhaExplorada* e *SistOperacional*, todos abordados anteriormente.

Na Tabela 5 é apresentado o conjunto de classes e atributos selecionados do modelo IODEF e os objetos do STIX com as suas respectivas propriedades. A Figura ilustra a correlação entre IODEF e STIX e a correlação destes com as classes e atributos propostos como novo modelo neste trabalho. Destaca-se que este mapeamento, além de demonstrar o alinhamento do novo modelo de dados ao dos padrões de representação IODEF e STIX, demonstra a versatilidade do modelo para receber e fornecer relatórios sobre incidentes reportados nestas duas importantes representações.

O modelo de dados pré-concebido pelo IODEF foi projetado para descrever todos os atributos possíveis e necessários em uma troca de incidentes de segurança, permitindo assim inúmeras possibilidades para representações de dados sobre incidentes. Além disso, no modelo de dados IODEF existem vários atributos e classes que podem ser utilizados de acordo com a necessidade das organizações.

Neste trabalho, as classes do modelo IODEF consideradas no novo modelo são apresentadas a seguir:

a) Classe *IODEF-Document*: a classe de nível mais alto do modelo de dados IODEF V2. As classes agregadas são: Incident e AdditionalData. A classe *Incident* contém informações relacionadas a um único incidente. A classe *AdditionalData* pode ser usada para aplicar extensões. Para atender ao modelo proposto foram selecionados os seguintes atributos:

- *Version*: é um atributo obrigatório, o número da versão de especificação IODEF no qual

Tabela 5 – Mapeamento de Atributos e Propriedades.

Classes IODEF V2	Atributos IODEF V2	Objetos STIX V2.1	Propriedades STIX V2.1	Atributos propostos	Classes propostas
IncidenteID	IncidenteID	Attack Pattern	id	codigo	Comum a todas
DetectTime	ntpstamp	Attack Pattern	created	DataHotaDetec	Comum a todas
Assessment	IncidentCategory	Attack Pattern	type/name	Categoria	Comum a todas
Discovery	description	Attack Pattern	description	Descricao	Comum a todas
Address	ipv4-addr	IPv4 Address	type/value	IPOrigem	DDos, Ataques Web, Malware, Spam, Scan, Phishing, Tentativas de Invasão, Defecement, Copyright
Address	ipv4-addr	IPv4 Address	type/value	IPBot	Botnet
DomainData	Name	domain-name	type/value	HostNameOrigem	DDos, Ataques Web, Malware, Tentativas de Invasão, Copyright
DomainData	Name	domain-name	type/value	HostNameCC	Botnet
Service	ServiceName	network-traffic	type/protocols	Protocolo	DDos, Botnet, Copyright
Service	port	network-traffic	type/src_port	PortaOrigem	DDoS
Service	port	network-traffic	type/src_port	PortaCC	Botnet
Service	Portlist	network-traffic	type/dst_port	PortasEscaneadas	Scan
Reference	URL	external-reference	source_name/url	url_ref	Comum a todas
Assessment	severity	Custom	impact	Impacto	Comum a todas
RecordData	RecordItem	Custom	logs	logs	Comum a todas
Node	Location	Location	type/description	Localizacao	Violação de Ativo
Method Class	sci:Vulnerability	Vulnerability	type/name	FalhaExplorada	DDoS, Ataques Web, Defecement
RelatedActivity	URL	external-reference	source_name/url	UrlComprometida	Ataques Web, Phishing, Defecement
RelatedActivity	URL	external-reference	source_name/url	UrlMaliciosa	Botnet, Malware
AttackPhase	URL	external-reference	source_name/url	Url_reclamante	Spam, Copyright
AttackPhase	URL	external-reference	source_name/url	UrlDivulgacao	Vazamento de Informação
AttackPhase	URL	external-reference	source_name/url	URL	Tentativa de Intrusão
NodeRole	category/ c2-server	ipv4-addr	type/value	IP_Controlador	Botnet
System	OperatingSystem	Malware	operating_system_refs	SistOperacional	Malware, Defecement
Reference	ReferenceName	Malware	malware_types	NomeMalware	Botnet, Malware
Incident/ AdditionalData	total_connections	process	type/opened_connection_refs	TotalCon	Botnet
Incident/ AdditionalData	title	Custom	title	Titulo	Copyright
Incident/ AdditionalData	filesize	Custom	size	Tamanho	Copyright

Fonte: Autor.

este documento está em conformidade. O valor deste atributo deve ser "2,00";

- *Lang*: é um atributo opcional, com uma lista enumerada que identifica o idioma, na qual os valores são descritos na [RFC5646].

b) Classe *Incident*: esta classe foi atualizada na versão 2 do IODEF para representar informações de tempo e fluxo de trabalho, bem como classes agregadas (descritas nos próximos itens). O atributo selecionado da classe Incident foi:

- *Purpose*: é um atributo obrigatório com uma lista enumerada que descreve uma justificativa pelo qual o documento foi criado. As enumerações possíveis são: *traceback*, *mitigation*, *reporting*, *watch* e *other*;

c) Classe *IncidentID*: esta classe representa um número exclusivo no contexto do CSIRT. Ele serve como um identificador para um incidente ou um identificador de documento ao compartilhar indicadores. Atributo selecionado:

- *IncidenteID*: um número de rastreamento de incidente atribuído a esse incidente pelo CSIRT que gerou o documento IODEF.

d) Classe *DetectTime*: a classe DetectTime registra a hora em que o incidente foi detectado, a qual utiliza o atributo *ntpstamp*.

e) Classe *Assessment*: descreve as repercussões do incidente para a vítima. Para descobrir o grau de impacto causado é necessário ter um mapeamento de ativos ou redes com o tipo de criticidade. No caso de um servidor de aplicação será considerado com o nível de criticidade alta e um *host* de usuário será classificado como nível baixo. O impacto desses dois *hosts* será diferente, pois o servidor *web* vai afetar milhares de usuários enquanto o *host* de usuário vai afetar poucos. As classes agregadas selecionadas para o modelo proposto são:

- *IncidentCategory*: fornece uma descrição de texto em formato livre que categoriza o tipo de incidente;

- *SystemImpact*: fornece uma caracterização técnica do impacto do incidente (baixa, média, alta);

f) Classe *Address*: representa um endereço de *hardware* (Camada 2), rede (Camada 3) ou aplicação (Camada 7). Para este trabalho é utilizado o endereço de rede, o qual é referenciado pelo atributo *ipv4-addr*.

g) Classe *DomainData*: descreve um nome de domínio e metadados associados a esse domínio. O atributo utilizado é o *name*, que é o nome do domínio de um *host*. Este atributo está associado a dois atributos propostos, que são o *HostNameOrigem* e *HostNameCC*, pois pertencem a classes propostas diferentes.

h) Classe *Service*: descreve um serviço de rede, que pode ser um protocolo, porta, campo de cabeçalho de protocolo e aplicação fornecendo ou usando o serviço. Foram utilizados os atributos *ServiceName*, nome do protocolo; *Port*, número da porta; e *PortList*, uma lista do números de portas. O atributo *Port* está associado a dois atributos propostos, que são o *PortOrigem* e *PortaCC*, pois pertencem a classes propostas diferentes.

i) Classe *Discovery*: descreve como um incidente foi detectado. É importante para o analista de segurança descrever como o incidente foi descoberto para mitigar futuras ameaças. As detecções podem basear-se em notificações externas, ferramentas de monitoração de rede como um IDS (sistema de detecção de intrusão), dados de *log* e investigação manual. A classe

agregada utilizada é a *Description*, que fornece uma descrição de texto em formato livre de como esse incidente foi detectado.

j) Classe *Reference*: é uma referência externa a informações relevantes como vulnerabilidade, alerta IDS, nome de *malware*, aviso ou técnica de ataque. Foi utilizado a classe agregada URL para o atributo proposto *url_ref* e a classe agregada *ReferenceName* para o atributo *NomeMalware*.

l) Classe *RecordData*: descreve ou faz referência a dados de *log* ou auditoria de um dado tipo de ferramenta e fornece os resultados. Foi utilizada a classe agregada *RecordItem* que armazena log, auditoria ou dados forenses para dar suporte as conclusões feitas durante a análise de um incidente.

m) Classe *Node*: identifica um sistema, ativo ou rede e sua localização. Foi utilizado a classe agregada *Location*, a qual apresenta uma descrição de texto da localização física.

n) Classe *Method*: descreve as táticas, técnicas, procedimentos ou fraquezas usadas pelo agente de ameaça em um incidente. Foi utilizado a classes agregada *Vulnerability*, a qual faz referência a [RFC7203], que trata sobre uma classe de extensão de vulnerabilidades.

o) Classe *RelatedActivity*: relaciona as informações descritas no documento a incidentes ou atividades observadas anteriormente e permite a atribuição a um ator ou campanha específica. A classe agregada URL é mapeada para dois atributos propostos, a *UrlComprometida* e a *UrlMaliciosa*, ambas pertencentes a classes propostas diferentes.

p) Classe *AttackPhase*: descreve uma fase específica do ciclo de vida do ataque. Foi utilizado a classe agregada URL para descrever um recurso da fase do ataque, a qual está relacionada a três atributos propostos: *Url_reclamante*, *UrlDivulgacao* e URL.

q) Classe *NodeRole*: descreve a função de um sistema, ativo ou rede específica. Foi mapeado o atributo categoria com valor *category/ c2-server*, servidor de comando e controle malicioso para o atributo proposto *IP_Controlador*.

r) Classe *System*: descreve um sistema ou rede envolvida em um evento. Neste caso foi utilizado a classe agregada *OperatingSystem* que serve para identificação do sistema operacional em execução no sistema.

s) Classe *Incident/AdditionalData*: serve como um mecanismo de extensão para informações que não são representadas no modelo de dados. Neste trabalho esta classe foi usada para estender o modelo IODEF para os seguintes atributos propostos: *TotalCon*, Titulo e Tamanho.

Diferente do modelo de dados do IODEF, no STIX são especificadas propriedades co-

muns que podem existir em objetos. Cada tipo de objeto STIX define quais propriedades comuns são necessárias, quais são opcionais e quais não estão em uso. Para o modelo de dados proposto nesta seção, foi utilizado do STIX as propriedades *ID* e *created*, as quais são comuns aos objetos. Além destas, do modelo STIX foi mapeado os seguintes objetos e propriedades de interesse:

a) Objeto *Attack Pattern*: descreve maneiras pelas quais os adversários tentam comprometer os alvos. Tem como finalidade categorizar ataques, generalizar ataques específicos aos padrões que eles seguem e fornecer informações detalhadas sobre como os ataques são realizados. As propriedades utilizadas deste objeto são: o *type*, que descreve o valor da propriedade, neste caso deve ser *Attack Pattern*; o *name*, nome usado para identificar o padrão de ataque, correspondente ao atributo proposto categoria; o *description*, descrição que fornece mais detalhes e contexto sobre o Padrão de Ataque, incluindo o objetivo e suas principais características. Este objeto é comun a todas as classes propostas, pois corresponde a classe Categoria, conforme apresentado no mapeamento da Tabela 5.

b) Objeto *IPv4 Address*: representa um ou mais endereços IPv4 expressos usando a notação de rede de 4 octetos (CIDR). As propriedades utilizadas deste objeto são: o *type*, que descreve o valor da propriedade, neste caso deve ser *ipv4-addr*; o value, que especifica os valores de um ou mais endereços IPv4 usando a notação CIDR. A propriedade *value* foi mapeada para os seguintes atributos propostos: *IPOrigem*, *IPBot* e *IP_Controladora*.

c) Objeto *Domain Name*: representa as propriedades de um nome de domínio de rede. As propriedades utilizadas deste objeto são: o *type*, que descreve o valor da propriedade, neste caso deve ser *domain-name*; o *value*, especifica o valor do nome do domínio. A propriedade *value* foi mapeada para os atributos propostos: *HostNameOrigem* e *HostNameCC*.

d) Objeto *Network Traffic*: representa o tráfego de rede arbitrário que se origina de uma fonte e é endereçado a um destino. As propriedades utilizadas deste objeto são: o *type*, que descreve o valor da propriedade, neste caso deve ser *network-traffic*; o *protocols*, especifica os protocolos observados no tráfego de rede, os nomes de protocolo devem vir dos nomes de serviço definidos no Registro de nomes e números de porta do serviço da IANA (*Internet Assigned Numbers Authority*) (SERVICE NAME AND TRANSPORT PROTOCOL PORT NUMBER REGISTRY, 2020); o *src_port*, especifica a porta de origem usada no tráfego de rede, como um número inteiro, o valor da porta deve estar no intervalo de 0 a 65535; o *dst_port*, especifica a porta de destino usada no tráfego de rede, como um número inteiro, o valor da porta deve estar

no intervalo de 0 a 65535. A propriedade *src_port* foi mapeada para os atributos propostos: *PortaOrigem* e *PortaCC*, no caso do *dst_port*, este foi mapeado para *PortasEscaneadas*.

e) Objeto *External Reference*: são usadas para descrever informações representadas fora do STIX. As propriedades utilizadas deste objeto são: o source_name, que descreve nome da fonte na qual a referência externa é definida (sistema, registro, organização etc.); a url, é uma referência de URL para um recurso externo. A propriedade *url* foi mapeada para os atributos propostos: *url_ref*, *UrlComprometida*, *UrlMaliciosa*, *Url_reclamante*, *UrlDivulgacao* e URL. Estes atributos serão diferenciados pela propriedade *source_name*.

