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

Marcelo da Luz Colomé

RACIOCÍNIO BASEADO EM CASOS COMO UMA TÉCNICA PARA GESTÃO DO CONHECIMENTO DA RESOLUÇÃO DE INCIDENTES DE SEGURANÇA

Santa Maria, RS
2018

Marcelo da Luz Colomé

RACIOCÍNIO BASEADO EM CASOS COMO UMA TÉCNICA PARA GESTÃO DO CONHECIMENTO DA RESOLUÇÃO DE INCIDENTES DE SEGURANÇA

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

Orientador: Prof. Dr. Raul Ceretta Nunes

Santa Maria, RS

2018

Ficha catalográfica elaborada através do Programa de Geração Automática
da Biblioteca Central da UFSM, com os dados fornecidos pelo(a) autor(a).

Colomé, Marcelo da Luz
Raciocínio Baseado em Casos como uma Técnica para Gestão do Conhecimento da Resolução de Incidentes de Segurança / Marcelo da Luz Colomé.- 2018.
75 f.; 30 cm

Orientador: Raul Ceretta Nunes
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Tecnologia, Programa de Pós-Graduação em Ciência da Computação, RS, 2018

1. Incidentes de Segurança 2. Raciocínio Baseado em Casos 3. Segurança da Informação 4. Sistemas de Resposta à Intrusão I. Ceretta Nunes, Raul II. Título.

Marcelo da Luz Colomé

RACIOCÍNIO BASEADO EM CASOS COMO UMA TÉCNICA PARA GESTÃO DO CONHECIMENTO DA RESOLUÇÃO DE INCIDENTES DE SEGURANÇA

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

Aprovado em 26 de janeiro de 2018:

Raul Ceretta Nunes, Dr.
(Presidente/Orientador)

Márcia Henke, Drª. (UFSM)

Érico Marcelo Hoff do Amaral, Dr. (UNIPAMPA)

Santa Maria, RS

2018

DEDICATÓRIA

Aos meus pais Antonio Blaz Colomé e Maria Salete da Luz Colomé, ao meu irmão Felipe da Luz Colomé e à minha namorada e parceira Renata Bolzan pelo apoio, carinho e compreensão.

AGRADECIMENTOS

Agradeço à minha família e namorada por estarem sempre ao meu lado me acolhendo e me incentivando a seguir na jornada com palavras sábias e sensibilidade ímpar.

Ao meu orientador Prof. Dr. Raul Ceretta Nunes o qual é um exemplo de profissional, sempre dedicado e disposto a contribuir com o que for necessário para o desenvolvimento de um ótimo trabalho.

Aos meus amigos que sempre torceram por mim.

Aos meus colegas de mestrado Everson Lucion, Gabriel Marchesan e Marcos Lucca que sempre estiveram disponíveis para contribuir com o meu trabalho.

Ao meu colega de trabalho Diego Carvalho o qual sempre contribuiu para que eu pudesse desempenhar minhas tarefas no Mestrado com tranquilidade, me cobrindo nas horas em que tive que me ausentar.

À UFSM por ser esta universidade de excelência da qual faço parte como servidor, que me possibilitou estudar desde o curso técnico, passando pela graduação e agora mestrado de forma gratuita.

“We know more than we can tell.”

(POLANYI 1966)

RESUMO

RACIOCÍNIO BASEADO EM CASOS COMO UMA TÉCNICA PARA GESTÃO DO CONHECIMENTO DA RESOLUÇÃO DE INCIDENTES DE SEGURANÇA

AUTOR: MARCELO DA LUZ COLOMÉ
ORIENTADOR: RAUL CERETTA NUNES

Este trabalho demonstra a importância da aplicação de técnicas computacionais para a gestão do conhecimento de incidentes de segurança, oferecendo uma abordagem metodológica para a retenção e reutilização do conhecimento do especialista, visando a resolução de novos incidentes. O conhecimento do especialista em segurança da informação é fundamental para as organizações, pois a resolução eficaz de incidentes de segurança depende do conhecimento dos mesmos. Porém as organizações não devem ser totalmente dependentes de seus funcionários. Desta forma, a metodologia proposta utiliza-se de Raciocínio Baseado em Casos com ponderação dos atributos e o padrão IODEF para a representação destes incidentes, visando a retenção do conhecimento do especialista na resolução de incidentes, possibilitando que outros membros da organização possam desempenhar tarefas similares, diminuindo a dependência da empresa em relação a seus funcionários. Os resultados demonstram que através desta metodologia o conhecimento fica efetivamente retido na base de casos e que novos funcionários podem se beneficiar de recomendações construídas e fornecidas pelo sistema, melhorando com isto a retenção do conhecimento nas organizações.

Palavras-chave: Incidentes de Segurança. Raciocínio Baseado em Casos. Segurança da Informação. Sistemas de Resposta à Intrusão.

ABSTRACT

CASE-BASED REASONING AS A TECHNIQUE FOR KNOWLEDGE MANAGEMENT OF SECURITY INCIDENT RESOLUTION

AUTHOR: MARCELO DA LUZ COLOMÉ
ADVISOR: RAUL CERETTA NUNES

This work demonstrates the importance of applying computing techniques in to the knowledge management of cybersecurity incidents, offering a metodological approach for the retention and reuse of the specialist's knowledge aiming the resolution of new incidents. The information security specialist's knlowledge is central for organizations, because the effective resolution of incidents depends on their knowledge. However organizations should not be totally dependent on their employees. Thus, the proposed metodology uses Cased-based Reasoning with weighted attributes and the IODEF pattern for the representation of those incidents, aiming the retention of the specialist's knowledge on the incidents resolution, allowing other organization members to perform similar tasks, decreasing the dependancy between the company and its employees. The results demonstrate that with this metodology the knowledge is effectively retained in the case-base and that new employees can be benefited from the recomendations built and provided by the system, improoving the knowledge retention in organizations.

Keywords: Case-based Reasoning. Cybersecurity. Incidents. Intrusion Response Systems.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

APT	Advanced Persistent Threat
Bot	Robot
CAIS	Centro de Atendimento a Incidentes de Segurança
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
CPD	Centro de Processamento de Dados
CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
FRM	Frequency, Recency, Monetary
IANA	Internet Assigned Numbers Authority
IDS	Intrusion Detection System
ISO	International Organization for Standardization
IODEF	Incident Object Desciption Exchange Format
IP	Internet Protocol
IPS	Intrusion Prevention System
IRS	Intrusion Response System
K-fold	K-fold Cross Validation
kNN	k-Nearest Neighbours Algorithm
LOOCV	Leave-one-out Cross Validation
MD5	Message-Digest Algorithm
RBC	Raciocínio Baseado em Casos
RFC	Request for Comments
RNP	Rede Nacional de Pesquisa
SGIS	Sistema de Gestão de Incidentes de Segurança
UFSM	Universidade Federal de Santa Maria
URL	Uniform Resource Locator
XML	Extensible Markup Language

SUMÁRIO

1 INTRODUÇÃO

O conhecimento é um ativo importante para as empresas, pois nele estão contidas as lições aprendidas ao longo do tempo, as quais são muito importantes para o desenvolvimento das mesmas (DALKIR; LIEBOWITZ, 2011). A retenção deste conhecimento pode beneficiar funcionários e a empresa como um todo, pois muitos dos problemas que aconteceram no passado podem ser iguais ou semelhantes aos problemas atuais e futuros de uma organização.

A gestão de conhecimento sobre a resolução de incidentes de segurança é algo crítico para muitas organizações, pois incidentes podem causar prejuízos se não forem sanados de forma eficaz. Equipes de Respostas a Incidentes de Segurança Computacionais (CSIRT) vivenciam experiências positivas (soluções que contribuíram com sucesso para resolver um problema) e experiências negativas (tentativas frustradas de solução de um problema). As equipes mudam e novamente elas precisam vivenciar experiências positivas e negativas, ocasionando um retrabalho e desperdício do tempo.

Por outro lado, os incidentes de segurança computacionais representam ameaças de diferentes tipos às organizações. Impactos nas finanças, na publicidade, ou ainda perda de dados são alguns dos exemplos de como uma empresa pode ser afetada por um incidente de segurança (JIANG et al., 2014). Apesar deste significativo número de incidentes, este gerenciamento não é feito de forma sistemática. No Brasil, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERTBR, 2017) reportou 647112 incidentes no ano de 2016, demonstrando a importância no tratamento deste tipo de evento. Sistemas de Resposta à Intrusão (IRS) (INAYAT et al., 2016) são utilizados para tratamento de incidentes de segurança que transpõe barreiras iniciais introduzidas por sistemas de Detecção de Intrusão.

Um IRS é projetado para melhorar as políticas de segurança, tratando incidentes/intrusões detectadas e mitigando os seus efeitos. Porém, a capacidade de um IRS oferecer uma resposta adequada à determinada intrusão está intimamente ligada ao conhecimento da equipe de Resposta e Tratamento de Incidentes, uma vez que a equipe deve construir um plano de resposta aos incidentes. Diferentes incidentes podem exigir diferentes planos de resposta. Este processo faz com que exista uma grande dependência desta equipe (pessoas) para que o incidente possa ser resolvido de forma adequada. O resultado são organizações dependentes do conhecimento de seus colaboradores para a resolução de incidentes. Esta dependência dificulta o reúso de soluções por diferentes colaboradores, devendo ser evitada.

O Raciocínio Baseado em Casos (KOLODNER, 1993) (RBC) é uma técnica capaz de auxiliar na resolução de novos incidentes, pois considera a resolução de incidentes passados. O conhecimento gerado na resolução de problemas passados é armazenado e então reutilizado. O RBC usa uma base de conhecimento para armazenar estes problemas (tupla <problema, solução>), reusando o conhecimento armazenado para a solução de novos problemas. Esta técnica pode ser utilizada para a retenção do conhecimento gerado através da resolução de incidentes de segurança por especialistas, armazenando e reutilizando as lições aprendidas neste contexto.

1.1 MOTIVAÇÃO

O uso de RBC para a resolução de incidentes de segurança começou a ser explorado em (CAPUZZI; SPALAZZI; PAGLIARECCI, 2006) com a proposta de um sistema de suporte à respostas de incidentes. Porém, o foco foi a melhora na detecção de incidentes e não a retenção do conhecimento do especialista. O mesmo acontece em (KIM; IM; PARK, 2010), que propõe a redução de falsos alertas gerando respostas colaborativas, e em (PING; HAIFENG; GUOQING, 2010), que propõem o uso de ontologias e RBC para a construção de um sistema de decisão e resposta à incidentes de segurança, mas que não realiza avaliação sobre a retenção de conhecimento do modelo. No trabalho de (JIANG et al., 2014) é proposto um sistema de RBC com o uso de lógica descritiva para a organização dos atributos para posterior cálculo de similaridade no sistema de RBC, porém o mesmo não apresenta um plano de respostas estruturado para os incidentes de segurança, não retendo este conhecimento. Logo, observa-se que, embora a técnica de RBC esteja sendo utilizada para ajudar na resposta a intrusões, a estruturação de respostas para estes incidentes, como a criação de planos de tratamento ou resposta não é explorada. A estruturação de respostas é fundamental para a retenção do conhecimento do especialista e para a resolução dos incidentes, pois permite criar uma memória organizada dos incidentes e seus tratamentos.

Observa-se ainda que a utilização de protocolos padrão para a troca de informações sobre incidentes de segurança também não é explorada, o que dificulta a comunicação entre CSIRT distintos. A ponderação de atributos de RBC é pouco explorada, o que poderia permitir ao especialista potencializar a precisão do sistema, uma vez que com esta ponderação é possível a atribuição de diferentes pesos aos atributos.

1.2 OBJETIVOS E CONTRIBUIÇÕES

O objetivo deste trabalho é a proposição de uma metodologia para IRS que explora RBC para automatização de recomendações de planos de resposta à incidentes de segurança. A metodologia difere-se das demais aplicações de RBC neste contexto, por explorar: i) a padronização IODEF (DANYLIW; MEIJER; DEMCHENKO, 2007)(TAKAHASHI et al., 2014) para representação de dados, um padrão voltado a informações relacionadas a incidentes de segurança e adotado pelo CERT.BR; ii) a ponderação de atributos dos casos de incidentes; e iii) a geração automatizada de *Planos para o Tratamento dos Incidentes*.

A principal contribuição deste trabalho é uma metodologia que permita às equipes dos CSIRT o reúso do conhecimento relativo à resolução de incidentes de segurança através do uso de técnicas de RBC. O resultado demonstra que o mecanismo proposto para IRS baseado em RBC proporciona potencialização de uso de experiência prévia de especialistas e a resolução eficiente de novos incidentes pela recuperação e reúso destas experiências.

1.3 ORGANIZAÇÃO DO TEXTO

O texto da dissertação está organizado da seguinte forma. O Capítulo 2 apresenta alguns fundamentos teóricos os quais abordam conceitos importantes para a compreensão deste trabalho. O Capítulo 3 apresenta trabalhos relacionados encontrados na literatura. O Capítulo 4 apresenta uma proposição metodológica de um IRS que utiliza o paradigma de RBC para a retenção do conhecimento do especialista sobre a resolução de incidentes de segurança computacionais. No Capítulo 5 são demonstrados experimentos os quais fundamentam a adoção da metodologia proposta. Por fim, o Capítulo 6 apresenta as conclusões do trabalho juntamente com sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Para a compreensão deste trabalho, são apresentados conceitos importantes a seguir. A Seção 2.1 aborda a Gestão do Conhecimento. Na Seção 2.2 é apresentada a técnica de Raciocínio Baseado em Casos (RBC). Na Seção 2.3 destaca-se a definição de incidentes de segurança, como é realizado o tratamento destes incidentes, o funcionamento dos CSIRT (Equipes de Resposta a Incidentes de Segurança Computacionais), o padrão para representação de incidentes IODEF (Incident Object Description Exchange Format) e o funcionamento de Sistemas de Resposta à Intrusão. Por fim, na Seção 2.4 são apresentadas as considerações parciais deste Capítulo.