f) Objetos e propriedades personalizados: haverá casos em que algumas informações podem ser aprimoradas adicionando objetos ou propriedades que não existem no modelo STIX. Isso torna esse modelo interoperável. Foi criado o objeto *Custom* para alocar as propriedades *impact*, *logs*, *title* e *size* no modelo STIX. A primeira para ser relacionado com o atributo proposto impacto; a segunda para o atributo *logs*, comuns a todas as categorias; a terceira foi mapeada para o atributo titulo; e a quarto foi mapeada com o atributo Tamanho. Essas duas últimas vinculadas à categoria violação de *copyright*.

g) Objeto *Location*: representa uma localização geográfica. As propriedades utilizadas deste objeto são: o *type*, que descreve o valor da propriedade, que neste caso deve ser *location*; o *description*, uma descrição usada para identificar o local. A propriedade *location* foi mapeada para o atributo proposto Localizacao.

h) Objeto *Vulnerability*: é uma fraqueza ou defeito nos requisitos, projetos ou implementações da lógica computacional (por exemplo, código) encontrada no software e em alguns componentes de *hardware* (por exemplo, firmware) que podem ser explorados diretamente para impactar negativamente a confidencialidade, integridade ou disponibilidade desse sistema. As propriedades utilizadas deste objeto são: o *type*, que descreve o valor da propriedade, neste caso deve ser *vulnerability*; o *name*, um nome usado para identificar a vulnerabilidade. A propriedade name foi mapeada para o atributo proposto *FalhaExplorada*.

i) Objeto *Malware*: representa código malicioso. Geralmente, refere-se a um programa que é inserido em um sistema de forma oculta. A intenção é comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicativos ou sistema operacional da vítima ou incomodar ou perturbar a vítima. As propriedades utilizadas deste objeto são: o *type*, que descreve o valor da propriedade, que neste caso deve ser *malware*; o *operating_system_refs*, sistema operacional no qual a família ou instância do código malicioso é executada; o *malware_types*, uma

categorização para o *malware* que está sendo descrito. A propriedade *operating_system_refs* foi mapeada para o atributo proposto *SistOperacional*, e a *malware_types* para o atributo *NomeMalware*.

j) Objeto *Process*: representa propriedades comuns de uma instância de um programa de computador, conforme executado em um sistema operacional. As propriedades utilizadas deste objeto são: o *type*, que descreve o valor da propriedade, que neste caso deve ser process; o *opened_connection_refs*, especifica a lista de conexões de rede abertas pelo processo, como uma referência a um ou mais objetos de Tráfego de rede. A propriedade *opened_connection_refs* foi mapeada para o atributo proposto *TotalCon*.

Finalmente, salienta-se que o processo de mapeamento dos modelos IODEF e STIX para o novo modelo de dados (vide Tabela 5) foi realizado em duas etapas consecutivas. Primeiro, identificada e revisada na literatura as representações de dados mais relevantes e de última geração (MENGES; PERNUL, 2018). Nesta revisão, foram identificados conceitos para representar os incidentes. Na segunda etapa, as estruturas e características desses formatos foram analisadas para validar com a revisão da literatura. A validação ocorreu por meio de correspondência entre os modelos. Esse processo resultou na identificação de elementos fundamentais, como classes, objetos, propriedades e relacionamentos dos incidentes. Esses elementos foram então finalmente combinados para criar o modelo de atributos.

4.4 REPRESENTAÇÃO DE CASO

Um caso é um "conhecimento contextualizado que representa uma experiência que ensina uma lição fundamental para alcançar os objetivos do raciocínio" (AAMODT; PLAZA, 1994). Nesse sentido, um caso pode ser considerado como um registro de experiências que contêm conhecimento explícito ou tácito, que não é apenas um resumo de uma solução para um problema anterior, mas também pode ser reutilizado na solução de novos problemas semelhantes. Em geral, um caso compreende:

- *Descrição do problema*, que descreve o caso ocorrido, como os dados de um incidente que aconteceu em um dado momento;
- *Solução do problema*, apresenta a solução para o problema especificado na descrição e pode ser uma ação, um plano ou uma informação útil para o usuário;

Cabe salientar que, do ponto de vista computacional, o "caso" pode corresponder a uma

tupla <problema, solução>, onde o problema pode estar associado ao incidente e a solução relacionada ao plano de tratamento daquele incidente específico (conhecimento do especialista sobre como tratar o incidente).

Como o processo de recomendação de ações proposto neste trabalho para o tratamento de incidentes é baseado em CBR e tem como base a utilização de casos, a representação de um caso corresponde a um registro de uma experiência passada armazenado em uma base de casos, e que pode ser descrito por meio de um grupo de atributos.

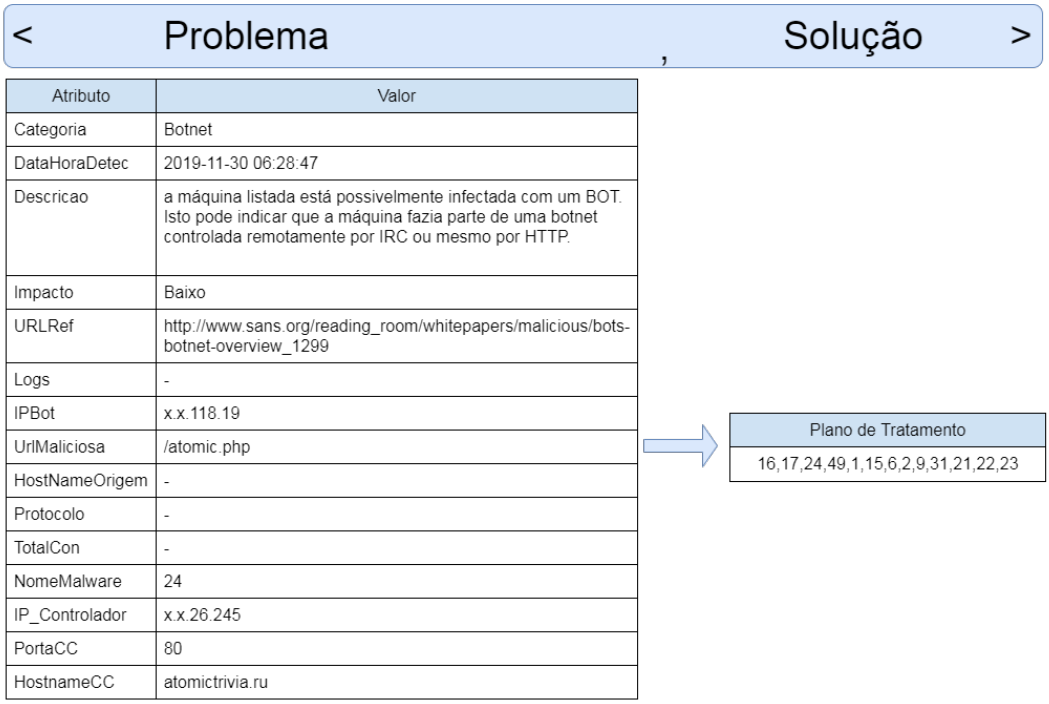
Para definir um caso para os incidentes relacionados à segurança, foi definido na seção 4.3 um conjunto de atributos por categoria de incidente, os quais podem ser empregados na descrição de um caso pertencente a uma dada categoria. Os atributos do caso são utilizados pelo CBR no cálculo de similaridade empregado para recuperação, a partir de um novo caso/incidente, dos casos mais similares da base de casos. Os atributos são assim usados para descrever o problema (categoria do incidente e detalhes sobre ele) e recuperar a solução (planos de tratamentos vinculados aos casos recuperados). As categorias e atributos definidos nas seções 4.2 e 4.3 constituem assim o conjunto de elementos chave na representação do caso, dado que permite a representação do problema e a recuperação dos planos de tratamento associados a ele.

A Figura 7 ilustra um exemplo de como este processo de representação de caso permite a descrição do problema num caso real. O problema descrito por uma série de atributos do incidente e a solução descrita por um plano de tratamento. Os atributos elencados na figura correspondem ao de um incidente categorizado como *botnet* e os respectivos valores correspondem a um caso de *botnet* em particular. Diferentes incidentes do tipo *botnet* serão enquadrados na categoria *botnet*. Cabe salientar que nem todos os atributos da categoria podem ser fornecidos junto com a descrição do incidente, como por exemplo o que ocorreu com os atributos Protocolo e *TotalCon* no caso da Figura 7. Porém, a falta de descrição não impede a análise de similaridade entre casos, dado que os atributos não preenchidos são desconsiderados na análise.

4.5 REPRESENTAÇÃO DO PLANO DE TRATAMENTO

No tratamento de um incidente, o plano de tratamento deve refletir um conjunto de ações que a equipe de segurança entende que devem ser realizadas para solucionar o incidente. Esse conjunto de ações, ou plano de tratamento, é elaborado após a resolução de incidentes e reflete o conhecimento dos especialistas no tratamento dos problemas enfrentados no dia-dia.

Figura 7 – Representação de um caso, via atributos do Problema.



Atributo	Valor
Categoria	Botnet
DataHoraDetec	2019-11-30 06:28:47
Descricao	a máquina listada está possivelmente infectada com um BOT. Isto pode indicar que a máquina fazia parte de uma botnet controlada remotamente por IRC ou mesmo por HTTP.
Impacto	Baixo
URLRef	http://www.sans.org/reading_room/whitepapers/malicious/bots-botnet-overview_1299
Logs	-
IPBot	x.x.118.19
UrlMaliciosa	/atomic.php
HostNameOrigem	-
Protocolo	-
TotalCon	-
NomeMalware	24
IP_Controlador	x.x.26.245
PortaCC	80
HostnameCC	atomictrivia.ru

Plano de Tratamento
16,17,24,49,1,15,6,2,9,31,21,22,23

Fonte: Autor.

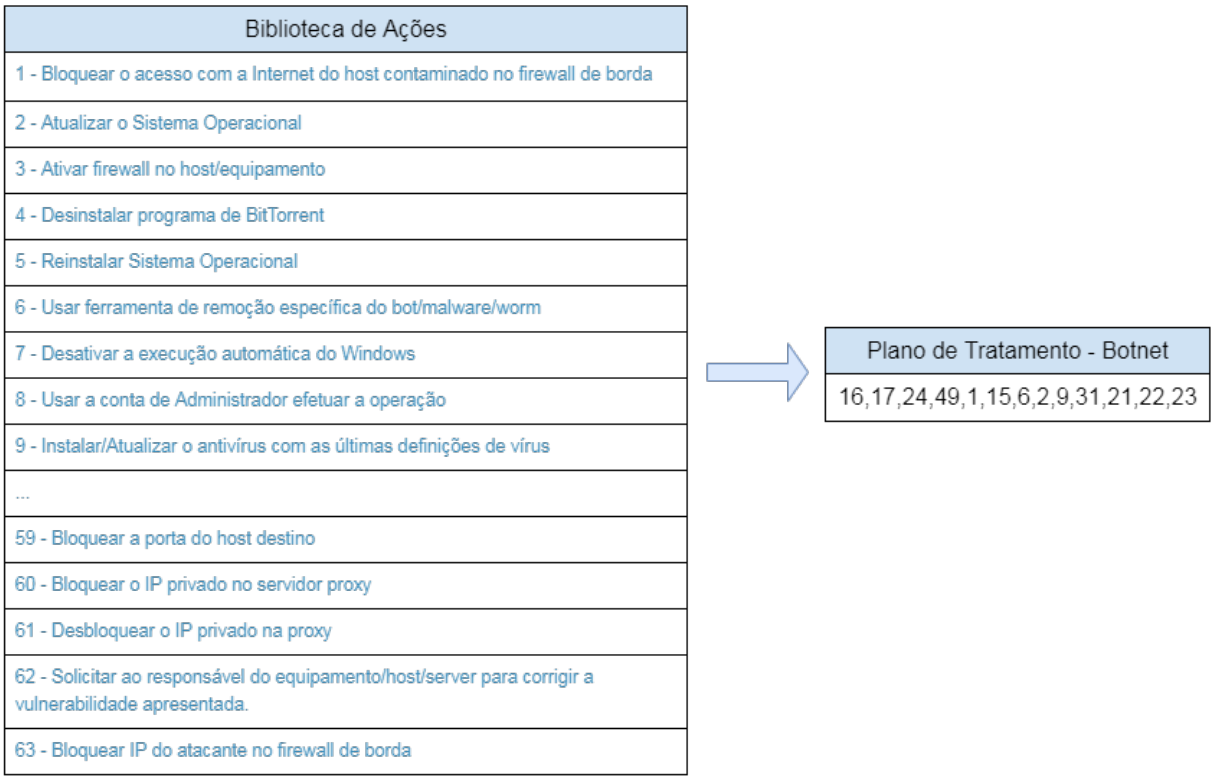
Na prática, junto à representação de um caso, o plano de tratamento pode ser composto por uma sequência de passos ordenados que representam ações específicas. As ”ações“ definem atividades práticas pontuais que o especialista deve realizar ao tratar um incidente, tal como bloquear um determinado IP no *firewall* ou instalar/atualizar o antivírus com as últimas definições de vírus. O conjunto de todas as ações mapeadas pela equipe de especialistas compõe o que denomina-se ”Base de Ações“. Essa base deve ser atualizada constantemente, seja para novos incidentes ou para os já conhecidos, com aprimoramento de conhecimento dos especialistas. Esse ”aprendizado“ através do banco de ações deve ser mantido fora da base de casos, mas a disposição dos especialistas que montam planos de tratamento para inserção nos casos da base de casos. Logo, as ações criadas para tratar os casos já solucionados podem ser compartilhadas para a criação de novos planos ligados a novos incidentes, ou seja, na criação de novos casos para a base de casos. Naturalmente, diferentes combinações de ações resultam em diferentes planos de tratamento e estas combinações é que, de fato, expressam o conhecimento dos especialistas.

Essa metodologia fará com que a retenção de ações aumente o número delas de acordo com a diversidade de incidentes que surgirem, resultando em um maior conhecimento na base de ações e de casos. Sempre que não existir uma solução para um caso apresentado, o espe-

cialista deverá informar para a base de ações os novos passos de tratamento para o referido caso e posteriormente compor o plano de tratamento a partir das ações armazenadas na base de ações. Isto torna a base de ações uma fonte de consulta em constante incremento de aprendizado (ações possíveis de serem realizadas). A biblioteca de ações representa assim uma fonte de informações que viabiliza que o conhecimento de um grupo de especialistas para solucionar os incidentes seja incorporado aos planos de tratamentos presentes na base de casos, potencializando o reúso de informações/ações e planos.

A Figura 8 ilustra uma biblioteca de ações e o plano de tratamento do caso representado na Figura 7, desdobrado num plano de ações para o usuário. Note que o respectivo plano de tratamento apresentado ao usuário deriva da sequência numérica de ações do plano de tratamento armazenado no caso. As descrições das ações são recuperadas da base de ações. Essas ações passam por revisões de forma periódica e podem ser alteradas, excluídas ou criado novas. Essa avaliação deve ser feita por especialistas, pois no momento do tratamento do incidente é verificado o quão eficiente foi a solução e no caso de insucesso o plano ou as ações podem ser readaptados. Essa base de ações deve ser mantida de forma segura, pois é um dado valioso para a organização e numa situação de vazamento da base de casos, o atacante não terá acesso aos planos de tratamento efetivos devido as ações estarem codificadas. Por isso a base de casos armazena apenas os códigos das ações.

Figura 8 – Plano de tratamento derivado de uma biblioteca de ações.



Fonte: Autor.

4.6 RECUPERAÇÃO DE CASOS

A recuperação de casos é o processo de localizar, dentro de uma base de casos, os incidentes mais parecidos com o incidente atual. Para executar a recuperação eficaz de casos, deve haver critérios de seleção que determinam como um caso é considerado adequado para recuperação e um mecanismo para controlar como a base de casos é pesquisada. Os critérios de seleção são necessários para determinar qual é o melhor caso a ser recuperado, determinando a proximidade do caso atual com os casos armazenados (PAL; SHIU, 2004). Neste sentido, a escolha de um mecanismo eficiente de recuperação de casos se torna crucial.

A atividade de recuperação utiliza mecanismos que contemplam três etapas: (i) avaliação da situação – quando identifica características que serão usadas para busca na base de casos, (ii) busca – recupera casos com potencial de serem similares utilizando mecanismos que consiste em relacionar a descrição do caso atual com os casos existentes na base de casos, e (iii) seleção – retorna uma lista de casos, dentre os selecionados na consulta, ordenados pelo grau de similaridade de acordo com um critério de seleção.

4.6.1 Avaliação da Situação

Para a avaliação da situação, a proposta deste trabalho é utilizar os atributos relacionados às categorias de incidentes previamente selecionadas e detalhadas. Ainda, dentre o conjunto de todos os atributos, utilizar numa análise apenas os relacionados à uma dada categoria. Para tal, este trabalho explora a ponderação de atributos (SILVA et al., 2010).

A identificação da categoria é de forma automática, na qual é realizada pelos valores dos atributos de um novo incidente, e posteriormente mapeado a uma dada categoria com os respectivos atributos propostos. Assim como também é verificado o atributo IP para a identificação automática do tipo de serviço, neste momento é realizado uma consulta em um banco de dados com todos os ativos cadastrados da organização. Cabe destacar que são armazenados os IPs relacionados ao tipo de serviço. Caso o serviço seja do tipo ”SERVIDOR“ o plano de tratamento será diferente de um outro tipo ”CLIENTE“. Mas existem outros tipos de serviços tais como: SMTP, DNS, *PROXY*, NAT, *WEB* e SSH. É possível inserir novos serviços nesta base de dados.

A ponderação de atributos (atribuição de pesos) no modelo CBR afeta na recuperação dos casos. Atributos mais importantes podem receber peso maior, enquanto atributos menos importantes podem ter peso menor. Atributos irrelevantes podem ter peso zero para serem desconsiderados. Deste modo, a recuperação do caso mais relevante pode ser determinada pela similaridade presente nos atributos mais importantes, ou seja, a recuperação de casos pode priorizar atributos relevantes via a ponderação. Neste trabalho, é proposto que os pesos dos atributos sejam determinados previamente por especialistas, mas que também possam ser informados no momento de uma consulta CBR.

Esta etapa permite que a equipe de segurança visualize, edite e faça ajustes nos valores de atributos do incidente relatado, bem como determine os valores de peso dos atributos para uso na consulta CBR. Desta forma, a abordagem adotada nesse trabalho é flexível em relação à ponderação dos atributos, e potencializa um resultado mais eficiente.

4.6.2 Busca

A parte principal de um sistema CBR é a etapa de recuperação. Esta etapa é essencial, uma vez que desempenha um papel vital no cálculo da semelhança entre dois casos. Dada uma descrição de uma situação atual, o algoritmo de recuperação calcula o valor de similaridade

para todos os casos em uma base de casos e recupera os casos mais semelhantes em comparação com o problema atual. Um dos métodos de recuperação mais comuns e conhecidos é o vizinho mais próximo (ou kNN) (PAL; SHIU, 2004), que se baseia na correspondência de uma soma ponderada dos recursos.

O método do vizinho mais próximo consiste em realizar comparação entre o caso com problema atual e os casos armazenados na base, realizando cálculos de similaridades. A semelhança entre uma consulta e um caso é calculada neste trabalho com semelhanças locais e globais. Medidas de similaridade local são usadas para medir a similaridade dos atributos individuais nos casos. Todas as semelhanças locais são então combinadas na medida de similaridade global que mede semelhanças para casos completos. A Similaridade Global está vinculada a atributos compostos e é usada para obter semelhança considerando o conjunto de atributos coletados. Como exemplo tem-se a função *Average*, que é um tipo de similaridade global que considera a média de todos os valores de similaridade local dos atributos.

Neste trabalho os cálculos de similaridade são realizados para buscar na base de casos o caso que descreve o incidente mais similar ao novo incidente. Idealmente, o que se espera é poder recuperar da base de casos um incidente já tratado e que seja igual ao incidente que precisa ser tratado. Desta maneira, na situação ideal, o tratador do incidente pode simplesmente executar as ações do plano de tratamento recuperado.

Na busca pelo melhor caso (o mais similar), primeiramente calcula-se a similaridade local a partir da função que determina o quão semelhantes são os valores para um determinado atributo. Em seguida, para cada atributo, é considerando o peso que representa seu grau de relevância na consulta realizada de acordo com a categoria, pois os pesos dos atributos podem variar. Finalmente, calcula-se a similaridade global representada pela média ponderada das similaridades locais.

A busca por um caso pode ser então resumida a aplicação de uma função de recuperação dada por *Sim(C,R)*, tal como define a Equação 4.1.

$$Sim(C,R) = \frac{\sum_{i=1}^{n} w_i * f(C_i R_i)}{\sum_{i=1}^{n} w_i} \tag{4.1}$$

Na Equação 4.1, *C* é o caso apresentado; *R* é o caso recuperado; *n* é o número de atributos do caso; *i* é o *i-ésimo* atributo; *w* é o peso atribuído ao *i-ésimo* atributo; e *f* é a função que calcula a similaridade entre os casos *C* e *R* para o *i-ésimo* atributo. A função *f* é a similaridade local e a função *Sim*, a similaridade global.

O cálculo da similaridade local dos atributos pode ser realizado por diferentes funções. A seguir apresenta-se algumas.

1) *Equal*: nesta função é retornado 0 ou 1, dependendo se o objeto 1 é idêntico ao objeto 2. O método de computação da classe usa o método equals implementado na superclasse Object, na forma de: C.equals(R).

2) *Interval*: essa função permite calcular a similaridade entre dois atributos numéricos dentro de um intervalo (vide Equação 4.2). Nesta função é subtraído o atributo do caso apresentado *C* com o atributo do caso recuperado na base de casos *R*, após é realizada a divisão pelo valor máximo do intervalo de possibilidades dos atributos. Por último, sendo o resultado entre 0 e 1, realiza-se a complementação em relação ao valor 1.

$$S_i = 1 - (\frac{C - R}{MAXi}) \tag{4.2}$$

3) *MaxString*: é uma adaptação do coeficiente de Jaccard, que retorna o valor da maior *substring* pertencente às duas *strings* e divide esse valor pelo tamanho da maior *string* dentre elas (vide Equação 4.3). É realizado a intersecção de C com R dividido pela união de C com R. Esta função foi aplicada para quase todos os atributos deste trabalho, dado que a maioria dos atributos é do tipo *string*.

$$Sim(C, R) = \frac{C \cap R}{C \cup R} \tag{4.3}$$

4) Distância Euclidiana: essa função é representada pela medida da distância entre dois objetos no espaço euclidiano. A distância é calculada a partir da raiz quadrada do quadrado da diferença aritmética entre duas coordenadas no espaço euclidiano ajustado pelo peso, no qual indica a importância do atributo no caso. O cálculo é apresentado na Equação 4.4.

$$d = \sqrt{\sum_{k-1}^{n} w_i \left(x_i - y_i\right)^2} \tag{4.4}$$

Como observado, a similaridade de diferentes atributos pode ser inferida de várias formas. Neste trabalho, de maneira distinta de (COLOMÉ; NUNES; SILVA, 2019), o qual utilizou a cálculo de distância euclidiana para todos os atributos tanto local como global, neste trabalho utiliza-se uma abordagem de explorar diferentes funções de similaridade local. Salienta-se que

é a melhor forma de tratar a diversidade de tipos, ou seja, adotando um método híbrido. A distinção leva em consideração a sintaxe e semântica de cada atributo.

A função *Equal*, embora de comportamento booleano, foi utilizada para avaliar alguns atributos: Categoria, *Servico*, *SistOperacional*, *FalhaExplorada* e *NomeMalware*. O atributo numérico Categoria é um dos atributos mais importantes deste trabalho, visto que é ele que define quais atributos irão compôr determinada categoria. Logo, o uso da função *Equal* é importante devido ao alto nível de precisão que a busca deve resultar. De maneira similar, o atributo chamado *Servico* deve ser equivalente entre os casos, pois de acordo com o tipo de serviço o plano de tratamento pode ser alterado drasticamente, assim como ocorre com o atributo *NomeMalware*. Como existe uma gama de *malwares* que possuem diferentes finalidades, o tratamento específico de cada um pode ir sendo incorporado na base de casos de acordo com novos incidentes, melhorando a busca.

A função *Maxstring*, por ser eficiente na recuperação de casos do tipo *string*, foi utilizada para o restante dos atributos.

Atributos compostos, como por exemplo *CaseComponents*, foram tratados com a função de similaridade global *Average* e funções de similaridade local para comparar atributos simples dentro do atributo composto.

A vantagem de ter elevados graus de semelhança é que pode ser comparado e ter uma maneira de determinar qual experiência está mais próxima do novo problema. Isso permite dizer qual é a experiência registrada mais semelhante, no qual é demonstrado a utilidade do conceito do vizinho mais próximo.

4.6.3 Seleção de Casos

A etapa de seleção de casos, consiste no ranqueamento dos casos, dado a similaridade calculada na etapa de busca. O processo de seleção de casos visa retornar uma lista com os casos que apresentaram os maiores graus de similaridade.

De posse da lista, um usuário deve realizar uma análise nos casos recomendados para identificar qual tem mais potencial para solucionar o problema. Note que a solução proposta apenas recomenda, restando ao usuário a decisão para escolha do caso recomendado a ser utilizado. Por exemplo, considere um incidente da categoria *Phishing* e cinco casos recuperados da mesma categoria com graus de similaridade diferentes: caso 1 com grau 0,6; caso 2 com grau 0,7; caso 3 com grau 0,8; caso 4 com 0,9; e caso 5 com grau 1,0. O resultado indica o caso 5

como sendo o mais similar e o recomenda como primeiro a ser considerado. O segundo a ser considerado deve ser o caso 4. A análise deve considerar a verificação manual se o plano de tratamento sugerido como solução pode ser aceito e usado.

4.6.4 Considerações Finais

Neste capítulo foi apresentado o detalhamento do processo proposto para a gestão de conhecimento no tratamento de incidentes de segurança. A abordagem foi baseada em CBR, possibilitando o aprendizado constante de novos casos.