2.1 GESTÃO DO CONHECIMENTO

A construção e difusão do conhecimento tem se tornado cada vez mais cruciais. Segundo (DALKIR; LIEBOWITZ, 2011), o conhecimento está presente em produtos tecnológicos e principalmente na mente de funcionários qualificados. Apesar do conhecimento ser atualmente considerado uma comódite, ou um ativo intelectual, ele demonstra-se radicalmente distinto de outros ativos ou comódites tradicionais, pois o mesmo pode ser utilizado e/ou transferido sem que haja gasto ou perda de conhecimento da parte de quem o possui. Apesar da importância deste ativo, muitas organização não atentam para o fato de que uma valiosa porção desta comódite simplesmente vai embora da empresa no final do expediente quando os funcionários vão para suas casas. Ademais, pode também haver uma fuga do conhecimento quando os funcionários deixam a empresa de forma definitiva.

O fato de o conhecimento ter se tornado um ativo importante para as empresas, fez com que se criasse uma grande necessidade de utilização de uma abordagem sistemática para o cultivo e compartilhamento do conhecimento, incluindo valiosas lições aprendidas pelas empresas, juntamente com melhores práticas para a execução de tarefas. Desse modo, para ganhar competitividade, as empresas tem investido cada vez mais no aprendizado a partir de experiências passadas, evitando que as mesmas necessitem reinventar uma solução que já foi aplicada, mas que não foi armazenada como uma lição aprendida (RAHIMLI, 2012). A gestão do conhecimento foi inicialmente definida como o processo de aplicar uma abordagem sistemática para a captura, estruturação, gestão e disseminação do conhecimento em cada parte da organização

objetivando um trabalho mais veloz, reutilizando as melhores práticas e assim reduzindo o custo do retrabalho em novos projetos (NONAKA; TAKEUCHI, 1995).

Segundo (DALKIR; LIEBOWITZ, 2011), alguns dos objetivos da gestão do conhecimento nas organizações são:

a) facilitar uma transição suave entre empregados que estão deixando a empresa e seus sucessores que foram recrutados para substituí-los;

b) minimizar a perda da memória corporativa durante aposentadorias ou redução de pessoal;

c) desenvolvimento de ferramentas (métodos) que possam ser utilizados pelas organizações para estancar possíveis perdas de capital intelectual.

Para que estes objetivos sejam alcançados é necessário entender os tipos principais de conhecimento que podem ser geridos: tácito e explícito. O conhecimento tácito é aquele o qual temos dificuldades em expressar, seja em palavras, textos ou desenhos. O conhecimento explícito é o que pode ser representado ou capturado, que é palpável, como textos, gravações ou imagens (DALKIR; LIEBOWITZ, 2011). Apesar da explicação simplista sobre os dois tipos de conhecimento, existe uma grande complexidade no que toca a definição do que é tácito e explícito para uma pessoa. Além do mais, o conhecimento a cerca de um tema pode ser considerado tácito para uma pessoa e explícito para outra. Ainda segundo o referido autor, especialistas habilidosos e experientes geralmente encontram maior dificuldade em explicitar o conhecimento. Já pessoas pouco experientes tem mais facilidade na verbalização pelo fato de eles estarem aprendendo algo com o auxílio de manuais e tutoriais.

Na perspectiva atual, a gestão do conhecimento tem um papel importante no que diz respeito ao desafio de gerenciar a complexidade criada por ambientes de trabalho sobrecarregados de informações. Todos os dias especialistas em diversas áreas, como o profissional de segurança da informação, tem que lidar com centenas de *e-mails*, relatórios, telefonemas e ainda resolver problemas de segurança. Assim, além de lidar com este conhecimento explícito, a gestão do conhecimento deve também elaborar estratégias para capturar o conhecimento tácito.

Um problema típico da gestão do conhecimento é a correta representação das lições aprendidas por uma organização. As lições aprendidas são armazenadas pelo simples fato de que ela pode se beneficiar em vários sentidos com o seu armazenamento. O principal objetivo é ensinar a qualquer membro da organização a desempenhar tarefas similares, com a vantagem

de uma abordagem inteligente que facilite o desempenho delas. No caso de incidentes de segurança, as lições aprendidas dão conta de como a empresa resolveu seus incidentes e como esse conhecimento deve ser armazenado para que o mesmo possa ser reutilizado para o tratamento de novos incidentes. Isto significa que não basta que seja feita apenas a retenção do conhecimento, sua gestão deve ser realizada de forma que possa ser facilmente reutilizado, criado e distribuído para que um sistema baseado em conhecimento possa ser efetivo.

2.2 RACIOCÍNIO BASEADO EM CASOS

A gestão do conhecimento compreende iniciativas que corroborem para uma alocação racional do conhecimento do ponto de vista organizacional e de sistemas computacionais (RICHTER; WEBER, 2013). A criação, distribuição e reúso do conhecimento fazem parte deste processo. A utilização de RBC é uma das formas de implementação da gestão do conhecimento sobre um repositório, que neste caso é denominado base de casos. Existe uma afinidade entre a metodologia de RBC e a gestão do conhecimento que possibilitam a sua utilização em conjunto. Porém deve-se notar a importância da correta representação do artefato de conhecimento armazenado em um caso de RBC.

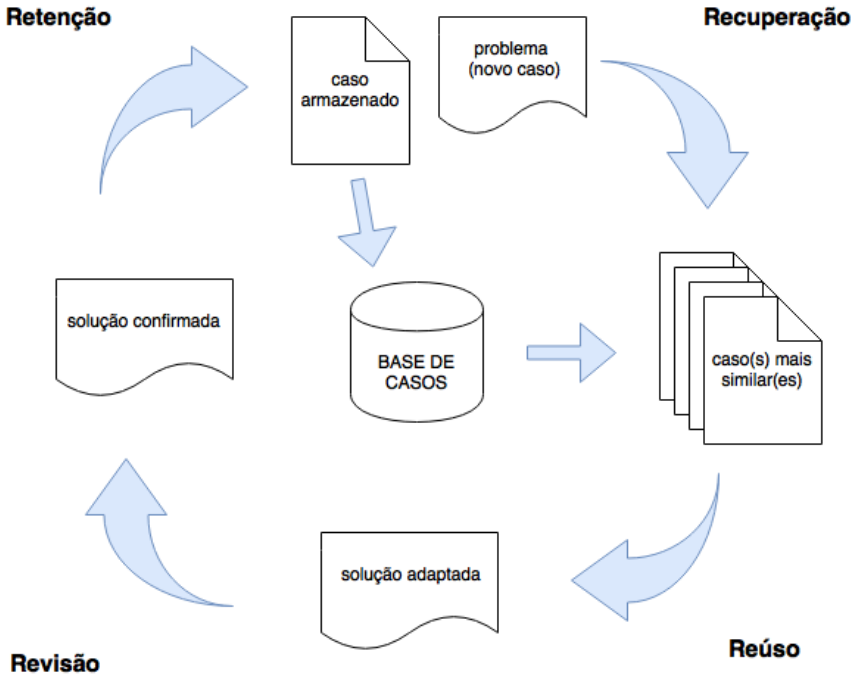
O Raciocínio Baseado em Casos (RBC), do inglês *Case-based Reasoning* (CBR), é um paradigma para a resolução de problemas e para o aprendizado com base em experiências passadas. Neste paradigma, a solução de novos problemas é realizada por meio da reutilização de soluções encontradas em problemas passados. Tais problemas são chamados de casos, os quais são mantidos em uma base de casos. Um caso representa a descrição de uma situação juntamente com as experiências adquiridas durante a resolução deste problema, sendo percebido como uma associação de dois conjuntos de informações: descrição do problema e sua solução (KOLODNER, 1993). O ciclo de funcionamento de um sistema de RBC que é ilustrado na Figura 1 é composto por quatro etapas de execução, conhecida como 4Rs:

a) Recuperação: recuperar da base um conjunto de casos onde a descrição do problema é similar ao problema atual (utilizado como consulta);

b) Reúso: reutilizar as soluções dos casos recuperados para solucionar o problema atual;

c) Revisão: revisar a solução proposta considerando possíveis diferenças entre o problema atual e casos passados recuperados;

Figura 1 – Ciclo de RBC.



Fonte: Adaptada de (WANGENHEIM; WANGENHEIM, 2013).

d) Retenção: aprender a nova experiência para solucionar problemas futuros.

Um dos principais aspectos de RBC diz respeito à similaridade entre os objetos. A cada pesquisa na base de casos são realizadas comparações para que seja possível apontar quais casos possuem semelhança, assim resgatando os mais semelhantes. O conceito de similaridade pode ser visto como uma relação e também como uma função. No caso da relação, busca-se identificar o quão perto estão os casos entre eles, e então agrupar os semelhantes. Para isto o algoritmo *k-Nearest Neighbours* (k-NN) é utilizado. Ele busca fazer um ranking dos vizinhos mais próximos, porém sem apontar um valor numérico que expresse o quão semelhantes são estes objetos, apenas apontando um valor binário que indica se os objetos são ou não semelhantes para que possam ser enquadrados como vizinhos. Já a noção de similaridade como uma função busca identificar o quão longe estão os casos entre eles. Após a seleção inicial dos vizinhos, executa-se o cálculo de distância, buscando-se expressar numericamente o quão semelhantes são os casos entre sí, possibilitando uma melhor precisão no que diz respeito a semelhança entre eles. Para o cálculo de distância podem ser utilizados diferentes métodos, sendo que um dos mais utilizados é o cálculo de distância euclidiana (RICHTER; WEBER, 2013).

No contexto de incidentes de segurança, RBC pode ser utilizado para apoiar o processo de resolução destes problemas. Como explicado por (WIIG, 1997), organizações podem adotar

diferentes estratégias para a gestão do conhecimento, que podem compreender gerenciamento de ativos intelectuais, criação e transferência de conhecimento. Assim, segundo (MANSAR; MARIR; REIJERS, 2003), de um ponto de vista técnico, existem muitos argumentos que suportam o uso de RBC para a gestão do conhecimento, facilitando a utilização destas estratégias. A forma de representação de dados com exemplos concretos são mais entendíveis e aplicáveis em vários contextos de resolução de problemas do que cadeias complexas de raciocínios gerados por regras ou modelos, justamente por ser possível um armazenamento em bases relacionais, que permitem inserções e atualizações de forma simplificada. Outro benefício é a possibilidade de o RBC aprender de forma sistemática com experiências passadas, através dos passos de revisão e retenção, providenciando um *framework* para a aquisição do conhecimento como parte do uso diário da aplicação.

2.3 INCIDENTES DE SEGURANÇA

Uma das principais premissas do monitoramento de redes de computadores é de que brechas de segurança são inevitáveis (BEJTLICH, 2013). Apesar do maciço uso de ferramentas de contenção como *firewalls*, Sistemas de Detecção e Prevenção de Intrusões, tentativas de intrusão podem transpor estas barreiras iniciais e se tornarem grandes ameaças às corporações. O correto tratamento de incidentes corrobora para a minimização de seus impactos. Um incidente é uma violação (ou uma ameaça iminente) às políticas de segurança, práticas de uso aceitáveis ou práticas de segurança. Portanto são considerados incidentes: ataques de negação de serviço, compartilhamento não autorizado de informações, ataques maliciosos em um computador ou rede, exclusão documentos por descuido, etc (AHMAD; HADGKISS; RUIGHAVER, 2012).

2.3.1 Tratamento de Incidentes de Segurança

Com o objetivo de tratar os incidentes, as empresas investem na coleta de dados sobre estas intrusões para que eles sejam analisados e melhor entendidos, e assim elas possam aprender a lidar de uma melhor forma com este tipo de ameaça. O fator temporal é um elemento chave no que toca as estratégias para o correto tratamento de um incidente, pois quanto antes um incidente é contido, menores são os impactos do mesmo (BEJTLICH, 2013). Um CSIRT pode obter sucesso na contenção de incidentes se ele obtiver meios rápidos de tratamento. A retenção das lições aprendidas é uma maneira de preparação para o enfrentamento de incidentes

de segurança.

De acordo com a ISO/IEC 27035 (ISO-27035, 2011), o processos de tratamento de incidentes dividi-se em cinco fases:

a) Planejar e preparar: nesta etapa deve-se pensar na elaboração de planos de tratamento de incidentes para tipos específicos, *check-lists* de tarefas e rotinas para quando uma eventualidade acontecer e planos de comunicação que irão conter informações de como as entidades envolvidas irão se comunicar durante a calamidade. Um plano de contenção, resposta ou tratamento de incidentes deve fazer parte da rotina de uma organização. É preciso estar preparado para o enfrentamento destes problemas, e a elaboração de um plano para realizar estas tarefas é algo fundamental. A geração deste plano pode ser facilitado com o uso das lições aprendidas, pois muitos problemas são recorrentes e/ou semelhantes aos que já foram enfrentados pelas organizações. O plano é uma estratégia que descreve um modo apropriado de se resolver um incidente (PROSISE; MANDIA; PEPE, 2003). Ele é descrito com as ações que devem ser tomadas para que o incidente seja contido. Essas ações são representadas por uma série de passos que são desenvolvidos através da análise dos *logs* gerados por incidentes e geralmente é elaborado por um especialista da área de segurança computacional. É importante também que as organizações tenham uma boa definição do que será considerado incidente, pois deve-se possuir capacidade para distinguir um incidente de outros problemas que possam ocorrer, como falhas de configuração. Nesta fase é também desejável que se tenha tarefas proativas como testes de penetração e vulnerabilidades. Também deve-se considerar a utilização de ferramentas que facilitem este processo, diminuindo assim o tempo no qual a organização estará exposta ao incidente (TøNDEL; LINE; JAATUN, 2014);

b) Detectar e reportar: (METZGER; HOMMEL; REISER, 2011) recomenda que sejam utilizados múltiplos meios para reportar um incidente. Eles podem ser reportados de forma automática por serviços ou outra entidade como CERTs, e também de forma manual, como por telefone e *e-mail*. O uso de ferramentas como antivírus, IDS, IPS, *firewall*, monitoramento de *e-mails* e análise de tráfego são importantes para a detecção de incidentes, porém não deve-se confiar totalmente nestas ferramentas visto que elas geram também muitos falsos-positivos. Faz-se também necessário observar que os incidentes podem não ser detectáveis por estas ferramentas, como em incidentes causados por empregados desleais (METZGER; HOMMEL; REISER, 2011). Tão logo um incidente acontece, o mesmo deve ser reportado e acompanhado (pode-se utilizar ferramentas de *tracking*) para que o mesmo seja resolvido.