Foi definida uma categorização de incidentes com o intuito de permitir que incidentes relatados em diferentes categorizações conhecidas e usadas mundialmente sejam mapeadas em uma categorização única e representativa, adotadas na solução do processo proposto. Além disso, ao associar os novos atributos aos padrões de representação de incidentes IODEF e STIX, essa nova categorização melhora a eficácia do processo de mapeamento de incidentes relatados, os quais podem ser de diferentes fontes, com a representação de caso adotada.

Na recuperação dos casos foram utilizados mecanismos de avaliação, busca e seleção. A proposição dessas etapas em conjunto com a ponderação realizada por um domínio de especialistas é chave para potencializar uma análise de similaridade qualificada para resolução do caso.

5 EXPERIMENTOS E RESULTADOS

Este capítulo foca na validação da processo proposto e detalha o ambiente de testes (Seção 5.1), os experimentos planejados (Seção 5.2) e os resultados alcançados (Seção 5.3).

5.1 AMBIENTE DE EXPERIMENTAÇÃO

Nos experimentos foi empregado um conjunto com 269 incidentes de segurança com as respectivas soluções, os quais foram coletados de uma organização real. Foi desenvolvido um protótipo *web* na linguagem Java e que utilizou o *framework jCOLIBRI* 2.0 (RECIO-GARCÍA; GONZÁLEZ-CALERO; DÍAZ-AGUDO, 2014), para fornecer suporte a decisões tomadas pelos especialistas, e um banco de dados *MySql*, para garantir a integridade das informações.

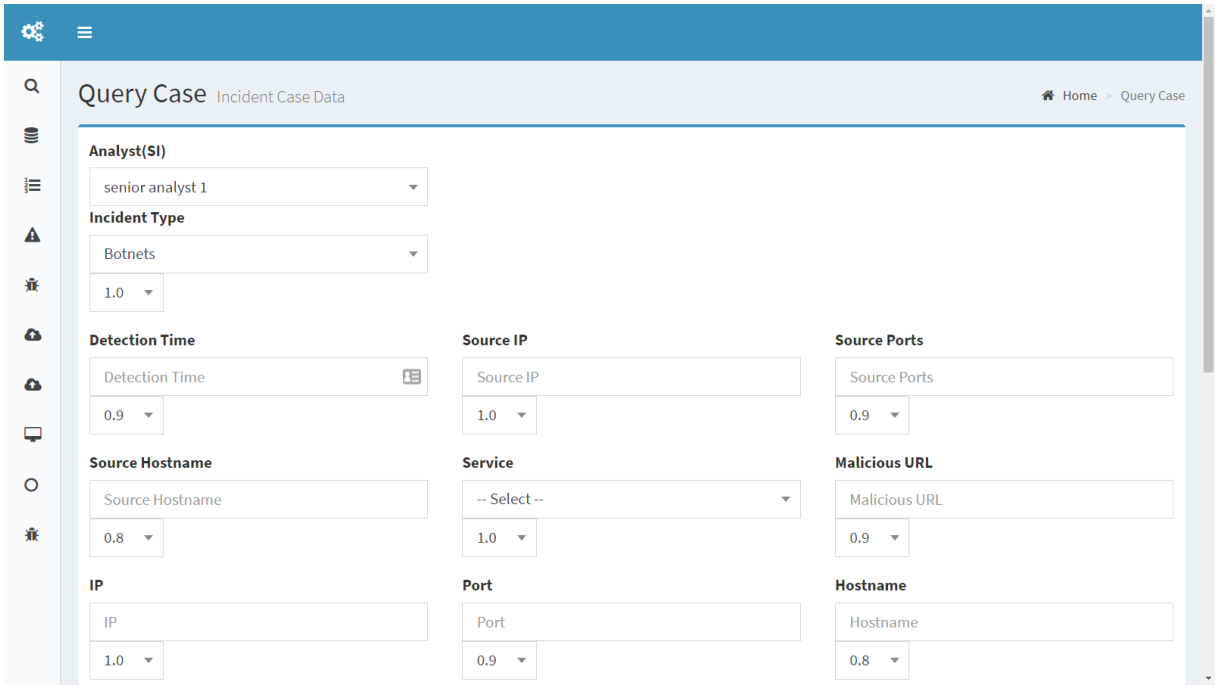
Considerando a nova modelagem de dados, que contém atributos alfanuméricos e códigos de referência, tal com identificadores, a função eucliana aplicada em (COLOMÉ; NUNES; SILVA, 2019) não pôde ser aplicada neste trabalho, pois não oferece uma medida adequada para esta modelagem. Por exemplo, o atributo Categoria é númerico, mas corresponde a um identificador, compromentendo o cálculo de medição de distância. Identificadores, por outro lado, devem ser analisados com a função de similaridade de igualdade. Neste sentido, neste trabalho, para diferenciar os atributos Categoria, *Servico*, *NomeMalware*, dentre outros que servem de identificadores, utilizou-se a análise de igualdade e não de distância.

A interface de consulta do protótipo da ferramenta implementada (CbCSecIRS) é apresentado na Figura 9, a qual pode ser selecionado a ponderação de um especialista do grupo ou a média no campo *Analist(SI)*, e de acordo com a opção selecionada os valores são populados ao lado de cada campo do formulário. Na ferramenta, os dados de incidentes são inseridos e armazenados de acordo com um modelo de dados comum. Para a importação de casos em IODEF ou em STIX foi utilizado, respectivamente, os formatos XML e JSON. Após a importação, o usuário tem a possibilidade de consultar no CBR experiências passadas e receber recomendações de planos de tratamento utilizados. Se não for encontrado nenhum plano de tratamento que tenha a solução (não há caso similar nas experiências passadas), o usuário informa ao especialista para elaborar um plano de tratamento para o incidente e criar mais um caso (problema/solução) na base de casos.

Na consulta CBR o usuário tem a possibilidade de escolher um grupo de pesos ponde-

rados pelos especialistas ou a média dessa ponderação, potencializando o uso desse conhecimento.

Figura 9 – Interface de consulta da Ferramenta CbCSecIRS.



Fonte: Autor.

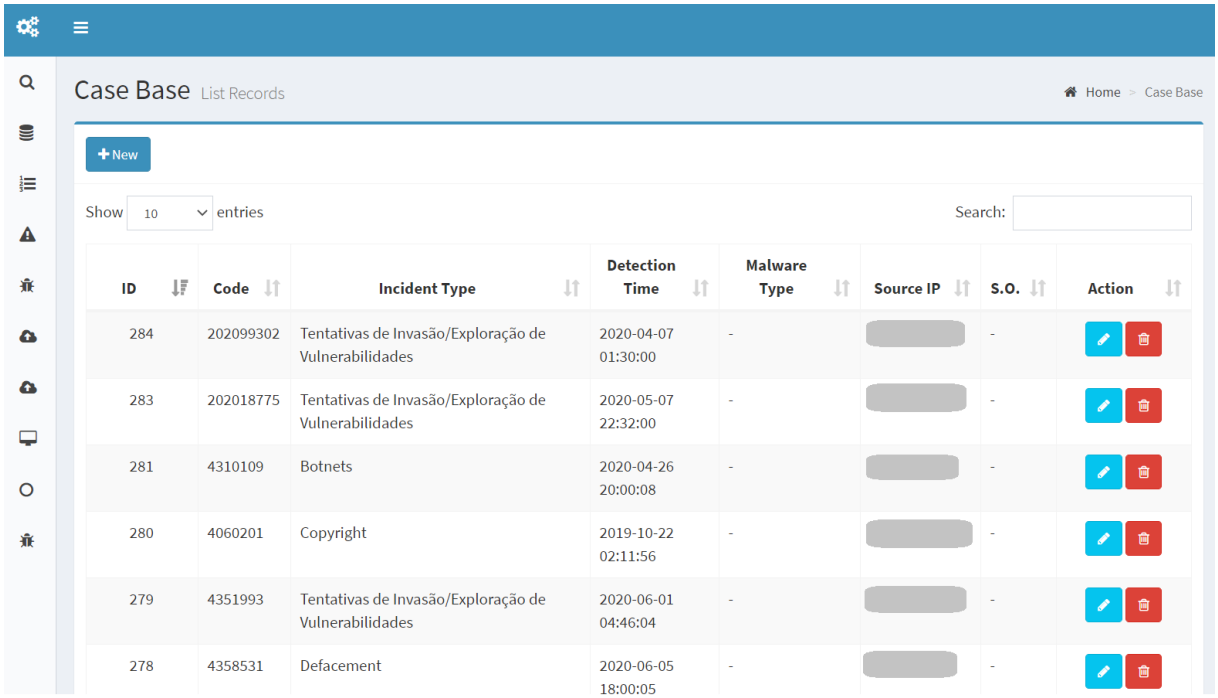
Considerando os formatos de dados das representações IODEF e STIX, adotadas neste trabalho, a ferramenta CbCSecIRS emprega funções híbridas (com funções *equals* e *maxstring*) para análise de similaridade.

É observado na Figura 10 os casos presentes na base com alguns atributos tais como: código, categoria do incidente, data e hora da detecção, tipo de *malware*, IP de origem e sistema operacional. No qual o especialista tem a possibilidade de edição e exclusão, essa opção existe para ser feita uma atualização periódica.

Na Figura 11 é apresentada a biblioteca de ações com os atributos *ID* e a descrição da ação, que é possível realizar o cadastro de uma nova ação, assim como editá-la ou excluí-la se não estiver vinculada a nenhum caso.

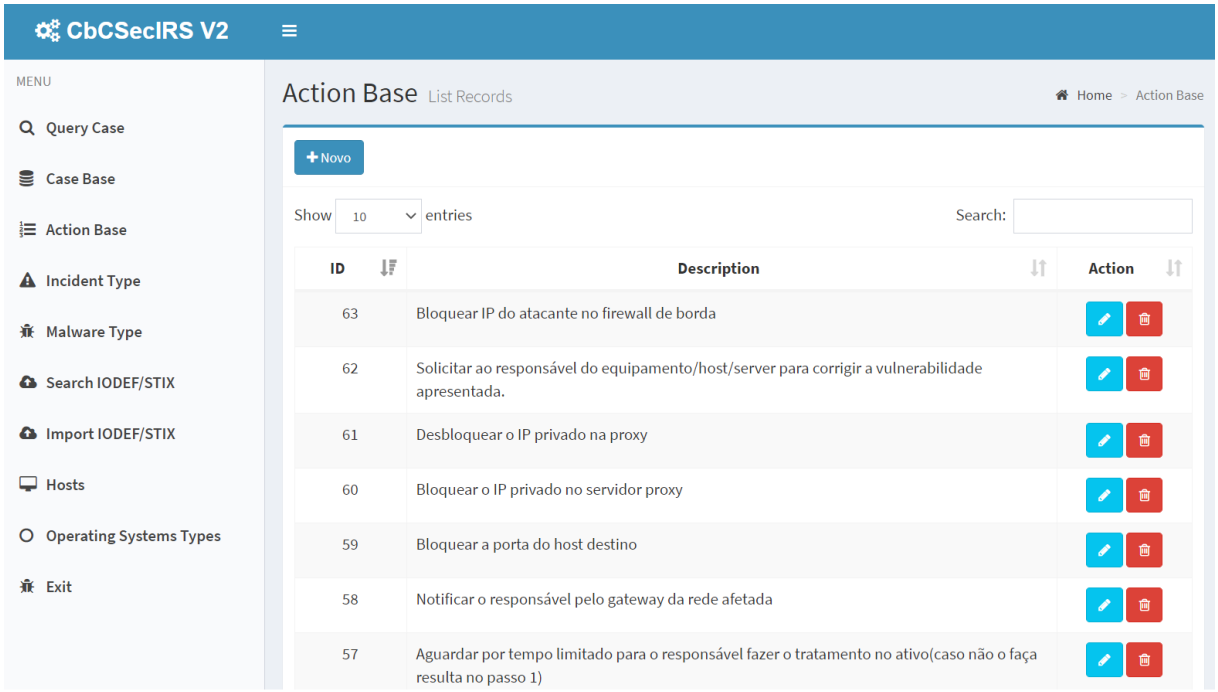
Na Figura 12 são apresentadas as categorias propostas com os atributos *ID* e a descrição, que é possível realizar o cadastro de uma nova categoria, assim como editá-la ou excluí-la se não estiver vinculada a nenhum caso. Na edição é permitido adicionar novos atributos à categoria, o que demonstra flexibilidade no protótipo.

Figura 10 – Interface de apresentação dos casos CbCSecIRS.



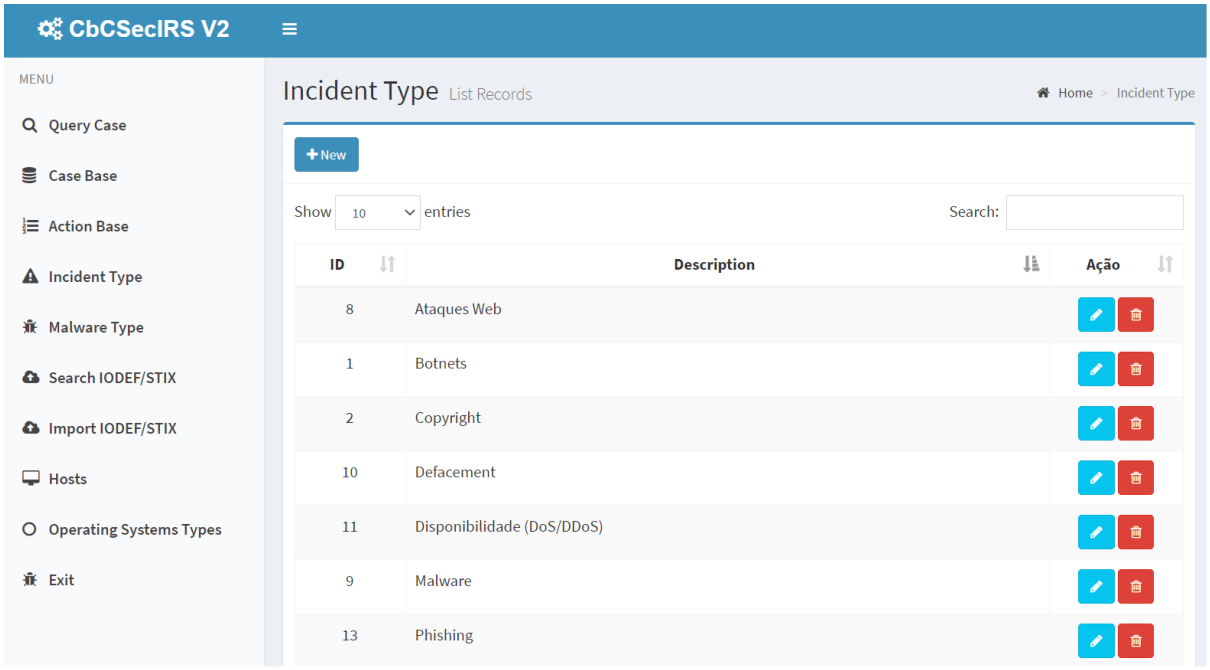
Fonte: Autor.

Figura 11 – Interface de Ações CbCSecIRS.



Fonte: Autor.

Figura 12 – Interface de Categorias de Incidente CbCSecIRS.



Fonte: Autor.

Na Figura 13 é apresentado os tipos de atividade maliciosa que pode estar vinculados a um incidente. Como exemplo na coluna descrição, o tipo *avalanche-andromeda* pode estar associado a categoria de *botnet*. Está base vai sendo populada de acordo com os casos já recebidos, que é possível realizar o cadastro de uma novo malware, assim como editá-lo ou excluí-lo se não estiver vinculada a nenhum caso.

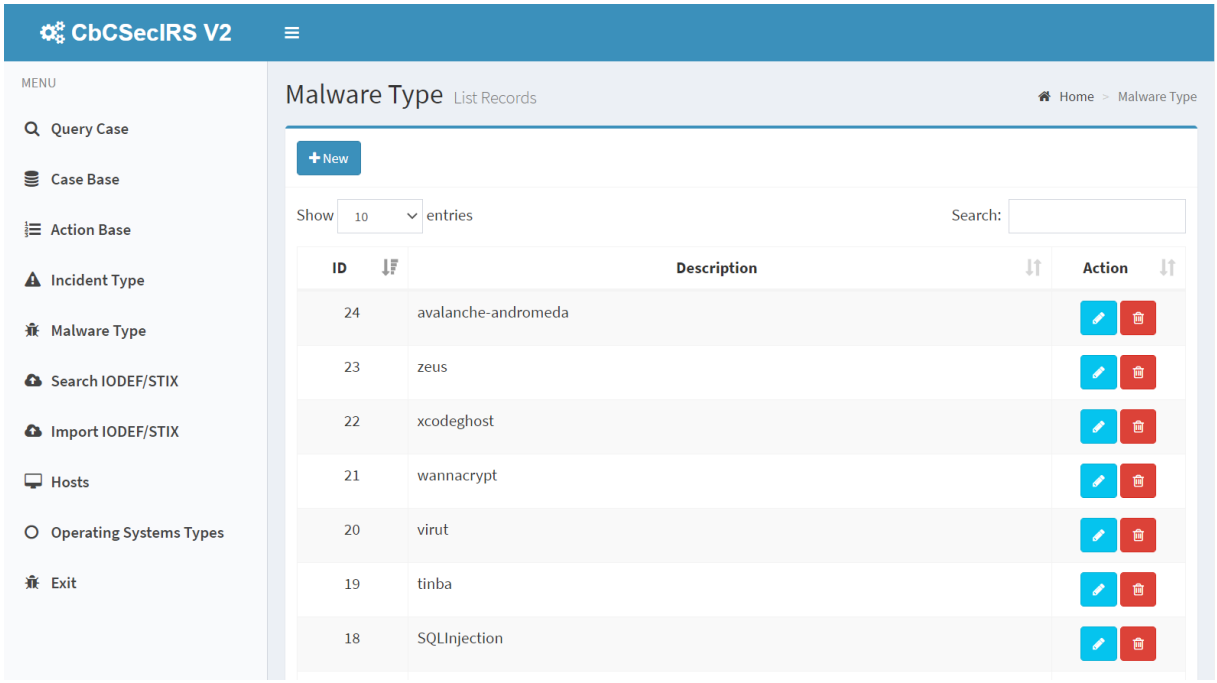
A Figura 14 ilustra como é possível fazer uma consulta CBR com informações de um arquivo de representação de dados IDODEF ou STIX após ser realizado o upload. O arquivo pode ser originado de um *IDS* ou de outras fontes capazes de gerar essas representações, o que facilita na recuperação dos casos similares.

A importação do caso é feito por meio de um arquivo XML ou JSON o qual pode ter o valor dos atributos ajustados pelo usuário, na Figura 15 é apresentado o formulário de submissão do arquivo.

Os *hosts* da organização devem estar cadastrados para ser identificado o serviço principal durante a importação do caso. Na Figura 16 é listado o IP, o serviço principal e a rede.

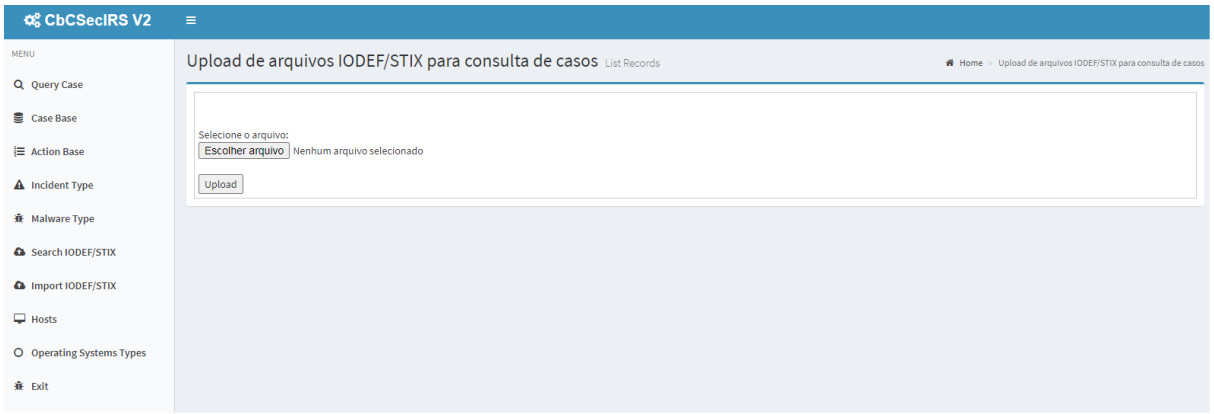
Na Figura 17 é apresentado os sistemas operacionais cadastrados no protótipo com a possibilidade de incluir outros, caso seja necessário.

Figura 13 – Interface de Tipos de Malware CbCSecIRS.



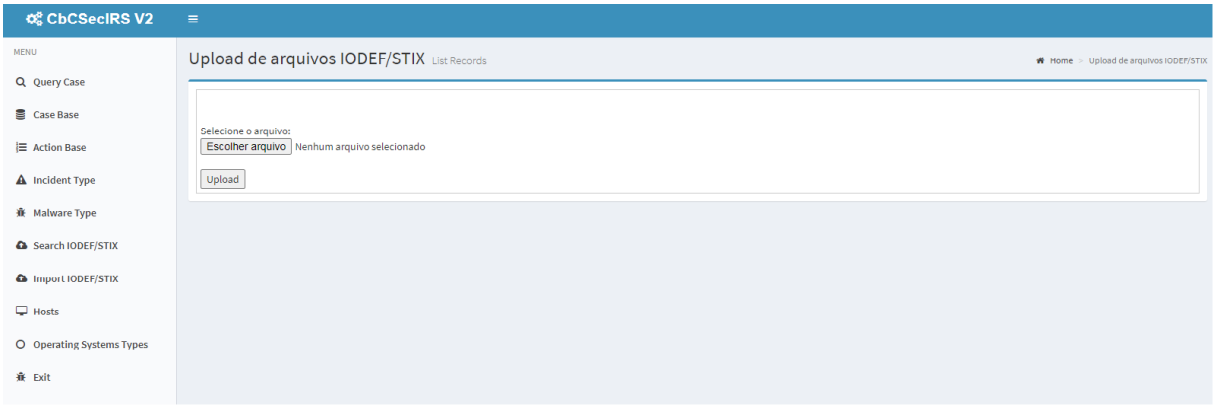
Fonte: Autor.

Figura 14 – Interface de Consulta - Upload CbCSecIRS.



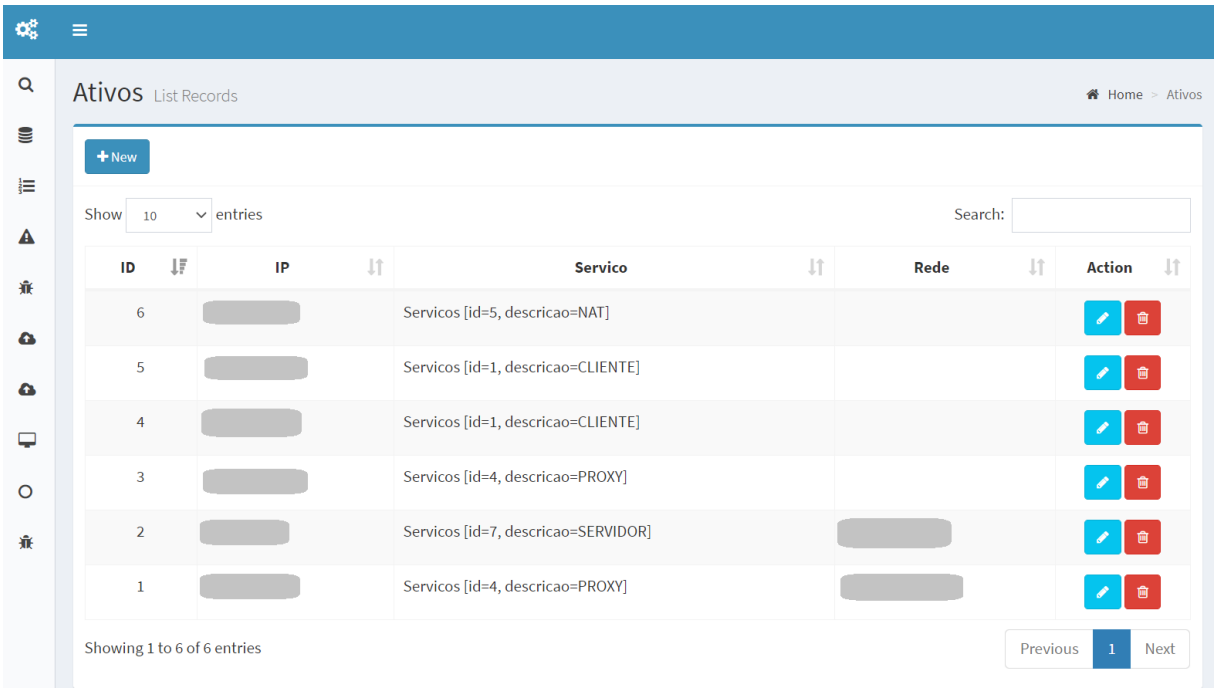
Fonte: Autor.

Figura 15 – Interface de Importação - Upload CbCSecIRS.



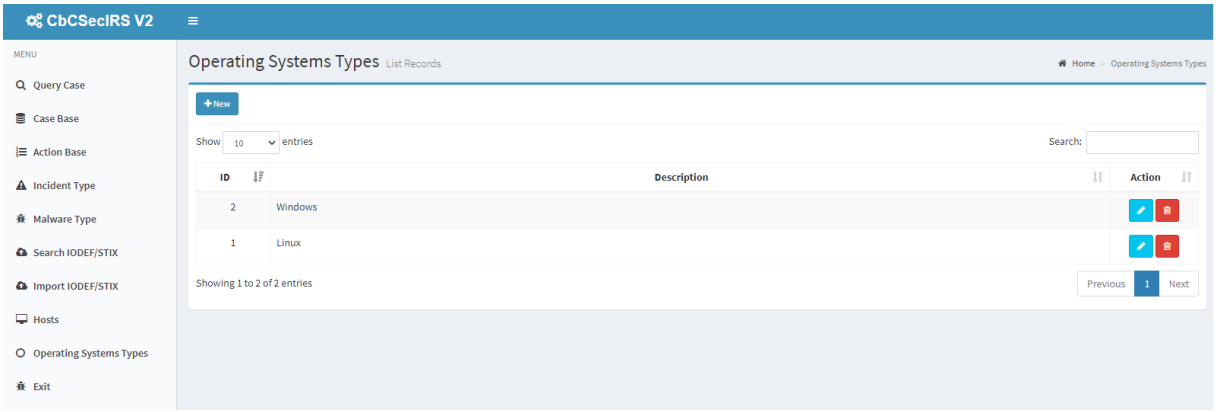
Fonte: Autor.