Porém em muitos casos os funcionários não os reportam por considerá-los de baixo impacto, ou ainda por temerem algum tipo de consequência em relação à sua reputação. Ainda de acordo com (METZGER; HOMMEL; REISER, 2011), a experiência profissional dos empregados é muito importante para a realização de análise, seguida pela documentação de incidentes passados e sistemas de *help desk*;

c) Avaliar e decidir: nesta etapa deve-se verificar primeiramente se o incidente realmente ocorreu, posteriormente verificando sua magnitude e consequências, e então rastrear sua origem. A decisão de como lidar com um incidente requer além de pessoal capacitado, que se observe quem deve tratar o incidente quando a empresa utiliza-se de recursos supridos por outra empresa. No caso em que a empresa A contrata serviços de banco de dados da empresa B, deve-se pensar em quem será o responsável por tratar incidentes de vazamento de informações caso ocorra, e como será feita a comunicação entre as empresas;

d) Responder: Segundo (HOVE; TARNES, 2013), as respostas a serem dadas devem refletir as ações planejadas na etapa anterior (avaliar e decidir). Utiliza-se o plano de tratamento como base para a tomada de ações o qual possui os passos recomendados para contornar o incidente. Deve-se tomar as medidas apropriadas, incluindo recuperar-se do incidente, documentação, e comunicação às partes interessadas. O autor ainda salienta que cada ação tomada deve ser documentada para que se possa no futuro analisar o quão efetiva foi a solução dada a um incidente. Uma vez que o incidente é contornado, o mesmo deve ser formalmente encerrado e registrado pelo CSIRT;

e) Registrar as lições aprendidas: esta última etapa deve ser iniciada tão logo o incidente foi encerrado e tem o intuito de analisar se a solução projetada pelo CSIRT teve sucesso. Aprender sobre os incidentes é importante, porém muitas organizações acham difícil colocar isso em prática (TøNDEL; LINE; JAATUN, 2014). Uma das tarefas realizadas neste passo é a documentação apropriada, garantindo que o método de tratamento do incidente é preciso. O compartilhamento de informações com outros CSIRT deve ser realizado de forma regular independentemente se ele ocorreu internamente, pois há meios de se compartilhar estes incidentes omitindo informações sensíveis (HOVE; TARNES, 2013). Ainda segundo o autor, revisões, análises de tendências e testes devem ser efetuados regularmente com o objetivo de melhorias no tratamento dos incidentes ao longo do tempo.

Percebe-se então que o tratamento de incidentes possui ainda alguns aspectos considera-

dos desafiadores, o que demanda o surgimento de novas ferramentas e recomendações específicas em algumas áreas (TøNDEL; LINE; JAATUN, 2014). Deve-se pensar na criação de planos de tratamento e classificação de incidentes, compromisso do profissional de segurança para com a resolução dos incidentes, envolvimento de funcionários para que os mesmos reconheçam e reportem incidentes, lidar com ferramentas apropriadas, manter uma memória organizada sobre os incidentes, colaboração entre times responsáveis por tarefas técnicas e de gestão, definir responsabilidades junto com parceiros, motivar os funcionários a gerar aprendizado com os incidentes e compartilhar as lições aprendidas para que outras organizações possam ser beneficiadas com as informações.

2.3.2 Equipes de Resposta a Incidentes de Segurança Computacionais - CSIRT

Uma vez que um incidente acontece, é necessário estar preparado para tomar as medidas necessárias para contorná-lo. Um CSIRT - Equipe de Resposta a Incidentes de Segurança Computacionais, do inglês *Computer Security Response Team*, é responsável por esta tarefa. Dependendo da estrutura da organização, este time pode ser composto apenas de um especialista ou de vários. A equipe pode ser responsável por eventos que afetem apenas a organização em questão ou também organizações externas. A tarefa de definir a abrangência é uma das primeiras a ser desenvolvida quando pretende-se criar um CSIRT.

Segundo (RAJNOVIC, 2011) um CSIRT deve ser uma entidade à parte em uma empresa, não devendo estar atrelado à hierarquias. Isto é necessário para que ela tenha independência, principalmente financeira em relação à organização. Ainda segundo o autor, CSIRT representam custos que muitas vezes são vistos como gastos desnecessários, pois as empresas podem ter uma visão de que equipes de segurança não trazem dinheiro para elas, apenas gastam. Desta forma, se um CSIRT é um órgão como qualquer outro dentro empresa, ele pode sofrer os primeiros cortes no orçamento em épocas de crise financeira. Um CSIRT deve possuir um *Executive Sponsor* que é a pessoa que faz o meio campo entre o time e a empresa. É ele que levará as demandas do time para a organização (principalmente financeiras) e tomará decisões emergenciais juntamente com o setor executivo.

Outro fato importante listado pelo autor, corrobora com a ideia da gestão do conhecimento sobre a resolução de incidentes de segurança. Cada vez que um novo especialista é contratado, ele deve estudar os processos e procedimentos envolvidos no tratamento dos incidentes. Isto pode causar uma "perda de memória" do time, pois o conhecimento dos antigos

membros, que eram mais experientes, não está mais presente. Esta "perda de memória" pode gerar uma grande perda de tempo, pois o time terá que reinventar uma solução para um incidente, porque ninguém mais do grupo antigo de especialistas experientes está presente para lembrar de como solucionar o problema. Assim, um CSIRT deve ser capaz de organizar suas lições aprendidas de modo que elas possam ser facilmente reutilizadas.

2.3.3 *Incident Object Description Exchange Format* - IODEF

A troca de dados entre sistemas e a padronização nas representações dos dados são elementos chave para interoperabilidade entre sistemas de segurança. Em geral padrões de representação de dados são compostos por diferentes tipos de informações, as quais são muitas vezes coletadas automaticamente. O padrão IODEF fornece um *framework* para o compartilhamento de informações comumente trocadas por CSIRT sobre incidentes de segurança computacionais.

O IODEF (DANYLIW; MEIJER; DEMCHENKO, 2007) é um padrão criado pela IETF que define uma representação de dados para informações relacionadas a incidentes de segurança, e que inclui dados relacionados a *hosts*, redes e serviços que são executados nestes sistemas; metodologia de ataques e evidências forenses; impacto da atividade; e abordagem para documentação do fluxo de trabalho. Este padrão possui 34 classes no total, sendo o mesmo desenvolvido para ser adaptável às diferentes necessidades das organizações. Pode-se utilizar todas as classes ou apenas as que sejam necessárias. Duas das principais classes são a classe $IODEF\text{-}Document$ e $Incident$.

A classe $IODEF\text{-}Document$ é a classe principal deste formato de dados, sendo todos os documentos IODEF uma instância desta classe. Esta classe possui informações sobre a versão do documento, linguagem e informações sobre o processamento do documento, bem como uma classe agregada $Incident$, a qual pode ter uma ou mais instâncias de incidentes (um documento pode se referir a um ou mais incidentes).

A classe $Incident$ oferece uma representação padrão para a troca de dados sobre incidentes comumente reportados. Ela possui informações sobre o motivo da criação do documento IODEF, linguagem do documento e restrições. Possui também quatorze classes agregadas para a representação das seguintes informações: identificador do incidente, identificadores alternativos, identificadores para incidentes relacionados, momento em que o incidente foi detectado, momento em que teve início o incidente, momento em que teve fim o incidente, momento em que o incidente foi reportado, descrição do incidente, técnicas usadas pelo invasor, informa-

ção de contato das partes envolvidas no incidente, descrição dos eventos que compreendem o incidente, histórico de eventos e ações que ocorreram durante contenção do incidente e dados adicionais que não cabem no modelo.

Posteriormente foi desenvolvida uma extensão ao padrão IODEF: o *IODEF Extension for Structured Cybersecurity Information* (TAKAHASHI et al., 2014) (TAKAHASHI; MIYAMOTO, 2016). Esta extensão visa uma melhora na troca de informações feitas por meios automatizados, melhorando a leitura automática (por computador) das mensagens. As seguintes informações foram contempladas nesta extensão: padrão do ataque, informação da plataforma, vulnerabilidades e fraquezas, instruções para contra medidas, *logs* de eventos computacionais e grau de severidade. Segundo os autores da extensão, apesar do IODEF permitir que essas informações fossem expressas, ele não definia formatos detalhados para especificar as informações.

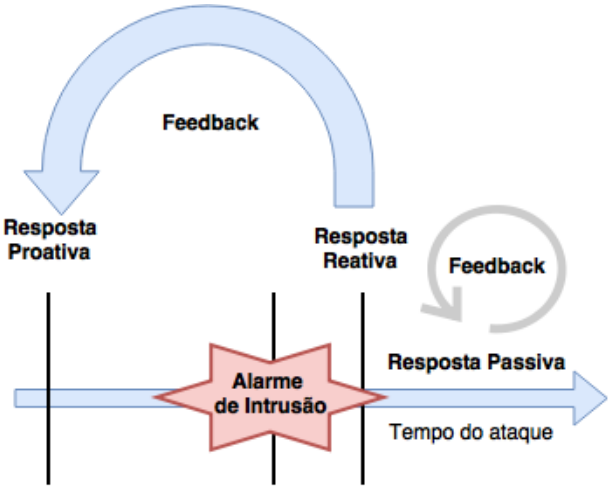
2.3.4 Sistemas de Resposta à Intrusão

Enquanto sistemas baseados em IDS e IPS detectam e previnem potenciais intrusões em tempo real, sistemas de IRS trabalham no intuito de gerar contra medidas para as intrusões que transpuseram essa barreira inicial (INAYAT et al., 2016). É sabido que apesar do grande uso de tecnologias baseadas em dados e conhecimento de problemas de segurança, os quais são voltados para alertar ou impedir intrusões, ainda assim entidades como CERTs espalhados pelo mundo recebem por dia milhares de alertas sobre novas intrusões. Cabe então a um sistema de IRS a responsabilidade de automatizar a identificação e tratamento de contra medidas para atenuar os efeitos de intrusões. Segundo (ANUAR et al., 2010), no que toca a taxonomia, um IRS pode ser dividido em dois tipos principais: ativo e passivo.

Um IRS ativo opera utilizando métodos inteligentes para a automatização da resposta, que pode ser proativa ou reativa. A resposta proativa é aquela em que o conhecimento sobre incidentes de segurança é utilizado para produzir uma resposta antes do incidente acontecer. Embora rápidas, respostas proativas podem oferecer respostas não apropriadas para alguns casos (falso-positivos), visto que não possuem interferência humana. Um exemplo de resposta é um servidor bloquear um *host* ou rede de forma equivocada causando um incidente de DoS (Negação de Serviço) na própria rede. Por outro lado, a resposta reativa caracteriza-se por acontecer apenas depois que a intrusão é detectada. Sua vantagem é viabilizar a interferência de um especialista antes da resposta ser efetivada. Em geral a experiência do especialista minimiza possíveis erros causados pela automatização do processo.

Um IRS passivo normalmente visa a notificação das partes interessadas sobre a ocorrência de um incidente, confiando nelas para que sejam tomadas decisões futuras. O sistema não visa minimizar o impacto do incidente em si. Ele agora tem a responsabilidade de notificar e coletar informações sobre a intrusão para que sejam usadas futuramente no combate a novos ataques, gerando memória reusável para apoiar e melhorar a solução destes problemas. A Figura 2 ilustra o relacionamento entre os diferentes tipos de resposta dos IRS e o tempo de reação do sistema aos incidentes. Percebe-se que, independente do tipo de IRS, o conhecimento de causa/tratamento relacionado a respostas reativas e passivas pode fornecer informações de *feedback* para respostas proativas, habilitando melhora na reação à novos incidentes.

Figura 2 – Relacionamento entre resposta passiva, proativa e reativa.



Fonte: Adaptada de (ANUAR et al., 2010).

2.4 CONSIDERAÇÕES PARCIAIS

Este Capítulo apresentou alguns conceitos fundamentais para o entendimento deste trabalho. Como foi observado, a Gestão do Conhecimento nos permite armazenar as lições aprendidas por uma organização a fim de que este conhecimento possa ser acessado por outros membros dela, facilitando a resolução de novos problemas. Foi destacado também a afinidade entre a Gestão do Conhecimento e o paradigma de RBC, o qual oferece uma abordagem sistemática para aquisição e reúso de experiências. Além disso foi destacado o funcionamento de um sistema de IRS o qual pode ser considerado ativo, no caso de o mesmo gerar contra medidas de forma automatizada, ou passivo se o mesmo depende da atuação de um especialista para contornar o incidente. Foi detalhado também o funcionamento e atuação dos CSIRT bem como a

importância do uso do IODEF para a troca de mensagens entre estes times.

3 TRABALHOS RELACIONADOS

Neste capítulo são apresentados os trabalhos relacionados que foram selecionados com a utilização do método de revisão sistemática de literatura. Após uma breve etapa de planejamento, foram definidas as seguintes plataformas como fontes de pesquisa: Association for Computing Machinery (ACM), Advanced Computing: An International Journal (ACIJ), Google Scholar, IEEE Explore, Portal de Periódicos CAPES/MEC e ScienceDirect. Foram então pesquisadas as plataformas em busca de livros, artigos, teses e resumos que possuíssem relação com a temática de gestão do conhecimento sobre incidentes de segurança computacionais, incluindo posteriormente também estudos que abordassem a resolução destes incidentes, bem como estudos que se utilizassem de Raciocínio Baseado em Casos para isso. Foram selecionados 31 trabalhos para avaliação de qualidade dos quais foram incluídos os apresentados neste capítulo. Na Seção 3.1 são apresentados trabalhos que possuem um viés organizacional. Na Seção 3.2 são apresentados trabalhos que sugerem *frameworks* para o tratamento dos incidentes. Na Seção 3.3 são apresentados trabalhos que utilizam-se de Raciocínio Baseado em Casos. Por fim, na Seção 3.4 são apresentadas as considerações parciais deste Capítulo.

3.1 TRABALHOS COM VIÉS ORGANIZACIONAL

O tratamento de incidentes de segurança computacionais é tratado em alguns estudos do ponto de vista de gestão organizacional, no qual são apontados alguns padrões e boas práticas, e também algumas experiências do mundo corporativo.

No trabalho de (HOVE; TARNES, 2013) é apontado que apesar de existirem alguns padrões que ofereçam boas práticas na gestão de incidentes de segurança, existem poucos estudos sobre como estas boas práticas tem sido conduzidas pelas organizações. Desta forma, neste estudo os autores apontam algumas das boas práticas e conduzem um estudo de caso em três empresas estabelecidas na Noruega utilizando-se de entrevistas e estudo da documentação das empresas. O estudo concluiu que as organizações estão relativamente de acordo com padrões e recomendações na gestão dos incidentes, mas que porém existe espaço para melhorias. Os resultados demonstraram que comunicação, disseminação da informação, envolvimento dos funcionários, experiência e definição de responsabilidades são fatores importantes para um processo de gestão efetiva e eficiente. Os autores ainda recomendam que as organizações utilizem

padrões e boas práticas, conduzam simulações regulares (ensaios), estimulem os funcionários a reportarem incidentes e realizem companhas de conscientização dos empregados sobre os incidentes de segurança.

No trabalho de (TøNDEL; LINE; JAATUN, 2014), é apresentada uma revisão sistemática de literatura sobre práticas e experiências relacionadas a gestão de incidentes de segurança nas organizações. O principal objetivo do trabalho foi a identificação de como os incidentes são gerenciados pelas empresas na prática. Os autores destacam que embora as empresas seguem em parte as diretrizes de recomendações e boas práticas, ainda existe uma necessidade de melhoria em relação às ferramentas de detecção e resposta. Além disso são apontadas algumas orientações necessárias, como a criação de *templates*, ou exemplos de planos tratamento de incidentes que possam ser utilizados no futuro. Ainda, os autores apontam a necessidade de um melhor entendimento do papel do conhecimento tácito, e implementação e avaliação de estratégias para lidar com a dependência em relação a este tipo de conhecimento.

O trabalho de (AHMAD; HADGKISS; RUIGHAVER, 2012), foi motivado pelo fato de que estudos prévios sugerem que a prática de respostas aos incidentes frequentemente não resultam em melhorias no processo estratégico, como o desenvolvimento de políticas e de relatórios de risco. Foi desenvolvido um estudo de caso em uma grande instituição financeira para examinar as suas deficiências na prática de resposta aos incidentes. O estudo revelou que as boas práticas existentes tendem a possuir um foco técnico que se limita a manter a continuidade dos negócios da empresa enquanto negligenciam aspectos estratégicos de segurança. Outro fator apontado no estudo diz respeito a revisão pós-incidente, adotada na etapa de registro das lições aprendidas da ISO/IEC 27035, que é mais direcionada a tratar incidentes de grande impacto, do que a incidentes que possam ser úteis para aprendizado.

O trabalho de (AHMAD; MAYNARD; SHANKS, 2015) apresenta um estudo de caso e aborda as deficiências relacionadas às práticas de resposta à incidentes de uma instituição financeira da Austrália. De acordo com o artigo, poucos estudos abordam como as experiências dos CSIRT podem ser utilizadas para a melhoria dos processos de segurança, sendo isto significante pelo fato de que estas equipes acumulam experiências consideráveis na resolução de falhas de segurança e ataques. Desta forma os autores concluem que a colaboração entre CSIRT, apesar de desejável, muitas vezes não ocorre porque eles consideram que pode ocorrer falta de entendimento entre os times ou que podem ocorrer conclusões precipitadas que podem levar a constrangimentos. O estudo também aponta que os CSIRT ignoram deliberadamente oportu-

nidades de registrar lições aprendidas por conta de prioridades relacionadas a restabelecimento de serviços, o que impede uma análise mais detalhada dos incidentes.

O trabalho de (LEMAY; LEBLANC; JESUS, 2015) cita a ciberespionagem como protagonista de novos e complexos ataques como o APT (*Advanced Persistent Threat*) e sugere a utilização de lições aprendidas na área militar com o objetivo de uma melhor abordagem para o tratamento de incidentes. Esta abordagem constituí-se de três soluções, conhecidas como: treinamento, intenção do comandante e tomada de decisão descentralizada. O treinamento tem como objetivo tornar a equipe mais preparada para lidar com situações reais. A intenção do comandante diz respeito a comunicação entre o *security manager* e a equipe que deve ser realizada de forma bem específica e direta. A decisão descentralizada diz respeito a uma cultura de decisão intuitiva, na qual a habilidade dos subordinados tomarem decisões é incentivada. A pesquisa não utiliza-se de métodos de validação e apenas conclui que a complexidade do ambiente militar é semelhante a de um CSIRT e por este motivo, algumas estratégias de guerra podem ser utilizadas para tratar estes novos ataques.

No trabalho de (METZGER; HOMMEL; REISER, 2011) é apresentado um sistema integrado de gerenciamento de incidentes que foi aplicado em uma rede de pesquisa de algumas universidades alemãs. Este sistema é composto de algumas soluções de detecção, *report* e resolução de incidentes. Os incidentes quando reportados são classificados em dez categorias como: *botnet*, *spam*, *scan*, etc. Posteriormente são juntadas mais informações provenientes de *logs*. O incidente então serve como entrada para um sistema que identifica, com ajuda de especialistas, se o mesmo vai ser resolvido de forma automática ou manual. Os incidentes considerados de baixo impacto são resolvidos com comandos de bloqueio no *firewall*, já os outros passam por um processo mais detalhado. De acordo com os autores o método se demonstrou eficiente para um gerenciamento integrado dos incidentes. Apesar disso, o artigo não aborda a gestão do conhecimento sobre incidentes de segurança, não considerando o potencial das lições aprendidas para a resolução dos incidentes.

3.2 TRABALHOS QUE APRESENTAM *FRAMEWORKS*

Em outros dois trabalhos são apresentados *frameworks* com um viés mais prático em relação a resolução dos incidentes de segurança.

No trabalho de (LAMIS, 2010) é apresentada uma abordagem forense para respostas a incidentes. Em relação à resolução dos incidentes, o trabalho propõe um *framework* para a

resolução dos mesmos o qual é compreendido dos seguintes passos: identificação, contenção, erradicação e acompanhamento. Segundo o artigo a abordagem forense é utilizada para analisar e documentar evidências digitais de origens variadas, com o uso de algumas técnicas, com o propósito de revelar as razões por detrás do incidente e as pessoas responsáveis pelo ataque. Os autores concluem que além da prevenção, é crucial que seja realizada a documentação de todo o processo de resolução, e que a abordagem forense pode trazer evidências que possam sustentar um processo legal contra os invasores.

Já (KHURANA et al., 2009) apresenta um *framework* para investigação e resposta colaborativa a incidentes de segurança. O trabalho parte do pressuposto que diante do aumento de complexidade e frequência de ataques, é insuficiente confiar no CSIRT para contornar incidentes. Os autores apresentam um *framework* que permite aos profissionais de segurança responderem aos incidentes de forma colaborativa. Eles argumentam que a ideia surgiu a partir das lições aprendidas em um ataque que aconteceu em 2004. O modelo é composto de dois componentes, o que define os papéis e responsabilidades, e o que define os passos da resolução do incidente. É criado um protótipo com um conjunto de ferramentas para responder aos incidentes, porém nenhuma informação relativa a incidentes passados é utilizada para resolver os novos incidentes. Os autores concluem que a utilização de ferramentas para apoiar a resolução de incidentes é fundamental diante da complexidade dos ataques atuais.

3.3 TRABALHOS QUE UTILIZAM RBC

Alguns trabalhos utilizam Raciocínio Baseado em Casos (RBC) para apoiar a resposta à incidentes de segurança, principalmente para fins de detecção de intrusão, onde dados de ataques que aconteceram no passado são utilizados para identificar novos ataques.

No trabalho (JIANG et al., 2014) é proposto um sistema de RBC com o uso de lógica descritiva para a organização dos atributos para posterior cálculo de similaridade. É proposta uma hierarquia de atributos advindos dos possíveis ataques para a representação do problema de RBC. Para a solução, uma descrição textual de contra medidas é proposta, juntamente com um atributo para expressar o grau de satisfação do usuário com a solução. Os atributos usados pelo autor para a formulação do problema são: o tipo de ataque, hora de ocorrência e duração, tipo de organização, informações do atacante (IP, porta, protocolo), recurso afetado (*host*, sistema operacional, etc.), efeito (perda financeira, perda de publicidade, etc.), estado do ataque (finalizado, acontecendo, etc.) e a resposta ao incidente (fechar conexão e desconectar a rede).

Embora o trabalho apresente uma boa abordagem de resolução do problema o mesmo sugere apenas dois tipos de respostas aos incidentes de segurança, não considerando a grande variedade de incidentes que portanto necessitam de variadas ações de controle.

Em (KIM; IM; PARK, 2010) a metodologia RFM (Recency, Frequency, Monetary) é proposta para a redução de falsos alertas com o uso de RBC. RFM analisa arquivos de *log* levando em consideração a "recência" , frequência e valor, em um processo estatístico levando à detecção de anomalias e mal uso. Posteriormente é aplicado o RBC para encontrar a similaridade de padrões de ataque já conhecidos. Em cada sensor de rede é instalado um agente que é atualizado com base em um agente central. Este agente é responsável por responder à um possível ataque. Cabe ao agente central decidir se deve ou não atualizar os outros agentes com base na detecção de novos ataques. Em relação aos atributos de rede usados pelos autores para a formulação do caso, foram usados: a data de detecção, o IP de origem do ataque, o IP de destino do ataque, o sistema operacional do destino, arquitetura do computador de destino e a porta relacionada ao ataque. O trabalho possui foco na detecção de incidentes e elaboração de respostas técnicas aos eventos como comandos aplicados a *firewalls* e IDS, sem oferecer planos de resposta para o contingenciamento do incidente.

(PING; HAIFENG; GUOQING, 2010) propõem o uso de ontologias e RBC para a construção de um sistema de decisão e resposta à incidentes de segurança. A ontologia é usada para a representação de incidentes. O sistema é alimentado por informações coletadas pelos sensores de forma automática, juntamente com informações inseridas manualmente. Após a extração dos dados é criada a ontologia e então o caso é processado pelo RBC. Os autores partem do pressuposto de que os dados do incidente de segurança já foram coletados e portanto usam apenas o identificador do incidente como entrada para o RBC. Outros atributos usados para a formulação do problema de RBC são: vulnerabilidade do sistema que gerou o incidente, tecnologia usada pelo atacante, ações tomadas para conter o incidente e momento de acontecimento do incidente. A proposição de ontologias permite uma boa organização hierárquica dos tipos de ataques existentes, porém o artigo não afere a qualidade da solução proposta.

No trabalho de (CAPUZZI; SPALAZZI; PAGLIARECCI, 2006) é proposto um sistema de suporte à respostas de incidentes. O sistema chamado IRSS foi desenvolvido com o uso de RBC. O sistema classifica novos ataques baseando-se na informação de ataques que aconteceram no passado visando uma melhora na segurança da rede. O sistema armazena na base de casos, pares de incidentes de segurança passados e a resposta para o incidente. Cada ataque é

representado por uma sequência de eventos e cada resposta é constituída por um conjunto de ações parcialmente ordenadas. A captura dos dados se dá por meio de análise de correlação de arquivos de *log* de sistemas operacionais. Para cada sequência de eventos correlacionados, é calculada a entropia da sequência de eventos, onde apenas as sequências com entropia superior a um determinado limiar são consideradas ataques. Estes ataques são então comparados com os ataques previamente armazenados na base de casos, reusando a resposta do ataque passado para solucionar o novo ataque. Embora este trabalho leve em consideração a produção de respostas aos incidentes, o mesmo encontra-se mais focado na detecção dos incidentes com o uso de RBC do que no desenvolvimento de uma ferramenta que apoie a decisão de uma equipe de resposta e tratamento de incidentes.

3.4 CONSIDERAÇÕES PARCIAIS

Este Capítulo apresentou os trabalhos que foram incluídos nesta pesquisa, de acordo com a revisão sistemática desenvolvida. A resolução de incidentes de segurança possui diferentes abordagens as quais foram aqui demonstradas. Alguns deles possuem um foco mais direcionado à utilização de diretrizes e boas práticas, e outros um foco mais prático, o que inclui o desenvolvimento de ferramentas. É válido destacar a importância dada pela grande maioria dos trabalhos às lições aprendidas, as quais são fundamentais para a resolução de incidentes, uma vez que são fonte de conhecimento, que conforme foi demonstrado na Seção 2.1, é um ativo fundamental no que diz respeito à competitividade no cenário atual.

Embora a maioria dos trabalhos destaquem a importância da utilização das lições aprendidas, apenas alguns trabalhos tratam como realizar gestão deste conhecimento de forma prática. Dentre estes, dois utilizam *frameworks* que apesar de coletarem informações, não as utilizam para apoiar a resolução de novos incidentes. Outros quatro utilizam-se de RBC para a gestão do conhecimento. Porém, eles possuem um viés diferente do apresentado neste trabalho, que é o desenvolvimento de uma metodologia que possibilite a retenção do conhecimento do especialista na resolução de incidentes de segurança. Desta forma, este trabalho se difere dos demais por ter foco na retenção do conhecimento do especialista de segurança, oferecendo uma metodologia que possibilite a elaboração de planos de tratamento de incidentes utilizando para isso RBC, ponderação de atributos e um protocolo padrão para comunicação entre sistemas de IRS.

A Tabela 1 demonstra de modo comparativo as características dos trabalhos relaciona-

dos que utilizam abordagem semelhante, no que diz respeito às contribuições deste trabalho. Desta forma os trabalhos com viés organizacional e que compreendem o uso de *frameworks* não foram incluídos nesta tabela, pois os mesmo não utilizam-se de ponderação de atributos, geração automatizada de planos de tratamento, e não utilizam-se de um protocolo de comunicação específico. Desta forma foram incluídos nesta tabela apenas os trabalhos que utilizam-se de RBC.