Figura 16 – Interface de *hosts* CbCSecIRS.



Fonte: Autor.

Figura 17 – Interface de Sistemas Operacionais CbCSecIRS.



Fonte: Autor.

5.2 PLANEJAMENTO DOS EXPERIMENTOS

Para a validação foram realizados três experimentos. O primeiro experimento foi conduzido considerando quatro especialistas em segurança e seu objetivo foi: i) definir valores de peso para serem associados a cada atributo usado no cálculo de similaridade CBR; e ii) avaliar a qualidade dos casos recuperados/recomendados com e sem a ponderação dos pesos. O segundo visa avaliar o uso da função híbrida. O terceiro experimento foca em avaliar a precisão do processo proposto. Nestes experimentos a ponderação foi definida com base na análise das categorias e atributos por quatro especialistas. Enfim, estes experimentos permitem avaliar a reutilização de experiências passadas na resolução de novos incidentes de segurança e também a precisão do sistema implementado.

5.3 RESULTADOS

No primeiro experimento, para a determinação prévia dos pesos, foi considerado a categorização de incidentes proposta neste trabalho com seus respectivos atributos. Com base nela, foi elaborado um questionário para avaliar junto aos especialistas os pesos de cada atributo por categoria. Para reduzir a subjetividade, participaram da avaliação quatro especialistas em segurança, incluindo o autor deste trabalho. Visto que podem ter diferentes visões e conhecimento sobre como medir similaridades em problemas de segurança.

Isso se deve ao fato de que a similaridade entre os problemas de segurança ser algo que pode ser avaliado e reavaliado de forma muito dinâmica, pois existe a constante disputa

entre ataque e defesa. Logo, esse conhecimento de similaridade pode ter que ser atualizado constantemente, ou mesmo permitindo aos usuários usarem diferentes configurações de pesos recomendados (previamente gravados no sistema) por esses especialistas, com a finalidade de recuperar com maior precisão os casos para apoiá-los a mitigar as consequências dos incidentes de segurança que já ocorreram.

Esta definição dos pesos de atributos foi para proporcionar valores de referência que potencializam a melhor qualidade na análise de similaridade entre um caso novo e os casos recuperados da base de casos.

É apresentado na Tabela 6, na primeira coluna, os atributos comuns a todas as categorias. Na segunda, terceira e quarta coluna é apresentada as respostas de cada especialista. E na última coluna, a média dos graus informados pelos especialistas. Estes valores médios foram assumidos como de referência e servem para fixação prévia de pesos aos atributos utilizados. Percebe-se nesta Figura uma dispersão dos valores, tal como o que ocorre no valor atribuído pelos especialistas 1 e 4 (Esp 1 e Esp 4) ao atributo Categoria que recebeu “1,0” e “0,7”, respectivamente. Esse atributo é o norteador na fase de recuperação, visto que é ele que realiza a definição de quais atributos pertencem a determinada categoria, portanto deve receber um peso máximo. A dispersão é também perceptível no atributo *DataHoraDetec*, pois os especialistas 2 e 4 avaliaram com os valores “0,5” e “1,0”, respectivamente. Este atributo deve ter um grau alto para fazer a recuperação de casos mais próximos ao da consulta. E como último exemplo de dispersão, no atributo Impacto, os especialistas 2 e 3 avaliaram como “1,0” e o especialista 4 avaliou como “0,6”. Esse atributo deve ter um grau relevante, pois é ele que vai medir o prejuízo para a organização.

Tabela 6 – Atributos comuns a todas as categorias.

Comuns	Esp 1	Esp 2	Esp 3	Esp 4	Média
Categoria	1,0	0,8	1,0	0,7	0,88
DataHoraDetec	0,9	0,5	0,8	1,0	0,8
Descricao	0,8	1,0	0,8	0,9	0,88
Impacto	0,9	1,0	1,0	0,6	0,88
URLRef	0,8	1,0	0,5	0,9	0,8
Logs	1,0	1,0	1,0	1,0	1,0

Fonte: Autor.

Com a mesma metodologia, os especialistas foram consultados para avaliar os pesos também para os atributos por categoria. A Tabela 7 apresenta o resultado para a categoria Dis-

ponibilidade. Os resultados para as demais categorias encontram-se no Anexo 1. Com base na Tabela 7, cabe destacar o atributo *IPOrigem*, ao qual foi atribuído valor máximo por todos os especialistas, dado que uma das ações mais comuns para o tratamento deste tipo de incidente é o bloqueio do IP do atacante. Outro atributo de destaque é o *FalhaExplorada*, pois ele corresponde a uma vulnerabilidade que pode ser facilmente tratada, após ser identificada. Nesta categoria a dispersão de valores foi menor. Não ocorreu tantas variações de valores, apesar de o atributo *PortaOrigem* ser avaliado pelo especialista 2 com peso "0,5" e pelos especialistas 3 e 4 com o peso "1,0". Conclui-se que esse atributo deve possuir um peso mediano, assim como o *HostNameOrigem*, pois eles não possuem um caráter expressivo na mitigação do incidente comparado aos outros atributos desta categoria.

Tabela 7 – Atributos da categoria Disponibilidade.

Disponibilidade	Esp 1	Esp 2	Esp 3	Esp 4	Média
IPOrigem	1,0	1,0	1,0	1,0	1,0
PortaOrigem	0,9	0,5	1,0	1,0	0,8
HostNameOrigem	0,8	0,6	0,5	0,5	0,6
FalhaExplorada	1,0	1,0	0,8	1,0	0,95
Protocolo	1,0	1,0	0,8	0,8	0,9

Fonte: Autor.

Como a ponderação do processo de atributos está fortemente ligada ao processo de recuperação do CBR, esta etapa contribui ao permitir que os valores dos pesos dos atributos sejam previamente determinados por especialistas, e também que possam ser informados ou ajustados previamente a cada consulta do CBR. Essa etapa também permite que diferentes ajustes sejam testados na busca por casos semelhantes. Nossa abordagem traz assim flexibilidade em relação à ponderação dos atributos e promove um resultado mais eficiente.

Ainda, no primeiro experimento, foram retirados quinze casos da base de casos, apresentados na Tabela 8, e os atributos foram ponderados por 4 especialistas. Os casos retirados correspondem à coluna *ID Caso consulta* e o respectivo plano deste caso na coluna Plano Consulta. As colunas *ID Caso Mais similar* e Plano recuperado são dados pertencentes a base de casos. A coluna *Similaridade entre os Casos* corresponde ao grau de similaridade (valor entre 0 a 1) entre o *ID Caso consulta* e o *ID Caso Mais similar*. Da mesma forma, a coluna Similaridade entre os planos corresponde ao grau de similaridade entre o Plano Consulta e o Plano Recuperado. Por fim, a coluna *Resolveu* indica se o especialista entende que o plano recuperado é efetivo, sendo avaliado a qualidade na resolução do incidente consultado.

Tabela 8 – Função híbrida com atributos ponderados por especialistas.

ID Caso consulta	ID Caso Mais similar	Similaridade entre os Casos	Plano Consulta	Plano recuperado	Similaridade entre os planos	Resolveu
281	274	0,7	16,17,24,49,1,15,6,2,9,31,21,22,23	16,17,24,49,1,15,6,2,9,31,21,22,23	1	SIM
273	275	0,78	16,17,24,1,45,46,22,23	16,17,24,1,45,46,22,23	1	SIM
37	63	0,80	16,17,28,29,8,6,9,2,3,31,38,23	16,17,28,29,8,6,9,2,3,31,38,23	1	SIM
25	27	0,79	16,17,1,11,12,42,21,22,23	16,17,1,11,12,42,21,22,23	1	SIM
77	16	0,81	16,17,1,15,33,31,21,22,23	16,17,1,15,33,31,21,22,23	1	SIM
107	133	0,81	16,17,1,11,35,12,42,21,22	16,17,1,11,35,12,42,21,22,23	0,97	SIM
158	154	0,89	16,17,11,12,23	16,17,11,12,23	1	SIM
178	141	0,96	16,17,1,15,25,5,2,3,9,31,21,22,23	16,17,1,15,25,5,2,3,9,31,21,22,23	1	SIM
256	257	0,94	16,17,11,39,25,37,36,23	16,17,11,39,25,37,36,23	1	SIM
58	64	0,82	16,17,1,40,11,12,21,22,41,23	16,17,1,11,35,25,21,22,23	0,82	SIM
60	43	0,90	16,17,11,39,25,37,36,23	16,17,11,39,25,37,36,23	1	SIM
34	35	1,00	16,17,1,11,35,12,42,21,22,23	16,17,1,11,35,12,42,21,22,23	1	SIM
21	20	0,72	16,17,1,15,8,6,9,2,3,31,21,22,23	16,17,1,15,8,6,9,2,3,31,21,22,23	1	SIM
42	4	0,74	16,17,1,11,35,21,22,23	16,17,1,11,12,42,21,22,23	0,86	SIM
95	254	0,97	16,17,11,39,25,37,36,23	16,17,11,39,25,37,36,23	1	SIM

Fonte: Autor.

Na consulta do *ID Caso consulta* 281 foi obtido o *ID Caso Mais similar* 274 com similaridade entre os casos de 0,7. Esse grau de similaridade foi considerado relevante, assim como os outros apresentados, porque a similaridade entre o plano consulta e o plano recuperado obteve grau máximo e para confirmar a qualidade do resultado, uma validação pelo especialista, que respondeu SIM para o plano recuperado. Para os *ID Caso consulta* 107, 58 e 42, a similaridade entre os planos não atingiu o grau máximo. No caso 107, que ficou mais próximo de 1 com 0,97, o plano recuperado teve uma ação a mais, a 23, mas o especialista respondeu *SIM* para o plano recuperado. O mesmo aconteceu no caso 58, que apresentou 0,82 de similaridade, e no caso 42, que apresentou 0,86.

A Tabela 9 ilustra, ainda no primeiro experimento, o resultado do experimento com a função híbrida e sem ponderação por especialistas. Todos os atributos foram ajustados com peso um. O *ID Caso consulta* 281 recuperou o caso 13, com similaridade de casos 0,66 e a similaridade entre os planos 0,85, diferente da situação apresentada na Tabela 8. Observa-se que foi recuperado um caso com plano diferente do plano da consulta, com a similaridade entre os casos e a similaridade entre os planos mais baixos, porém o especialista considerou *SIM* para a resolução do incidente, o que demonstrou efetividade no plano recuperado. O *ID caso consulta* 77 e o 21, recuperam os casos, respectivamente, 76 e 22, diferentes dos casos recuperados no experimento anterior, assim como os planos recuperados que não atenderam a resolução do incidente de acordo com a análise do especialista. As ações não condiziam com as do plano da consulta.

Neste primeiro experimento, o resultado com a função híbrida e com ponderação demonstra que no tratamento de um incidente pode haver mais de um plano que atenda a resolução

do incidente e se obteve 100% de acerto, sendo analisado a qualidade no tratamento do plano recuperado. Já no resultado com a função híbrida e sem ponderação se obteve 86% de acerto.

Isso demonstra que a ponderação por especialistas teve melhores respostas no plano de tratamento, visto que todos os planos foram satisfatórios.

Tabela 9 – Função híbrida com atributos com valor um.

ID Caso consulta	ID Caso Mais similar	Similaridade entre os Casos	Plano Consulta	Plano recuperado	Similaridade entre os planos	Resolveu
281	13	0,66	16,17,24,49,1,15,6,2,9,31,21,22,23	16,17,1,15,25,5,2,3,9,31,21,22,23	0,85	SIM
273	275	0,65	16,17,24,1,45,46,22,23	16,17,24,1,45,46,22,23	1	SIM
37	47	0,92	16,17,28,29,8,6,9,2,3,31,38,23	16,17,28,29,8,6,9,2,3,31,38,23	1	SIM
25	27	0,78	16,17,1,11,12,42,21,22,23	16,17,1,11,12,42,21,22,23	1	SIM
77	76	0,78	16,17,1,15,33,31,21,22,23	16,17,28,29,8,6,9,2,3,31,38,23	0,8	NÃO
107	113	0,73	16,17,1,11,35,12,42,21,22	16,17,1,15,33,31,21,22,23	0,84	SIM
158	125	0,87	16,17,11,12,23	16,17,11,12,23	1	SIM
178	141	0,93	16,17,1,15,25,5,2,3,9,31,21,22,23	16,17,1,15,25,5,2,3,9,31,21,22,23	1	SIM
256	257	0,87	16,17,11,39,25,37,36,23	16,17,11,39,25,37,36,23	1	SIM
58	64	0,77	16,17,1,40,11,12,21,22,41,23	16,17,1,11,35,25,21,22,23	0,82	SIM
60	43	0,88	16,17,11,39,25,37,36,23	16,17,11,39,25,37,36,23	1	SIM
34	35	1,00	16,17,1,11,35,12,42,21,22,23	16,17,1,11,35,12,42,21,22,23	1	SIM
21	22	0,71	16,17,1,15,8,6,9,2,3,31,21,22,23	16,17,28,29,25,5,2,3,9,31,32,38,23	0,79	NÃO
42	81	0,69	16,17,1,11,35,21,22,23	16,17,1,15,33,31,21,22,23	0,84	SIM
95	254	0,94	16,17,11,39,25,37,36,23	16,17,11,39,25,37,36,23	1	SIM

Fonte: Autor.

Para o segundo experimento visando avaliar o uso da função híbrida, foi realizado com a validação cruzada *Leave-One-Out* (LOOCV) (KOHAVI et al., 1995), que tem como finalidade retirar um caso por vez da base de casos comparando-o com os outros para ser contabilizado o número de acertos e erros do sistema. Isso recupera um conjunto de casos similares a cada caso usado como consulta no qual é utilizado o método 1-NN, que contabiliza apenas o caso mais similar. Os demais são descartados. Foi considerado quatro limiares de similaridade, 90%, 80%, 70% e 60%. Na tabela 10 são apresentados os resultados com os percentuais de acertos das funções híbrida e equal.

Tabela 10 – Comparativo de funções

Limiar	Híbrida(%)	Equal(%)
90%	59	36
80%	70	62
70%	86	76
60%	95	84

Fonte: Autor.

Os resultados demonstraram que a função híbrida obteve um percentual de recuperação maior que a função equal em diferentes limiares de similaridade, comprovando a sua aplicabilidade.

No terceiro experimento, também realizado com a validação cruzada *Leave-One-Out* (LOOCV), porém para analisar a precisão do método. Foi considerado os mesmos limiares de similaridade usados anteriormente, 90%, 80%, 70% e 60%. Foi analisada a comparação dos pesos de atributos ponderados por especialistas e o peso dos atributos igual a "um" utilizando a função híbrida de acordo com a tabela 11. Esse experimento comprova o uso eficiente da ponderação no método aplicado.

Tabela 11 – Ponderação de pesos

Limiar	Com ponderação(%)	Sem ponderação(%)
90%	59	47
80%	70	66
70%	86	80
60%	95	92

Fonte: Autor.

Na tabela 12, é apresentado o percentual de acertos utilizando a validação cruzada com o conjunto de pesos informados por cada especialista. Percebe-se uma proximidade entre os valores de cada limiar, demonstrando apenas um distanciamento maior no limiar de 70%. Isso representa que os especialistas podem possuir opiniões divergentes sobre o tratamento dos incidentes, pois na mitigação dele pode-se atribuir uma importância maior para um atributo do que outro. E isso também corrobora que podem existir mais de uma solução para um determinado problema.

Tabela 12 – Ponderação de pesos - Especialistas

Limiar	Esp1(%)	Esp2(%)	Esp3(%)	Esp4(%)
90%	59	57	60	60
80%	69	70	71	69
70%	87	85	90	80
60%	96	95	96	94

Fonte: Autor.

Os testes demonstraram que com a ponderação de especialistas obteve-se uma melhor precisão nos resultados com os limiares considerados.

Como resultado geral dos experimentos verifica-se que a ferramenta demonstra que o uso de função híbrida (*Equal* e *MaxString*) no cálculo de similaridade resulta em recomendações mais precisas. De maneira similar, os experimentos demonstram que o uso da ponderação também auxilia na obtenção de melhores resultados.

6 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho procurou tratar como as organizações podem reter e recuperar o conhecimento em um processo de resposta a incidentes de segurança cibernética. Neste ambiente complexo e dinâmico atual, as organizações estão enfrentando cada vez mais ameaças complexas e em evolução, tanto externas quanto internas. E a escassez de mão de obra qualificada nesta área pode acabar impactando diretamente nas organizações. Por isso a experiência destes profissionais deve ser retida.

Conforme discutido neste trabalho, foi apresentado um processo de gestão do conhecimento baseado em CBR para gerenciamento de tratamento de incidentes. O primeiro aspecto deste processo está relacionado à forma como os incidentes são compartilhados e relatados. Uma ferramenta de tratamento de incidentes deve estar alinhada aos padrões de representação de incidentes bem conhecidos (IODEF e STIX). Neste sentido, foi proposta uma nova categorização que não entra em conflito com outras categorizações, mas que associada aos padrões de representação permitem melhorar o mapeamento de incidentes compartilhados e relatados para casos de consulta. O segundo aspecto é a análise de similaridade entre o incidente presente e os passados. O trabalho demonstrou que é importante selecionar funções de similaridade adequadas, que apresentaram resultados eficientes, principalmente porque deve-se considerar que o tipo de dados dos atributos apresenta impacto significativo na precisão da ferramenta de tratamento de incidentes baseada no CBR. O trabalho demonstra também que é importante ponderar atributos na análise de similaridade e que definir valores de pesos para atributos de incidentes com base na opinião de um grupo de especialistas é adequado. Demonstra-se também, que a experiência de especialistas para a ponderação pode ser assumida como configuração padrão de ponderação, mantida a possibilidade de a ponderação ser parametrizada pelo usuário, potencializando a recuperação mas precisa de soluções (planos de tratamento).

A implantação da solução num protótipo de ferramenta de software permitiu avaliar e validar a eficácia da solução e dos melhoramentos propostos num processo de gestão de conhecimento baseado em CBR. Os resultados dos experimentos e demonstraram eficácia na recuperação de planos de tratamento.

As dificuldades encontradas durante a elaboração deste trabalho foram o número de registro na base de casos e o número de especialistas para participar dos experimentos. Foram coletados um total de 269 casos (<incidente, plano de tratamento>, sendo que o ideal seria tra-

balhar com uma base de casos maior. Porém, não foi possível encontrar bases com a descrição do incidente e o plano de tratamento. Encontrar especialistas é desafiador para as organizações e o projeto também teve dificuldade similar, dado que foram necessários especialistas em segurança com experiência para realizar a ponderação de atributos.

Com base nos resultados e descobertas deste trabalho, podem ser exploradas como trabalhos futuros diferentes técnicas de priorização na recuperação dos casos, tais como recenticidade e efetividade nas consultas CBR. Nestas técnicas pode existir um conjunto de requisitos para serem priorizados na fase de recuperação. Podem também ser pesquisadas e implementadas outras funcões de similaridade na busca de melhores resultados na consulta CBR, podendo resultar em planos de tratamentos mais adequados.

A criação de um indicador de qualidade para o plano de tratamento, como uma métrica de reúso, para apontar um plano de melhor qualidade dentro daqueles que forem recuperados é também uma abordagem interessante que pode ser alvo de trabalhos futuros.

7 ARTIGOS SUBMETIDOS/PUBLICADOS

Como primeiro autor, foi submetido o artigo intitulado *A Support Method and Decision Making in the Treatment of Information Security Incidents* ao *ACM Symposium on Applied Computing* (SAC'21). Este artigo foca nas contribuições desta dissertação.

O autor desta dissertação participou também como co-autor do artigo intitulado *A Case-Based Reasoning Approach for the Cybersecurity Incident Recording and Resolution* publicado na *International Journal of Software Engineering and Knowledge Engineering, Vol. 29, No. 11n12, pp. 1607-1627* (2019). DOI: https://doi.org/10.1142/S021819401940014X

REFERÊNCIAS

AAMODT, A.; PLAZA, E. Case-based reasoning: foundational issues, methodological variations, and system approaches. **AI communications**, [S.l.], v.7, n.1, p.39–59, 1994.

ABDEL-AZIZ, A.; STRICKERT, M.; HÜLLERMEIER, E. Learning solution similarity in preference-based CBR. In: INTERNATIONAL CONFERENCE ON CASE-BASED REASONING. **Anais...** [S.l.: s.n.], 2014. p.17–31.

AJJOURI, M.; BENHADOU, S.; MEDROMI, H. Case Retrieval Implementation For Intrusion Detection Architecture Based On Multi Agent Systems And Case Based Reasoning Technique. **Int. Journal of Scientific and Engineering Research**, [S.l.], v.10, p.1184–1189, 10 2019.

ASGARLI, E.; BURGER, E. Semantic ontologies for cyber threat sharing standards. In: IEEE SYMPOSIUM ON TECHNOLOGIES FOR HOMELAND SECURITY (HST), 2016. **Anais...** [S.l.: s.n.], 2016. p.1–6.

BACH, K.; ALTHOFF, K.-D. Developing Case-Based Reasoning Applications Using myCBR 3. In: CASE-BASED REASONING IN RESEARCH AND DEVELOPMENT. INTERNATIONAL CONFERENCE ON CASE-BASED REASONING (ICCBR-2012), 20TH, SEPTEMBER 3-6, LYON, FRANCE. **Anais...** Springer-Verlag, 2012. p.17–31. (LNCS, v.7466).

BASKERVILLE, R.; SPAGNOLETTI, P.; KIM, J. Incident-centered information security: managing a strategic balance between prevention and response. **Information & management**, [S.l.], v.51, n.1, p.138–151, 2014.

BIRKENKRAHE, M. How large multi-nationals manage their knowledge. **Business Review**, [S.l.], v.4, n.2, p.2–12, 2002.

BJØRNSON, F. O.; DINGSØYR, T. Knowledge management in software engineering: a systematic review of studied concepts, findings and research methods used. **Information and Software Technology**, [S.l.], v.50, n.11, p.1055–1068, 2008.

BURGER, E. W. et al. Taxonomy model for cyber threat intelligence information exchange technologies. In: ACM WORKSHOP ON INFORMATION SHARING & COLLABORATIVE SECURITY, 2014. **Proceedings...** [S.l.: s.n.], 2014. p.51–60.

CERT-BR. **Estatísticas dos Incidentes Reportados ao CERT. br - Total.** Disponível em: <https://www.cert.br/stats/incidentes/2019-jan-dec/total.html>. [Online; acesso 12-abril-2020].

CERT-BR. **Estatísticas dos Incidentes Reportados ao CERT.br - Tipos de Ataques.** Disponível em: <https://www.cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.html>. [Online; acesso 12-abril-2020].

CERT-PT. **Taxonomia Comum para a Rede Nacional de CSIRTs.** Disponível em: <https://www.redecsirt.pt/files/Taxonomiav2.5.pdf>. [Online; acesso 16-abril-2020].

CERT/CC. **Computer Security Incident Response Team Frequently Asked Questions**. Disponível em: <https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485654.pdf>. [Online; acesso 01-dezembro-2019].

CICHONSKI, P. et al. **NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide**. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>. [Online; acesso 14-julho-2019].

COLOMÉ, M. d. L.; NUNES, R. C.; SILVA, L. A. d. L. Técnica para Retenção e Recuperação de Conhecimento na Resolução de Incidentes de Segurança. **XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais**, [S.l.], 2019.

CTIR-GOV. **Estatísticas dos Incidentes Reportados ao CTIR Gov. 2020**. Disponível em: <https://emnumeros.ctir.gov.br/incidentes/>. [Online; acesso 12-abril-2020].

DANYLIW, R. **The Incident Object Description Exchange Format Version 2**. [S.l.]: RFC Editor, 2016. n.7970. (Request for Comments).

DE, S.; CHAKRABORTY, B. Case Based Reasoning (CBR) Methodology for Car Fault Diagnosis System (CFDS) Using Decision Tree and Jaccard Similarity Method. In: IEEE INTERNATIONAL CONFERENCE FOR CONVERGENCE IN TECHNOLOGY (I2CT). **Anais...** [S.l.: s.n.], 2018. p.1–6.

DHAYAL, H.; KUMAR, J. Botnet and P2P Botnet Detection Strategies: a review. In: INTERNATIONAL CONFERENCE ON COMMUNICATION AND SIGNAL PROCESSING (ICCSP), 2018. **Anais...** [S.l.: s.n.], 2018. p.1077–1082.

ELKAFRAWY, P.; MOHAMED, R. A. Comparative study of case based reasoning software. **International Journal of Scientific Research and Management Studies**, [S.l.], v.1, n.6, p.224–233, 2015.

EUROPOL, E. Common taxonomy for law enforcement and the national network of csirts, version 1.3. Technical report, ENISA and Europol E3. , [S.l.], 2017. Disponível em: <https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts>. [Online; acesso 12-abril-2020].

GHAZIRI, H.; AWAD, E. Is there a future for knowledge management. **Journal of Information Technology Management**, [S.l.], v.16, n.1, p.31–38, 2005.

GRISPOS, G. **On the enhancement of data quality in security incident response investigations**. 2016. Tese (Doutorado em Ciência da Computação) — University of Glasgow.

GUPTA, S.; SINGHAL, A.; KAPOOR, A. A literature survey on social engineering attacks: phishing attack. In: ICCCA), 2016. **Anais...** [S.l.: s.n.], 2016. p.537–540.