É possível identificar na Tabela 1 que a ponderação de atributos é explorada apenas por um dos trabalhos. No que diz respeito a geração automatizada de planos de tratamento percebe-se que, embora alguns trabalhos abordem o assunto, a criação destes é explorado de forma muito sutil, não levando em consideração a importância deste na contenção de incidentes. Já em relação a utilização de protocolos padrão para a comunicação entre CSIRT, percebe-se que isto não é explorado em nenhum destes trabalhos, apesar de ser um protocolo padrão para esta finalidade.

Tabela 1 – Tabela comparativa entre trabalhos incluídos que utilizam a técnica de RBC.

Trabalho	**Ponderação dos atributos**	**Geração automatizada de planos de tratamento**	**Protocolo de dados padrão**
JIANG et al., 2014.	Não menciona o uso de ponderação de atributos.	Apesar de usar lógica descritiva para elaborar um modelo de resposta automatizada, não foca na elaboração de planos de resposta.	Não menciona a utilização de protocolos padrão.
KIM; IM; PARK, 2010.	Utiliza ponderação com pesos definidos por especialista.	Apesar de oferecer respostas "colaborativas", não foca na elaboração dos planos de resposta.	Não menciona a utilização de protocolos padrão.
PING; HAIFENG; GUOQING, 2010.	Não menciona o uso de ponderação de atributos.	Apresenta apenas algumas ideias de planos de resposta, porém não há validação da ideia.	Não menciona a utilização de protocolos padrão.
CAPUZZI; SPALAZZI; PAGLIARECCI, 2006.	Não menciona o uso de ponderação de atributos.	Gera um *script* de resposta o qual deve ser validado pelo especialista.	Não menciona a utilização de protocolos padrão.

Fonte: Autoria própria.

4 RACIOCÍNIO BASEADO EM CASOS COMO UMA TÉCNICA PARA GESTÃO DO CONHECIMENTO DA RESOLUÇÃO DE INCIDENTES DE SEGURANÇA

Este capítulo descreve a construção de um modelo para que o conhecimento do especialista na resolução de incidentes de segurança computacionais possa ser armazenado e reutilizado para o tratamento de novos incidentes. O conhecimento do especialista é retido em uma base de conhecimento, a qual utiliza-se da técnica de Raciocínio Baseado em Casos para automatizar recomendações de planos de respostas a novos incidentes. A metodologia objetiva que as organizações passem a ser detentoras do conhecimento gerado por seus especialistas, diminuindo a dependência que as mesmas têm de seus funcionários experientes para a resolução de problemas de segurança. Além da retenção do conhecimento, a metodologia proporciona a reutilização do conhecimento retido para sugerir a solução de novos problemas de segurança.

A Seção 4.1 apresenta a proposição do uso de RBC para a criação de uma memória relativa a resolução de incidentes de segurança computacionais. A Seção 4.2 detalha como é realizada a modelagem de dados provenientes dos incidentes para uma base de casos, levando em consideração a escolha de atributos para a representação do incidente e o mapeamento dos mesmos para o padrão IODEF. A Seção 4.3 demonstra como é estruturada a parte de respostas aos incidentes, o que inclui gerar um Plano de Tratamento para os mesmos. Por fim, na Seção 4.4 são apresentadas as considerações parciais.

4.1 PROPOSTA

No cenário atual, praticamente todas as empresas estão conectadas à Internet, e consequentemente estão vulneráveis à incidentes de segurança computacionais. Desta forma, o tratamento destes incidentes deve receber atenção adequada por parte das organizações, pois representam uma ameaça importante. O prejuízo causado por incidentes deste tipo podem incluir danos à sua reputação e finanças. Deste modo, as empresas devem, além de mitigar estes incidentes, armazenar as lições aprendidas com os mesmos, facilitando o tratamento de novos incidentes que ocorram no futuro.

O conhecimento gerado pelo especialista ao resolver um incidente pode ser retido e posteriormente utilizado para tratar incidentes semelhantes. Assim, o incidente pode ser resolvido mais rapidamente, beneficiando a empresa e seus funcionários com este conhecimento armaze-

nado. A técnica de Raciocínio Baseado em Casos é uma técnica de gestão do conhecimento. Esta técnica funciona como um *framework* para aquisição e reuso deste conhecimento. Assim, as informações relativas a resolução de um incidente de segurança podem ser armazenados como lições aprendidas e posteriormente manipulados com auxílio do RBC para recomendar soluções para novos incidentes.

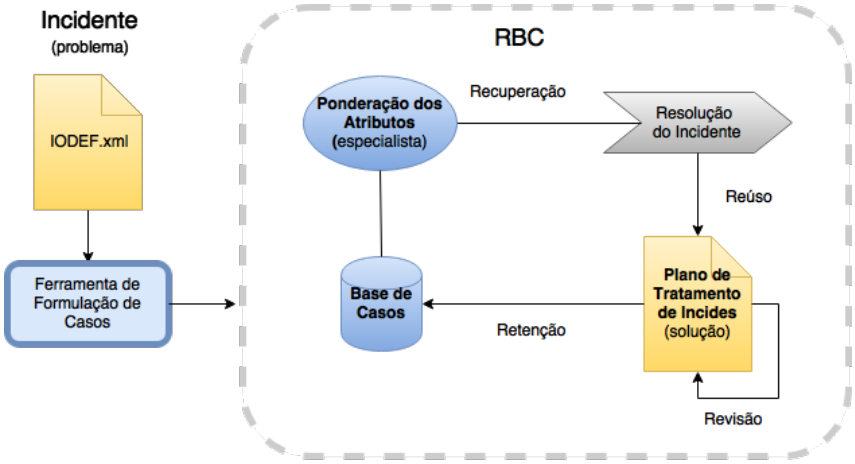
Diante disso, a ideia central deste trabalho é o desenvolvimento de uma memória de resolução de incidentes de segurança com a utilização de RBC com atributos ponderados e padronização de dados. Na metodologia proposta, inicialmente cada incidente de segurança é transformado em um *caso* que é inserido em uma base de conhecimento denominada *base de casos*. Os incidentes são representados no padrão IODEF, o que mantém a metodologia em conformidade com os esforços para melhora de capacidades operacionais para CSIRTs (DANYLIW; MEIJER; DEMCHENKO, 2007).

Uma *ferramenta de formulação de casos* auxilia a transformação de um novo incidente de segurança em um caso, bem como no correto preenchimento dos atributos advindos de uma representação de incidente gerada automaticamente ou manualmente. Incidentes podem também ser gerados por terceiros. Quando recebidos de terceiros ou gerados automaticamente as representações em IODEF muitas vezes apresentam informações incompletas ou ambíguas, podendo sofrer ajustes manuais por especialistas de segurança. *Logs* recebidos juntamente com os incidentes podem assim ser também utilizados para a extração de informações que permitem complementar os dados do incidente.

A Figura 3 ilustra a arquitetura funcional para implantação da metodologia proposta. No passo inicial, incidentes representados em IODEF são gerados ou recebidos pela equipe responsável. A equipe pode então fazer uso da ferramenta de formulação de casos para revisar ou preencher informações faltantes. A ferramenta transforma o incidente em um caso. O uso da ferramenta não é obrigatório, podendo o incidente ser automaticamente assumido como um novo caso. Salienta-se que o novo caso gerado a partir do incidente ainda não possui solução. O RBC é então utilizado para pesquisar a base de casos por problemas similares ao problema atual. Como resultado da aplicação do RBC, são recomendados um ou mais planos de tratamento de incidentes para o novo incidente. Pode-se utilizar a solução recomendada ou adaptá-la para que a mesma reflita as particularidades do problema em questão (incidente relatado). Após utilizado o(s) plano(s) sugerido(s), o novo caso é armazenado na base de casos, retendo o conhecimento/experiência do especialista e gerando aprendizado ao sistema. Assim, quando um

novo incidente surgir, a recomendação de um plano é realizado de forma automatizada, isto é, o RBC irá resgatar os planos que e sugerir aos especialista uma ou mais soluções.

Figura 3 – Arquitetura funcional para implantação da metodologia proposta.



Fonte: Autoria própria.

4.2 MODELAGEM DE DADOS PARA A BASE DE CASOS

A flexibilidade proporcionada pela adoção do padrão IODEF na descrição de incidentes faz com que em alguns casos os documentos relatando incidentes sejam preenchidas de forma incorreta, como é o caso de informações que possuem campos específicos para preenchimento no IODEF mas são descritos em campos de dados adicionais. Logo, para que um incidente seja inserido na base de casos o mesmo deve passar por uma etapa de verificação/modelagem.

Uma vez que o incidente esteja adequadamente modelado pelo especialista de segurança, tem-se o elemento "problema" de um caso. Num sistema de RBC, um caso é composto por um problema a ser resolvido e sua solução. No escopo deste trabalho, o problema a ser resolvido é o incidente de segurança gerado e a solução é um plano de tratamento para este incidente.

No *caso*, a representação do problema corresponde ao *conjunto de atributos do incidente* e a representação da solução corresponde a uma *sequência de passos do plano de tratamento* elaborada para a contenção do incidente. Note que esta relação problema/solução está inicialmente retida nos especialistas, mas pode, a partir da metodologia proposta, ficar retida no sistema computacional da organização. Deste modo, uma parte importante deste trabalho é a seleção e proposição de um conjunto de atributos para descrição dos incidentes de segurança.

4.2.1 Representatividade dos atributos

As diferentes características contidas em incidentes de segurança, as quais fazem com que seja possível a diferenciação entre eles, podem ser representadas por atributos. Para isso, faz-se necessário o mapeamento dos mesmos para a metodologia utilizada pelo RBC. Nele, o conhecimento retido é representado em forma de casos. Portanto, com a utilização deste paradigma, cada incidente deve ser representado por um caso, o qual também possuirá os seus atributos. Alguns destes atributos são mais importantes que outros para apontar uma possível similaridade entre dois casos.

Em RBC, na etapa de recuperação, estes atributos podem ser ou não indexados. Os atributos indexados são aqueles utilizados para a recuperação de casos semelhantes, pois são preditivos para encontrar a solução para um caso (incidente). Já os não indexados não são utilizados para a recuperação por não serem preditivos, porém podem conter informações úteis quando o incidente é recuperado. Desta forma, um atributo como a descrição textual extensa de um evento pode não ser útil para a indexação, já que muito dificilmente será encontrado na base de casos um texto semelhante. Segundo (RICHTER; WEBER, 2013), índices devem ser preditivos e discriminatórios. Assim, cabe ao especialista avaliar e decidir o que será ou não indexado.

Deste modo, neste trabalho foram selecionados alguns atributos para que fosse possível a representação das informações contidas nos incidentes de segurança. Lembrando que os atributos podem ser ou não incluídos como índices nos processos de recuperação à critério do especialista.

Previamente à seleção dos atributos, foram identificados alguns tipos de incidentes mais comuns, visando posteriormente elencar os atributos necessários para a representação dos mesmos. Assim, a partir desta identificação elaborou-se a seguinte lista de tipos de incidentes:

a) Bot: o incidente do tipo Bot (abreviatura de *robot* - robô em inglês) é aquele no qual um ativo da organização passa a fazer parte de uma rede de computadores "zumbi" , na qual os computadores integrantes são recrutados e controlados por um hacker (*botmaster*);

b) DoS: o ataque de negação de serviço é geralmente efetuado contra um servidor *Web* onde interrompe-se um recurso tornando-o inacessível aos seus utilizadores. Ele pode ser centralizado ou distribuído (DDoS);

c) $Proxy$: este é um incidente no qual o servidor *proxy* é infectado com o intuito de oferecer anonimato aos hackers que se utilizam do mesmo para cometer outros ataques;

d) URL Maliciosa: incidentes deste tipo dizem respeito a computadores que estão armazenando arquivos maliciosos que podem ser acessados por uma URL;

e) $Copyright$: neste tipo de incidente um *host* compartilha ou recebe material protegido por direitos autorais;

f) $Spam$: este incidente se caracteriza pelo envio de mensagens não solicitadas de um *host* a outros usuários;

g) $Scan$: neste evento, um *host* escaneia portas de outros *hosts* à procura de vulnerabilidades que possam facilitar um ataque;

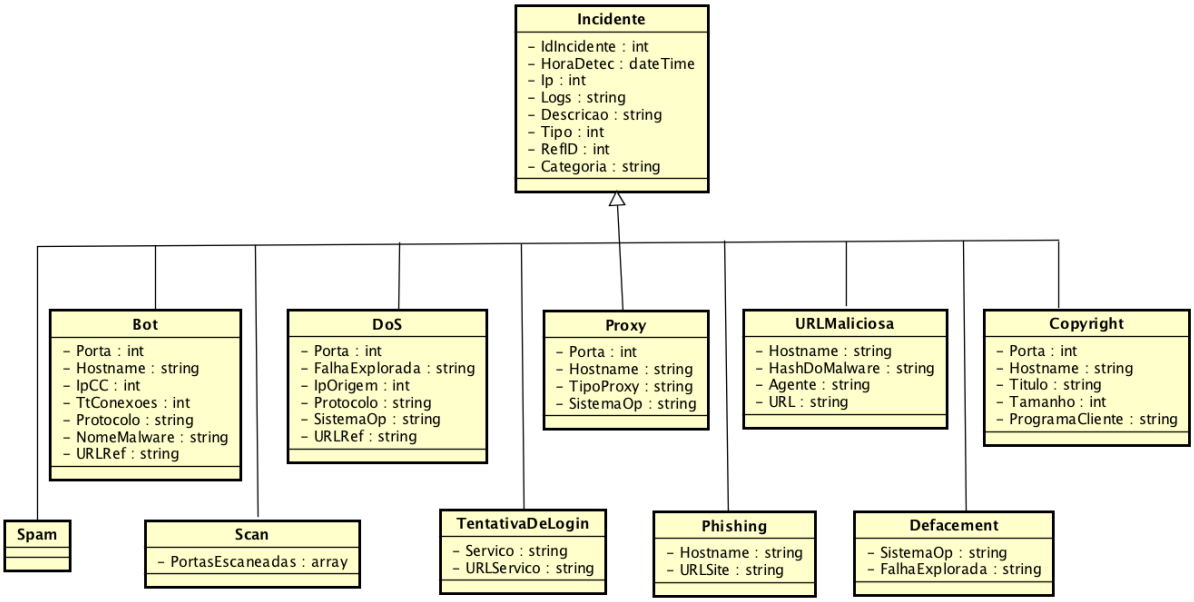
h) Tentativa de Login: neste incidente são geradas tentativas de login por "força bruta" em uma conta de um serviço na tentativa de ganho de acesso indevido;

i) $Phishing$: esta é uma tentativa de ludibriar usuários legítimos utilizando uma página falsa semelhante a uma página verdadeira;

j) $Defacement$: o incidente $Defacement$ resume-se a uma modificação de conteúdo de um site legítimo sem autorização.