HERNANDEZ, N. NOC/SOC Integration: opportunities for increased efficiency in incident response within cyber-security. **SANS-INSTITUTE**, [S.l.], 2018. Disponível em: <https://www.sans.org/reading-room/whitepapers/incident/paper/38290>. [Online; acesso 01-dezembro-2019].

HUMAYUN, M. et al. Cyber Security Threats and Vulnerabilities: a systematic mapping study. **Arabian Journal for Science and Engineering**, [S.l.], p.1–19, 2020.

IOANNOU, M.; STAVROU, E.; BADA, M. Cybersecurity Culture in Computer Security Incident Response Teams: investigating difficulties in communication and coordination. In: INTERNATIONAL CONFERENCE ON CYBER SECURITY AND PROTECTION OF DIGITAL SERVICES (CYBER SECURITY), 2019. **Anais...** [S.l.: s.n.], 2019. p.1–4.

JAFARI, M. et al. Exploring the contextual dimensions of organization from knowledge management perspective. **VINE**, [S.l.], v.38, n.1, p.53–71, 2008.

JIANG, F. et al. Case Retrieval for Network Security Emergency Response Based on Description Logic. In: INTERNATIONAL CONFERENCE ON INTELLIGENT INFORMATION PROCESSING. **Anais...** [S.l.: s.n.], 2014. p.284–293.

KAMPANAKIS, P. Security automation and threat information-sharing options. **IEEE Security & Privacy**, [S.l.], v.12, n.5, p.42–51, 2014.

KAMPANAKIS, P.; SUZUKI, M. **Incident Object Description Exchange Format Usage Guidance**. [S.l.]: RFC Editor, 2017. n.8274. (Request for Comments).

KILLCRECE, G. et al. **State of the practice of computer security incident response teams (CSIRTs)**. [S.l.]: CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2003.

KOHAVI, R. et al. A study of cross-validation and bootstrap for accuracy estimation and model selection. In: IJCAI. **Anais...** [S.l.: s.n.], 1995. v.14, n.2, p.1137–1145.

KRAL, P. Incident Handler's Handbook. **SANS-INSTITUTE**, [S.l.], 2011. Disponível em: <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>. [Online; acesso 08-novembro-2019].

KUYPERS, M. A.; MAILLART, T.; PATÉ-CORNELL, E. An empirical analysis of cyber security incidents at a large organization. **Department of Management Science and Engineering, Stanford University, School of Information, UC Berkeley**, [S.l.], v.30, 2016.

LEI, N. 13.709, de 14 de Agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da República Federativa do Brasil (14 ago. 2018)**, [S.l.], 2018.

MALLIKARJUNAN, K. N.; MUTHUPRIYA, K.; SHALINIE, S. M. A survey of distributed denial of service attack. In: INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS AND CONTROL (ISCO), 2016. **Anais...** [S.l.: s.n.], 2016. p.1–6.

MEIJER, J.; DANYLIW, R.; DEMCHENKO, Y. **The Incident Object Description Exchange Format**. [S.l.]: RFC Editor, 2007. n.5070. (Request for Comments).

MENGES, F.; PERNUL, G. A comparative analysis of incident reporting formats. **Computers & Security**, [S.l.], v.73, p.87–101, 2018.

MITRE. **STIX Structured Threat Information Expression**. Disponível em <stix.mitre.org/>. [Online; acesso 14-abril-2020].

MORIARTY, K. **Real-time Inter-network Defense (RID)**. [S.l.]: RFC Editor, 2012. n.6545. (Request for Comments).

NUNES, R. C.; AL. et. A Case-Based Reasoning Approach for the Cybersecurity Incident Recording and Resolution. **Int. Journal of Software Engineering and Knowledge Engineering**, [S.l.], v.29, n.11n12, p.1607–1627, 2019.

OLTSIK, J. The life and times of cybersecurity professionals. **ESG and ISSA: Research Report**, [S.l.], 2020.

PAL, S. K.; SHIU, S. C. **Foundations of soft case-based reasoning**. [S.l.]: John Wiley & Sons, 2004. 75–80p. v.8.

PING, L.; HAIFENG, Y.; GUOQING, M. An incident response decision support system based on CBR and ontology. In: INTERNATIONAL CONFERENCE ON COMPUTER APPLICATION AND SYSTEM MODELING (ICCASM 2010), 2010. **Anais...** [S.l.: s.n.], 2010. v.11, p.V11–337.

PODZINS, O.; ROMANOVS, A. Why SIEM is Irreplaceable in a Secure IT Environment In: OPEN CONFERENCE OF ELECTRICAL, ELECTRONIC AND INFORMATION SCIENCES (ESTREAM), 2019. **Anais...** [S.l.: s.n.], 2019. p.1–5.

RANI, S. S.; REEJA, S. A Survey on Different Approaches for Malware Detection Using Machine Learning Techniques. In: INTERNATIONAL CONFERENCE ON SUSTAINABLE COMMUNICATION NETWORKS AND APPLICATION. **Anais...** [S.l.: s.n.], 2019. p.389–398.

RECIO-GARCÍA, J. A.; GONZÁLEZ-CALERO, P. A.; DÍAZ-AGUDO, B. jcolibri2: a framework for building case-based reasoning systems. **Science of Computer Programming**, [S.l.], v.79, p.126–145, 2014.

RECIO-GARCIA, J. jCOLIBRI: a multi-level platform for building and generating cbr systems. **PhD in Computer Science, Universidad Complutense de Madrid. Grupo GAIA**, [S.l.], 2008.

ROWLEY, J. The wisdom hierarchy: representations of the dikw hierarchy. **Journal of information science**, [S.l.], v.33, n.2, p.163–180, 2007.

SANTOS, D.; NOBRE, J. C. Vulnerability Identification on GNU/Linux Operating Systems through Case-Based Reasoning. **Revista de Informática Teórica e Aplicada**, [S.l.], v.26, n.3, p.13–25, 2019.

SAUERWEIN, C. et al. Threat intelligence sharing platforms: an exploratory study of software vendors and research perspectives. , [S.l.], 2017. Disponível em: <https://aisel.aisnet.org/wi2017/track08/paper/3/>.

SCHMITT, S. et al. Reference incident Classification Taxonomy. enisa. 2018. , [S.l.], 2018. Disponível em: <https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy>. [Online; acesso 10-setembro-2019].

Service Name and Transport Protocol Port Number Registry. **Internet Assigned Numbers Authority (IANA)**, [S.l.], 2020. Disponível em: <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>. [Online; acesso 03-outubro-2020].

SFAKIANAKIS, A. et al. ENISA Threat Landscape Report 2018: 15 top cyberthreats and trends. **DOI**, [S.l.], v.10, p.622757, 2019.

SHACKLEFORD, D. Who's using Cyberthreat Intelligence and how? **SANS Institute. Retrieved January**, [S.l.], v.24, p.2018, 2015.

SILVA, L. A. et al. A case for folk arguments in case-based reasoning. In: INTERNATIONAL CONFERENCE ON CASE-BASED REASONING. **Anais...** [S.l.: s.n.], 2010. p.317–331.

SINGH, A. et al. Taxonomy of Attacks on Web Based Applications. In: INTERNATIONAL CONFERENCE ON INTELLIGENT COMPUTING, INSTRUMENTATION AND CONTROL TECHNOLOGIES (ICICICT), 2019. **Anais...** [S.l.: s.n.], 2019. v.1, p.1231–1235.

Sohime, F. H. et al. Exploration Study of Skillsets Needed in Cyber Security Field. In: INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY AND MULTIMEDIA (ICIMU), 2020. **Anais...** [S.l.: s.n.], 2020. p.68–72.

STANDARD, D. E. National Institute of Standards and Technology. **Federal Information Processing Standard (FIPS) Publication**, [S.l.], p.46–1, 2002.

Strategies for Building and Growing Strong Cybersecurity Teams. **(ISC)2 CYBERSECURITY WORKFORCE STUDY**, [S.l.], 2019. Disponível em: <https://www.isc2.org/-/media/ISC2/Research/2019-CybersecurityWorkforce-Study/ISC2-CybersecurityWorkforce-Study-2019.ashx?la=enhash=1827084508A24DD75C60655E243EAC59ECDD4482>. [Online; acesso 05-dezembro-2020].

TAKAHASHI, T.; LANDFIELD, K.; KADOBAYASHI, Y. **An Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information**. [S.l.]: RFC Editor, 2014. n.7203. (Request for Comments).

TAKAHASHI, T.; MIYAMOTO, D. Structured Cybersecurity Information Exchange for Streamlining Incident Response Operations. In: IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOMS 2016): EXPERIENCE SESSION PAPER, Los Alamitos, CA. **Proceedings...** IEEE, 2016. p.949–954.

US-CERT. U.S. Department of Homeland Security | US-CERT Federal Incident Notification Guidelines. , [S.l.], 2017. Disponível em: <https://www.us-cert.gov/incident-notification-guidelines>. [Online; acesso 13-abril-2020].

VON WANGENHEIM, C. G.; VON WANGENHEIM, A. **Raciocínio baseado em casos**. [S.l.]: Editora Manole Ltda, 2003. 19p.

WATSON, I. **Case-based reasoning is a methodology not a technology**. [S.l.]: Springer, 1999. 213–223p.

ZAKARIA, W. Z. A. Application of case based reasoning in it security incident response. In: INT. CONF. RECENT TRENDS IN ENGINEERING AND TECHNOLOGY. **Anais...** [S.l.: s.n.], 2015. p.106–109.

8 ANEXOS

8.1 ANEXO 1

Ataques Web	Esp 1	Esp 2	Esp 3	Esp 4	Média
IPOrigem	1,0	1,0	1,0	1,0	1,0
HostNameOrigem	0,8	0,6	0,5	0,5	0,60
UrlComprometida	0,9	1,0	0,8	1,0	0,93
FalhaExplorada	1,0	1,0	0,8	1,0	0,95

Violação de Ativo	Esp 1	Esp 2	Esp 3	Esp 4	Média
Localizacao	1,0	0,8	1,0	1,0	0,95

Spam	Esp 1	Esp 2	Esp 3	Esp 4	Média
Url_reclamante	1,0	0,8	0,8	0,8	0,85
IPOrigem	1,0	1,0	1,0	1,0	1,0

Botnet	Esp 1	Esp 2	Esp 3	Esp 4	Média
IPBot	1,0	1,0	1,0	1,0	1,0
UrlMaliciosa	0,9	1,0	0,8	0,8	0,88
HostNameOrigem	0,8	0,6	0,5	0,5	0,60
Protocolo	0,9	1,0	0,8	0,9	0,90
TotalCon	0,8	0,7	0,5	0,6	0,65
NomeMalware	0,9	0,9	0,8	1,0	0,90
IP_Controlador	1,0	1,0	1,0	1,0	1,0
PortaCC	0,9	0,5	0,6	0,7	0,68
HostnameCC	0,8	0,6	0,5	0,5	0,60

Malware	Esp 1	Esp 2	Esp 3	Esp 4	Média
IPOrigem	1,0	1,0	1,0	1,0	1,0
HostNameOrigem	0,8	0,6	0,5	0,5	0,60
UrlMaliciosa	0,9	1,0	0,8	0,8	0,88
NomeMalware	0,9	1,0	0,8	1,0	0,93
IPInterno	1,0	1,0	0,8	1,0	0,95
SistOperacional	0,8	0,9	0,7	0,8	0,80

Phishing	Esp 1	Esp 2	Esp 3	Esp 4	Média
IPOrigem	1,0	1,0	1,0	1,0	1,0
UrlComprometida	1,0	1,0	1,0	1,0	1,0

Vazamento de informação	Esp 1	Esp 2	Esp 3	Esp 4	Média
UrlDivulgacao	1,0	1,0	1,0	1,0	1,0

Defacement	Esp 1	Esp 2	Esp 3	Esp 4	Média
IPOrigem	1,0	1,0	1,0	1,0	1,0
UrlComprometida	1,0	1,0	1,0	1,0	1,0
FalhaExplorada	1,0	1,0	1,0	1,0	1,0
SistOperacional	0,9	1,0	0,8	0,8	0,88

Scan	Esp 1	Esp 2	Esp 3	Esp 4	Média
IPOrigem	1,0	1,0	1,0	1,0	1,0
PortasEscaneadas	0,9	1,0	0,8	1,0	0,93

Tentativas de Invasão / Exploração de vulnerabilidades	Esp 1	Esp 2	Esp 3	Esp 4	Média
IPOrigem	1,0	1,0	1,0	1,0	1,0
HostnameOrigem	0,8	0,6	0,5	0,5	0,60
IPDestino	1,0	1,0	1,0	1,0	1,0
Servico	1,0	0,8	1,0	0,9	0,93
Vulnerabilidade	1,0	1,0	1,0	1,0	1,0
URL	0,9	1,0	0,8	0,8	0,88

Copyright	Esp 1	Esp 2	Esp 3	Esp 4	Média
IPOrigem	1,0	1,0	1,0	1,0	1,0
PortaOrigem	0,9	1,0	0,5	1,0	0,85
Hostname	0,8	0,6	0,5	0,5	0,60
Titulo	0,8	0,5	1,0	1,0	0,83
Tamanho	0,7	0,5	0,5	0,5	0,55
Protocolo	0,8	0,5	0,7	0,8	0,70
Url_reclamante	0,9	0,5	1,0	0,8	0,80