Após esta categorização prévia de alguns tipos comuns incidentes, foi realizada a seleção de atributos. Inicialmente, foram selecionados para a representação de um incidente, atributos presentes nos trabalhos de (CAPUZZI; SPALAZZI; PAGLIARECCI, 2006), (KIM; IM; PARK, 2010), (PING; HAIFENG; GUOQING, 2010) e (JIANG et al., 2014), sendo que foram selecionados atributos os quais eram comuns às quatro abordagens. Posteriormente avaliou-se se estes atributos estavam de acordo com os que estavam presentes nos casos reportados pelo Centro de Atendimento a Incidentes de Segurança - CAIS/RNP, isto é, se os atributos previamente selecionados compreendiam uma situação real do mundo corporativo. Então estes atributos foram reanalisados para refletir a aplicação da metodologia aos incidentes provenientes do CAIS/RNP. Após estas etapas, foram selecionados então os atributos que fazem parte deste modelo, conforme ilustra a Figura 4. Nesta Figura, a classe principal $Incidente$, possui os atributos comuns a todos os incidentes. As outras classes são classes agregadas a classe $Incidente$ as quais possuem os atributos específicos para cada tipo de incidente.

Figura 4 – Conjunto dos tipos de incidentes identificados e seus atributos.



Fonte: Autoria própria.

No modelo proposto, diferentes tipos de incidentes possuem alguns atributos específicos e outros que são compartilhados entre eles. O conjunto padrão de atributos de um *problema*, presente em todos os incidentes corresponde ao: identificador do incidente ($IdIncidente$), tipo de incidente ($Tipo$), descrição do mesmo ($Descricao$), dia e hora da detecção ($HoraDetec$), endereço IP do *host* comprometido (Ip), *logs* do incidente ($Logs$), um campo para indicar o papel do *host* (origem, destino, etc.) na hora do incidente ($Categoria$) e um identificador para a correlação de incidentes ($RefID$), para casos como ataques de negação de serviço distribuído, em que mais de um *host* efetua o ataque. A este conjunto padrão podem ou não ser agregados novos atributos, dependendo do interesse do especialista em segurança. Por exemplo, um incidente do tipo $Spam$ pode possuir apenas os atributos do conjunto padrão. Os outros tipos de incidentes podem possuir outros atributos de interesse.

Os outros atributos que podem estar presentes nos incidentes são: Porta de Origem ($Porta$), nome do *host* ($Hostname$), endereço IP do atacante da *botnet* ($IpCC$), total de conexões efetuadas pelo atacante ($TtConexoes$), protocolo pelo qual foi realizado o ataque ($Protocolo$), nome do *malware* que infectou o *host* ($NomeMalware$), falha explorada no ataque ($FalhaExplorada$), endereço IP de onde o ataque foi originado ($IpOrigem$), sistema operacional do *host* em questão ($SistemaOp$), tipo de configuração do $Proxy$ utilizada ($TipoProxy$), código criptográfico MD5 gerado sobre o $malware$ em questão ($HashDoMalware$), aplica-

ção utilizada para a troca de informações entre o *host* e o servidor responsável por receber estas informações ($Agente$), a URL de referência do incidente ($URLReferencia$, $URLMaliciosa$, $URLSite$), título e tamanho do arquivo com direitos autorais ($Titulo$, $Tamanho$), programa utilizado para compartilhamento de arquivo com direitos autorais ($ProgramaCliente$), portas que foram escaneadas ($PortasEscaneadas$), serviço utilizado para tentativa de login ($Servico$) e falha explorada na intrusão ($FalhaExplorada$).

Conforme (RICHTER; WEBER, 2013) os atributos do *caso* podem ser variáveis de acordo com a necessidade do especialista. Desta forma, de acordo com o modelo apresentado (vide Figura 9) o preenchimento destes atributos é personalizado para cada tipo de incidente reportado. Se o incidente for do tipo Bot, por exemplo, o campo destinado ao preenchimento do IP do *Command and Control* deve ser preenchido. Porém, se o incidente for do tipo Violação de Direitos Autorais ($Copyright$), o campo $Tamanho$ que descreve o tamanho do arquivo ilegalmente compartilhado deve ser preenchido. Em geral, a ideia central é armazenar de forma padronizada a maior quantidade de dados e informações destes incidentes, construindo um modelo de casos compreensivo que possa ser utilizado na identificação e solução de diferentes tipos de problemas de segurança.

4.2.2 Mapeamento do modelo para o padrão IODEF

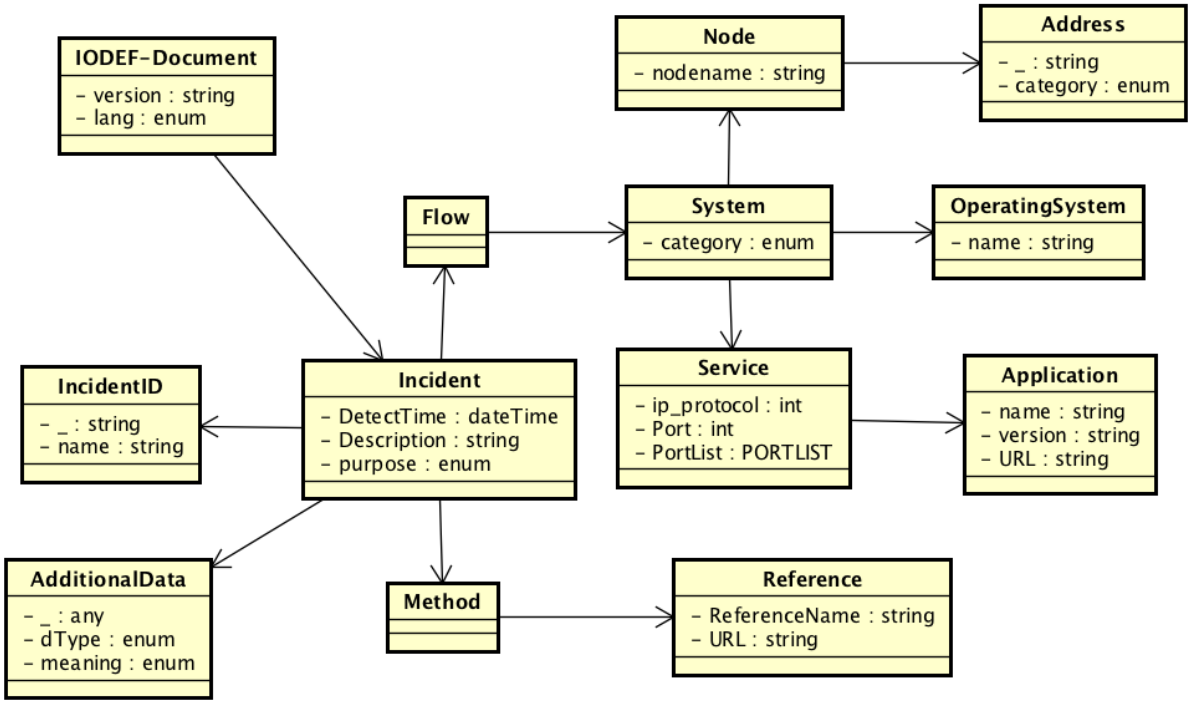
Após a seleção inicial de atributos, o modelo criado necessita ser mapeado para o padrão IODEF. Cada atributo do modelo foi mapeado para sua respectiva representação no padrão. A figura 5 ilustra o padrão IODEF adaptado ao modelo proposto. O IODEF fornece a representação para alguns atributos em classes específicas do modelo, e uma classe denominada $AdditionalData$, a qual pode ser utilizada para a representação de outras informações. Ainda, o IODEF obriga a criação de algumas classes e atributos os quais foram incorporados ao modelo. Assim, as classes do modelo, atributos e respectiva representação dos atributos do modelo são apresentados a seguir:

a) Classe IODEF-Document:

   A classe $IODEF - Document$ é a classe raiz do modelo, sendo todos os documentos IODEF uma instância desta classe. Ela possuí como atributos obrigatórios: $version$ e $lang$. O atributo $version$ serve para a especificação do número da versão do documento IODEF sendo o tipo do atributo $string$ e valor obrigatoriamente "1.00". Já o atributo $lang$ especifica o código da linguagem do documento a qual consta no RFC4646 (PHILLIPS; DAVIS, 2006).

Esta classe ainda possui a classe agregada $Incident$ que expressa informações relacionadas a um incidente;

Figura 5 – Padrão IODEF adaptado ao modelo proposto.



Fonte: Autoria própria.

b) Classe Incident:

A classe $Incident$ é utilizada para a representação de um incidente fornecendo uma descrição padronizada para dados de incidentes comumente compartilhados. A classe agregada $DetectTime$ é utilizada para expressar o momento no qual o incidente foi reportado, sendo correspondente ao atributo $HoraDetec$ do modelo. A classe agregada $Description$ é utilizada para a descrição textual sobre o incidente, sendo a mesma utilizada para expressar o atributo $Descricao$ do modelo. O atributo obrigatório $purpose$ é utilizado para expressar o propósito pelo qual o documento IODEF foi criado ($traceback$, $mitigation$, $reporting$, $other$);

c) Classe Flow:

A classe $Flow$ agrupa *hosts* de origem e destino relacionados. Ela não possui atributos, apenas a classe agregada $System$;

d) Classe System:

A classe $System$ descreve um sistema ou rede envolvidas em um evento. Ela possui o atributo obrigatório $category$ que é utilizado para expressar o papel que o *host* teve no incidente ($source$, $target$, $intermediate$, etc.). Este atributo corresponde ao atributo $Categoria$ do modelo;

e) Classe Node:

A classe $Node$ do IODEF foi criada para nomear um ativo de rede ou uma rede. Ela possuí o atributo $NodeName$ que é utilizado para expressar o atributo $Hostname$ do modelo;

f) Classe Address:

A classe $Address$ representa o endereço de um ativo de rede. Ela é utilizada para expressar o endereço IP da classe $Incidente$ do modelo. Ela possui ainda o atributo obrigatório $category$ que é utilizado para definir o tipo de endereço ($ipv4$ e $ipv6$).

g) Classe OperatingSystem:

A classe $OperatingSystem$ descreve o sistema operacional do ativo envolvido no incidente. O atributo $name$ é utilizado para expressar o atributo $SistemaOperacional$ do modelo;

h) Classe Method:

A classe $Method$ descreve a metodologia utilizada pelo invasor para desenvolver o ataque. Ela não possui atributos obrigatórios, apenas a classe agregada $Reference$;

i) Classe Reference:

A classe $Reference$ é utilizada para referenciar vulnerabilidades, alertas de IDS, dados sobre *malwares*, etc. São utilizadas duas classes agregadas a esta: $ReferenceName$ e URL. $ReferenceName$ é utilizada para expressar os atributos do modelo $NomeMalware$ e $FalhaExplorada$ das classes Bot e DoS respectivamente. O atributo URL permite que seja adicionada um link para esta referência, sendo a mesma utilizada para expressar os atributos do modelo $URLRef$. Este atributo não é obrigatório no padrão IODEF, porém observou-se que o CSIRT estudado referenciava na descrição dos eventos uma URL relativa a *malwares* e falhas exploradas. Desta modo, tais referências foram adicionadas ao modelo;

j) Classe Service:

A classe $Service$ é utilizada para descrever um serviço de um *host* ou rede. Ela possui as classes agregadas $Port$, $PortList$ que foram utilizadas para mapear os atributos $Porta$

e $PortasEscaneadas$. A classe $Port$ descreve a porta do serviço e a classe $PortList$ descreve um conjunto de portas. Esta classe ainda possui o atributo obrigatório $ip-protocol$ que é utilizado para expressar o número do protocolo IANA (*Internet Assigned Numbers Authority*) os quais são definidos nas RFC 5237 (ARKKO; BRADNER, 2008) e RFC 7045 (CARPENTER; JIANG, 2013);

k) Classe Application:

A classe $Application$ é utilizada para descrever uma aplicação que é executada por um sistema ($SystemClass$) que provê um serviço ($ServiceClass$). A única classe agregada a esta é a URL. Ela é utilizada para representar os atributos URL, $URLServico$ e $URLSite$ presentes respectivamente nas classes $URLMaliciosa$, $TentativaDeLogin$, $Phishing$ do modelo. Ela também possui alguns atributos não obrigatórios, dentre eles o atributo $name$. Ele é utilizado para representar os atributos $Servico$ e $ProgramaCliente$ das classes $TentativaDeLogin$ e $Copyright$;

l) Classe AdditionalData:

A classe $AdditionalData$ serve para a extensão do modelo de dados do IODEF. Ela é utilizada para representação do restante dos atributos $Logs$, $HashDoMalware$, $Agente$, $Titulo$, $Tamanho$, $IpCC$, $IpOrigem$, $TtConexoes$, $TipoProxy$. Ela possui alguns atributos, dentre eles $meaning$ e $dType$. O atributo $meaning$ serve para descrever o conteúdo do elemento, neste caso, o nome de algum dos atributos do modelo representados na classe $AdditionalData$. O atributo $dType$ é utilizado para representar o tipo de dado que o atributo do modelo possui (int, $string$, $boolean$, etc.).

A figura 6 exemplifica a representação XML do documento IODEF adaptado, onde as *tags* representam as classes e seus atributos. O documento na linha 2 apresenta a definição da classe principal $IODEF\text{-}Document$. A *tag* $Incident$ é a classe que define o incidente, sendo que as outras classes subsequentes são todas classes agregadas a esta. O documento segue com a definição destas classes, sendo que na linha 29 é definida a classe $AdditionalData$, na qual o atributo $meaning$ define o tipo de informação que será representado por esta classe.

Figura 6 – Exemplo de representação XML do padrão IODEF adaptado.

```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<IODEF-Document lang="en" version="1.00" xmlns="urn:ietf:params:xml:ns:iodef-1.0" xmlns:iodef="
urn:ietf:params:xml:ns:iodef-1.0" xmlns:iodef-sci="urn:ietf:params:xml:ns:iodef-sci-1.0" xmlns:xsi="http://www.w3.
org/2001/XMLSchema-instance">
  <Incident purpose="reporting">
    <IncidentID name="ufsm">123456</IncidentID>
    <DetectTime>2017-08-31T17:34:15-03:00</DetectTime>
    <Description>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus aliquam condimentum nisl eget
    rhoncus. Nunc convallis ut libero accumsan hendrerit. Nunc laoreet eros eleifend, rutrum sapien in, finibus dolor.
    Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Donec mauris massa,
    tempor ac diam tempor, lacinia laoreet dui. Curabitur sollicitudin sit amet nulla ac congue. Aliquam ac odio a
    velit ullamcorper vehicula. Donec nec sollicitudin metus. Proin pellentesque blandit est, eu hendrerit ante
    fermentum vel. Quisque id enim sit amet eros convallis lacinia.
    </Description>
    <Method>
      <Reference>
        <ReferenceName>Vestibulum ante ipsum</ReferenceName>
        <RefURL>http://www.vestibulum.com</RefURL>
      </Reference>
    </Method>
    <Flow>
      <System category="source">
        <OperatingSystem name="pellentesque"/>
        <Node nodename="pellentesque">
          <Address category="ipv4-addr">0.0.0.0</Address>
        </Node>
        <Service ip_protocol="0">
          <Port>0</Port>
          <PortList>0,1,1-12</PortList>
          <Application name="blandit" version="1.2">
            <AppURL>http://www.blandit.com</AppURL>
          </Application>
        </Service>
      </System>
    </Flow>
    <AdditionalData dtype="string" meaning="IpCC">0.0.0.0</AdditionalData>
  </Incident>
</IODEF-Document>
```

Fonte: Autoria própria.

4.3 RESOLUÇÃO DE INCIDENTES DE SEGURANÇA

Após modelagem do caso, que é feita utilizando-se as informações presentes no incidente reportado, é realizada a resolução do incidente de segurança. Neste estágio, um novo caso representa um incidente que ainda não possui solução. Para que seja sugerida uma solução para este novo problema, é realizada a pesquisa na base de casos por casos mais similares.

Esta seção detalha como é tratada a ponderação dos atributos (Seção 4.3.1) e a montagem e recuperação dos planos de tratamento dos incidentes (Seção 4.3.2).

4.3.1 Ponderação dos Atributos

Dado um novo incidente ainda não resolvido, o objetivo da metodologia é resgatar um conjunto de incidentes (casos) da base de casos considerados os mais similares para dar suporte à decisão dos profissionais de segurança na resolução deste novo incidente.

De acordo com (RICHTER; WEBER, 2013), dois problemas são considerados simila-

res se eles possuem soluções similares. Essa pesquisa segue um processo de recuperação dos casos mais similares ao problema atual para que seja possível oferecer sugestões de planos de tratamento para este novo incidente. O plano de tratamento é um documento composto por uma sequência de passos ordenados os quais representam a solução para o problema. Dado um par de incidentes de segurança a e b, no RBC a similaridade entre os incidentes é definida pelo cálculo da distância entre dois conjuntos de atributos que representam os incidentes, conforme ilustra a Equação (4.1). A função de similaridade indica um valor entre 0 e 1, de acordo com o menor ou maior grau de similaridade, respectivamente.

$$sim(a, b) \rightarrow [0, 1]. \tag{4.1}$$

Assim, quando iniciada a resolução de um novo incidente é calculada a distância entre este incidente e os incidentes armazenados na base de casos, buscando, dado um limiar mínimo de similaridade, os incidentes com mais semelhança ao novo incidente. Desta forma a equipe responsável, ou um novo profissional de segurança, podem rapidamente analisar a solução dada ao caso mais semelhante recuperado e usar ou adaptar o plano de tratamento ao incidente proposto para o incidente recém recebido. Ao aplicar a solução reutilizada, o especialista então pode analisar se o incidente foi corretamente solucionado. Após este processo, esta nova experiência de solução de problemas pode ser armazenada na base de casos com suas possíveis adaptações, gerando aprendizado ao sistema.

O limiar de similaridade é tido como o valor mínimo de similaridade, o qual dois incidentes devem possuir para que sejam considerados similares. Desta forma, pode-se ajustar o limiar para que sejam recuperados apenas incidentes que tenham semelhança mínima de certa porcentagem em relação ao incidente em questão. Para que seja possível determinar o limiar de similaridade ideal faz-se necessário o desenvolvimento de experimentos para o cálculo da precisão do sistema com validação cruzada, o qual indica para cada valor de limiar de similaridade o valor da precisão do sistema.

Como visto na Seção 2.2, a recuperação dos casos é realizada primeiramente verificando-se a similaridade entre os casos e posteriormente calculando-se a distância entre eles.

Dados dois casos a e b, a comparação de similaridade é realizada avaliando-se os n pares de atributos a_i e b_i dos casos individualmente, utilizando um peso W para dar maior relevância ao atributo, conforme a Equação (4.2). A medida sim é a comparação entre os casos de um ponto de vista global, e sim_i é a comparação de valores de atributos individuais. O resultado da

comparação, que deve ser um valor entre 0 e 1, indicará o quão semelhantes são os casos a e b.

$$sim(a,b) = \sum_{i=1}^{i=n} W_i \times sim_i(a_i, b_i). \tag{4.2}$$

Já o cálculo de distância é realizado da seguinte forma: cada caso é representado por um vetor de n atributos, o que permite a comparação atributo a atributo entre dois casos, medindo-se então a distância entre ambos. Quanto menor a distância, mais similares são os casos. A ponderação de atributos serve para que se possa dar maior importância a determinado atributo no cálculo de similaridade. A cada atributo é dado um peso W o qual influencia no cálculo final da distância. Dados dois casos a e b, onde a é o novo caso, e b o caso recuperado, é realizado o cálculo de Distância Euclidiana Ponderada, conforme Equação (4.3).

$$d(a,b) = \sqrt{\sum_{i=1}^{n} W_i \times (a_i - b_i)^2} \tag{4.3}$$

onde é calculada a raiz quadrada do somatório dos pesos W multiplicados pela diferença quadrada entre os atributos i dos casos a e b.

A atribuição de pesos pode ser local ou global. Local se for aplicado em um pequeno subgrupo de casos que compõe a base de casos, ou global de for aplicado a toda a base ou a uma grande porção dela (ZHANG, 1997) (RICHTER; WEBER, 2013). Na atribuição global, que é a utilizada neste trabalho, faz-se necessário uma análise cuidadosa dos casos presentes na base de caso para que se possa determinar quais atributos possuem uma maior importância para o cálculo de similaridade. Deste modo, os especialistas em segurança irão utilizar-se de seus conhecimentos e experiências para decidir quais atributos são mais importantes, e quais são menos.

Os pesos podem ser atribuídos de forma estática ou dinâmica. São atribuídos de forma dinâmica, quando os pesos variam de acordo com aspectos do contexto, sendo considerado para quando a base de casos é utilizada para diferentes propósitos. Porém, quando a base de casos é utilizada para um propósito único, como é o caso deste trabalho que foi projetado unicamente para auxiliar na resolução de incidentes de segurança, a atribuição de pesos é feita de forma estática, pois os pesos não são alterados de acordo com cada consulta.

Apesar de sua grande importância, a correta atribuição de pesos em RBC ainda é considerado um desafio. Existem alguns métodos manuais e outros automatizados para isso, com a utilização de técnicas de aprendizado de máquina, algorítimos genéticos, mineração de da-

dos, etc. (RICHTER; WEBER, 2013). Uma das técnicas manuais que podem ser utilizadas diz respeito à utilização do aprendizado por reforço (RICHTER; WEBER, 2013). O processo de aprendizado possui basicamente três passos: 1) executar um teste com os pesos para gerar um $feedback$ do sistema; 2) se o resultado foi positivo, aumenta-se o peso; 3) se o resultado for negativo, diminui-se o peso. Deste modo, a cada peso modificado, pode-se testar o sistema e, calculando-se sua precisão, identificar se o peso modificado trouxe melhorias ou não para o processo de recuperação.

Desta forma, no modelo proposto, o conhecimento do especialista em relação a importância de determinado atributo pode ser retido no sistema e utilizado para melhorar o processo de recuperação dos casos, fazendo com que a metodologia proposta reflita o conhecimento do especialista na resolução de incidentes.

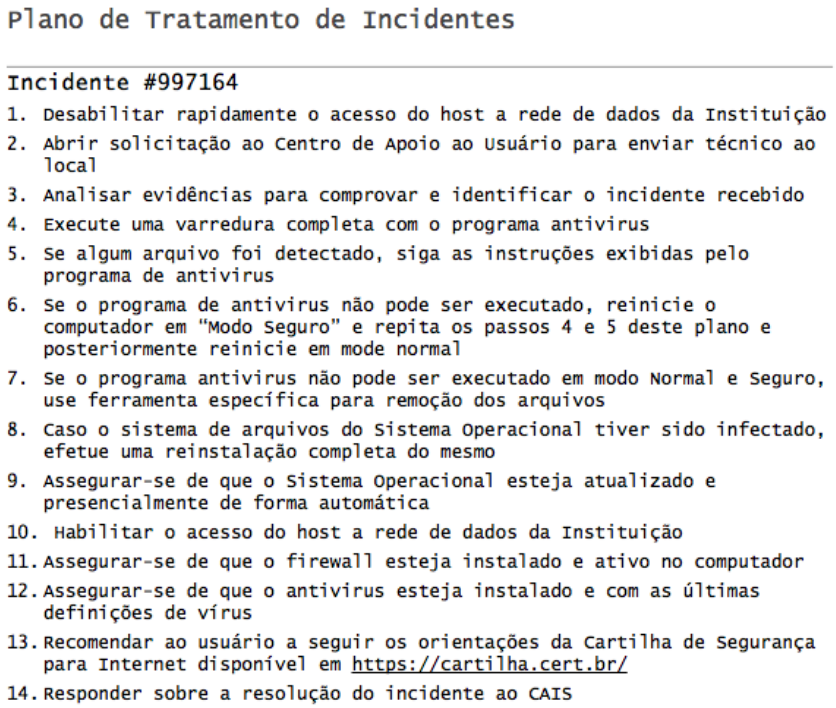
4.3.2 Plano de Tratamento de Incidentes

Ao final de todo o processo de resolução de um incidente, é gerado um documento que corresponde ao plano de tratamento para este incidente. A Figura 7 exemplifica um plano de tratamento de incidentes para um incidente do tipo Bot específico. Ele representa o passo a passo de como contornar o incidente. No início do documento temos o identificador do incidente e logo abaixo os passos recomendados para tratar o incidente (passos 1 a 14).

Este plano é composto por uma sequência de passos ordenados que representam ações que foram tomadas para tratar este incidente. Estas ações ou passos, são armazenadas separadamente em uma biblioteca de ações, para que sejam reusadas no tratamento de incidentes futuros. Logo, o especialista pode utilizar-se de passos previamente criados ou adicionar novos passos ao plano, de acordo com a necessidade de resolução do problema atual. Consequentemente estas ações podem ser utilizadas para tratamento de futuros incidentes. Assim, os casos que já foram solucionados podem compartilhar um ou mais passos, porém com diferentes arranjos entre eles conforme a Figura 8. Esta Figura demonstra, no quadro da esquerda, três casos cujos passos para a solução encontram-se na biblioteca de ações que está representado pelo outro quadro à direita. A biblioteca contém todos os passos que foram utilizados para tratar diferentes incidentes. A biblioteca de ações reflete o conhecimento do especialista no desenvolvimento de passos para resolver os incidentes.

A característica de utilização desta metodologia faz com que quanto mais incidentes acontecerem ao longo do tempo, maior será a quantidade de conhecimento retido e posterior-

Figura 7 – Plano de resposta para o tratamento de um incidente do tipo Bot.



Plano de Tratamento de Incidentes

Incidente #997164

1. Desabilitar rapidamente o acesso do host a rede de dados da Instituição
2. Abrir solicitação ao Centro de Apoio ao Usuário para enviar técnico ao local
3. Analisar evidências para comprovar e identificar o incidente recebido
4. Execute uma varredura completa com o programa antivirus
5. Se algum arquivo foi detectado, siga as instruções exibidas pelo programa de antivirus
6. Se o programa de antivirus não pode ser executado, reinicie o computador em "Modo Seguro" e repita os passos 4 e 5 deste plano e posteriormente reinicie em mode normal
7. Se o programa antivirus não pode ser executado em modo Normal e Seguro, use ferramenta específica para remoção dos arquivos
8. Caso o sistema de arquivos do Sistema Operacional tiver sido infectado, efetue uma reinstalação completa do mesmo
9. Assegurar-se de que o Sistema Operacional esteja atualizado e presencialmente de forma automática
10. Habilitar o acesso do host a rede de dados da Instituição
11. Assegurar-se de que o firewall esteja instalado e ativo no computador
12. Assegurar-se de que o antivirus esteja instalado e com as últimas definições de vírus
13. Recomendar ao usuário a seguir os orientações da Cartilha de Segurança para Internet disponível em https://cartilha.cert.br/
14. Responder sobre a resolução do incidente ao CAIS

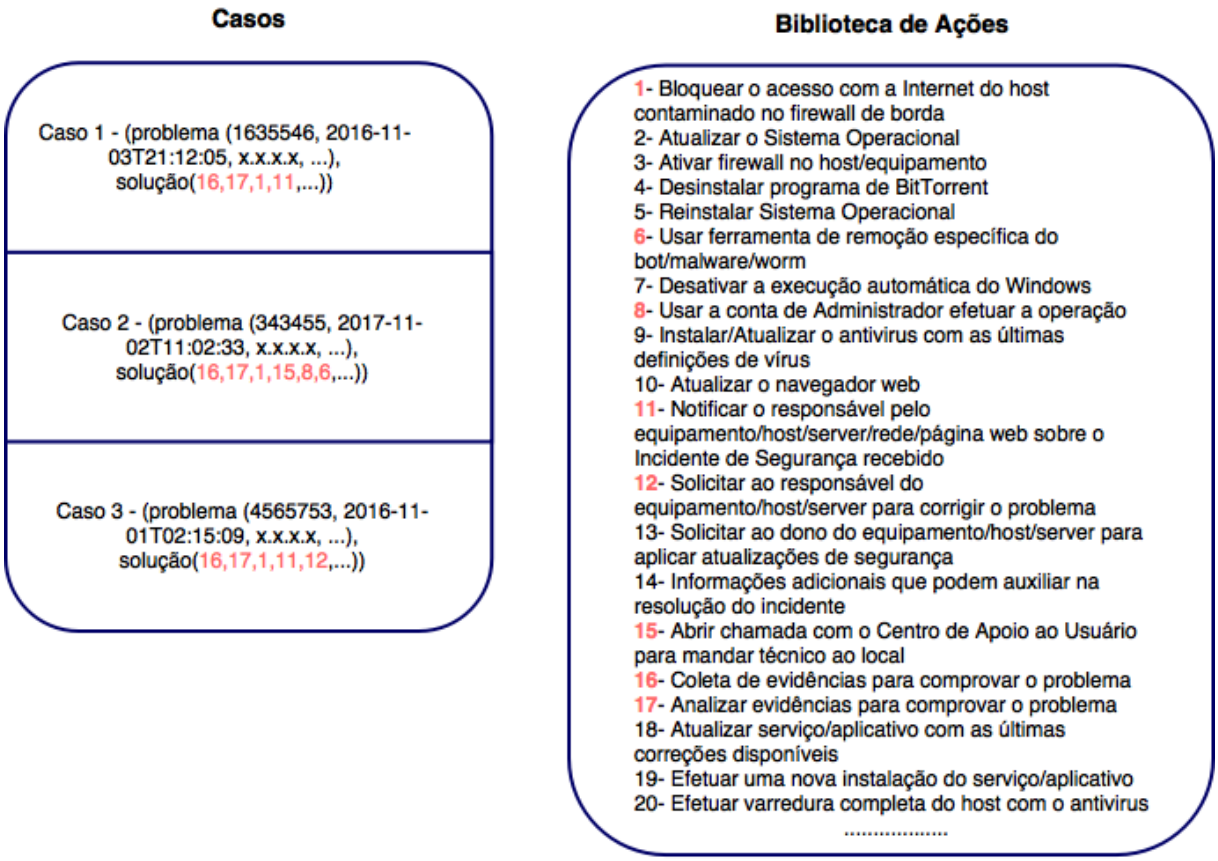
Fonte: Autoria própria.

mente ofertado ao especialista para que o mesmo possa solucionar um problema. Deste modo, principalmente no uso inicial deste método, um incidente novo pode não encontrar um incidente suficientemente semelhante, isto é, não houve ainda nenhum incidente no passado cujo grau de similaridade entre ele e este novo incidente seja suficiente para recomendá-lo como uma solução. Assim, o especialista irá utilizar seu conhecimento tácito para elaborar um plano de tratamento para este incidente, e após o sucesso no tratamento do mesmo, o conhecimento do especialista, que está contido no plano de tratamento deste incidente, será retido.

No entanto, se o incidente a ser tratado possui representatividade na base de casos, o especialista poderá utilizar-se do conhecimento que foi armazenado para o tratamento de um incidente semelhante. O especialista irá então adaptar o plano escolhido dentre os recomendados, para que o mesmo reflita as necessidades de resolução do incidente atual. Para tal, o mesmo pode adicionar e/ou remover um ou mais passos contidos no plano, e então gerar aprendizado ao sistema.

Em ambos os casos citados, quando o especialista monta um plano de tratamento, o mesmo deve escolher os passos que serão usados para mitigar o incidente. Ao adicionar um passo, o especialista pode utilizar-se de algum dos passos já criados para a solução de algum

Figura 8 – Compartilhamento de ações entre incidentes.



Fonte: Autoria própria.

problema anterior, ou criar novos passos que ainda não foram utilizados para conter o incidente.

A Figura 9 demonstra como um caso do tipo $Copyright$ é representado na base de casos. O incidente reportado representa o problema que se deseja resolver, e os passos ordenados, que dão origem ao plano de respostas, representam a solução para este problema. Esta representação possui relação com a apresentada na Figura 8, a qual demonstra o caso (problema e solução) e também a biblioteca de ações na qual os identificadores são utilizados para representar o plano de tratamento. A Figura 6 apresenta também um exemplo de um caso, porém representado com a utilização do padrão IODEF, o qual consiste em um arquivo XML com as informações sobre um incidente.

Figura 9 – Exemplificação de um caso.

PROBLEMA								
IdIncidente	Timestamp	IpDeOrigem	Logs	PortaOrigem	Hostname	Título	Tamanho	ProgramaCliente
1633546	2016-11-03T21:12:05	X.X.X.X	.....	55951	11	Toy Story 3	331098894	1

SOLUÇÃO								
Passo 1	Passo 2	Passo 3	Passo 4	Passo 5	Passo 6	Passo 7	Passo 8	Passo 9
16	17	1	15	33	31	21	22	23

Fonte: Autoria própria.

4.4 CONSIDERAÇÕES PARCIAIS

Este Capítulo apresentou o detalhamento da proposta de um modelo para a gestão do conhecimento gerado através da resolução de incidentes de segurança computacionais. A modelagem de dados faz com que seja possível aplicar a técnica de RBC para auxiliar na resolução de incidentes de segurança computacionais, permitindo uma alocação racional do conhecimento.

A seleção de atributos é parte importante deste processo por possibilitar a identificação das características importantes dos incidentes as quais tornam possível, através de análise de similaridade, apontar semelhanças entre incidentes distintos. Esta seleção de atributos que dá origem à uma representação de dados que é então adaptada ao padrão IODEF. Esta adaptação tem o intuito de possibilitar que o incidente seja expresso em um formato padrão amplamente utilizado por equipes responsáveis pelo tratamento de incidentes, facilitando a troca de informações entre diferentes times.

A importância da ponderação para o cálculo de similaridade foi discutida juntamente com um exemplo de como os pesos podem ser definidos com ajuda do aprendizado por reforço. Foi apresentado também como um incidente novo pode ser resolvido com o auxílio de informações armazenadas na base de casos. Esta resolução utiliza análise de similaridade e ponderação de atributos para sugerir um plano de tratamento para o incidente em questão. Ao resolver um novo incidente, o especialista utiliza-se de seu conhecimento tácito para identificar os passos necessários para mitigar o incidente. Quando o incidente é resolvido, os passos contidos no plano de tratamento são armazenados. Isso gera aprendizado ao sistema, permitindo que este conhecimento seja reutilizado para instruir outros membros da organização a desempenharem tarefas similares.

5 VALIDAÇÃO

Neste capítulo são apresentados e discutidos experimentos realizados para avaliação da metodologia proposta. Eles buscam analisar os efeitos da ponderação de atributos em relação a precisão do sistema e avaliar a retenção do conhecimento do especialista em segurança na resolução dos incidentes de segurança.

Na Seção 5.1 é apresentada a metodologia utilizada nos experimentos. A Seção 5.2 apresenta experimentos relacionados à ponderação dos atributos e a Seção 5.3 apresenta experimentos relacionados à retenção e reúso do conhecimento. Por fim a Seção 5.4 apresenta as considerações parciais deste Capítulo.

5.1 METODOLOGIA

Os incidentes captados para o desenvolvimento deste trabalho tiveram sua origem no setor de segurança de redes do CPD/UFSM. Os incidentes foram enviados pelo CAIS - Centro de Atendimento a Incidentes de Segurança - da RNP ao CPD/UFSM através do Sistema de Gestão de Incidentes de Segurança (SGIS), pois estes incidentes foram originados dentro da UFSM, e portanto s'ao resolvidos pelo CPD desta instituição. Foram utilizados 258 casos advindos de diferentes tipos de incidentes. A acurácia em todos os experimentos foi medida utilizando-se limiares de similaridade (Sim) de 50% à 100% em intervalos de 5%. Foi utilizada a ferramenta FreeCBR para o desenvolvimento de um protótipo visando a validação deste trabalho, sendo o mesmo configurado para o uso do algoritmo *k-Nearest Neighbours* para classificação inicial e distância euclidiana ponderada para o cálculo de similaridade.

A avaliação do método é realizada através do cálculo de precisão do sistema que visa identificar a representatividade dos casos presentes na base. O cálculo é realizado para diferentes valores de limiar de similaridade verificando-se assim para quais valores de similaridade obtém-se uma melhor precisão. Este cálculo é realizado com um grupo de treinamento e outro de testes. Dividi-se aleatoriamente os n casos da base de casos em p partições de tamanho t. A cada rodada uma das p partições assume a posição de grupo de testes enquanto as demais são consideradas parte do grupo de treinamento. Cada um dos casos presentes no grupo de testes tem sua representatividade aferida quando busca-se então, no grupo de treinamento, outros casos semelhantes que possuem um plano de tratamento também semelhante. Cabe ressaltar que

(RICHTER; WEBER, 2013) define que dois problemas são considerados similares se eles possuem soluções similares. Desta forma, quando um incidente encontra um semelhante no grupo de treinamento, testa-se se o plano de tratamento também é semelhante. No caso de os dois incidentes semelhantes possuírem planos semelhantes soma-se um acerto, do contrário, um erro. Calcula-se então ao final de cada rodada a subtração de acertos e erros dividido pelo número total de testes realizados. A precisão do sistema é então calculada pela média dos resultados de todas as rodada de testes.

Foram utilizados nos experimentos dois métodos para a estimativa de precisão: *Leave-one-out Cross Validation* (LOOCV) e *K-Fold Cross Validation*, ambos considerando de um a cinco vizinhos mais próximos. Os métodos de validação cruzada (*Cross-Validation*) são métodos estatísticos para avaliação e comparação de algoritmos de aprendizagem (REFAEILZADEH; TANG; LIU, 2009). Ambos os métodos utilizados são similares, diferindo apenas no número de k partições que serão utilizados para o teste. No *Leave-one-out Cross Validation* retira-se um caso por vez do grupo de testes comparando-o com os do grupo de treinamento, fazendo assim $n - 1$ comparações, sendo então $k = n$. O método *K-Fold Cross Validation* consiste em dividir os dados em k subconjuntos mutuamente exclusivos de mesmo tamanho, e então cada subconjunto é utilizado como conjunto de teste e o restante dos dados como conjunto de treinamento. Assim, este processo é realizado k vezes com alternância circular dos subconjuntos de teste, sendo neste experimento utilizado $k = 10$, pois foi constatado no estudo de (KOHAVI et al., 1995), que a divisão em 10 partições k tende oferecer uma estimativa de acurácia menos tendenciosa do que quando se utiliza outros valores para k.

5.2 PONDERAÇÃO DE ATRIBUTOS

A ponderação de atributos diz respeito ao ajuste que pode ser realizado no cálculo de similaridade. Com ela pode-se dar maior importância a determinados atributos com o intuito de melhorar a precisão do sistema. Este ajuste pode ser realizado por um especialista ou com a utilização de técnicas que visem uma melhora no resultado da precisão do sistema. Deste modo, neste experimento foram realizados duas diferentes avaliações para investigar a influência da ponderação na precisão do sistema. A primeira avaliação foi realizada com todos os atributos dos casos com peso w = 1, ou seja, todos os atributos com a mesma importância para o cálculo. A segunda avaliação foi realizada com ajuste de pesos realizado por um especialista em segurança da informação, o qual ajustou os pesos considerando seu conhecimento empírico em

relação à importância dos atributos para a resolução dos incidentes de segurança.

Ainda, pode-se utilizar diferentes limiares para a similaridade entre soluções, isto é, pode-se definir o percentual de similaridade entre o problema pesquisado e os problemas semelhantes a serem resgatados. Desta forma, quando define-se um limiar de similaridade e o método não retorna nenhum caso semelhante, pode-se diminuir então este percentual com o objetivo de se encontrar casos semelhantes ao caso pesquisado.

Quando os algoritmos de validação LOOCV e K-FOLD executam o cálculo de precisão do sistema, como mencionado anteriormente, são feitas comparações atributo a atributo entre dois casos para que seja aferida a similaridade entre os dois. Se a similaridade é superior a um dado limiar, é então calculada a similaridade entre as soluções destes dois casos. Isso é realizado pelo fato de que dois casos semelhantes devem possuir respostas semelhantes. Assim, pode-se ajustar o grau de similaridade entre as soluções para que dois casos possam ser considerados semelhantes. Neste trabalho foram considerados limiares de solução entre 100% e 70% com vistas a uma melhora da precisão do sistema. Porém, foi constatado que, para a base de casos em questão, houve uma melhora muito discreta em relação a precisão do sistema quando se utilizou diferentes limiares. Desta forma, resolveu-se considerar apenas o limiar de 100%, o que define que dois incidentes são semelhantes apenas se a parte do "problema" possuir similaridade maior ou igual a um determinado limiar (50% a 100%) e possuir a parte de "solução" com limiar de similaridade de exatamente 100% (idêntico).

A utilização de um a cinco vizinhos mais próximos (*k-Nearest Neighbors*) para o cálculo de similaridade, nos permite ter uma ideia de quantas soluções seriam possíveis de serem utilizadas caso a primeira solução não fosse escolhida para sanar o problema. É necessária a avaliação de mais de uma solução pois pode acontecer de a solução recomendada não obter sucesso na resolução do problema, fazendo com que o especialista necessite de mais recomendações. Assim, quando o número de vizinhos está entre 2 e 5, é realizada um média dos acertos obtidos para os vizinhos em questão, deste modo, considerando a qualidade das soluções possíveis de serem selecionadas.

A Tabela 2 demonstra os resultados de precisão quando utilizado o método *K-Fold Cross Validation* sem ponderação de atributos, isto é, quando todos os pesos w dos atributos são ajustados para $w = 1$. O número de partições p utilizados é p = 10, o número de vizinhos k = 5 e o limiar de similaridade (Sim) entre 50% e 100%.

Observa-se que, para os limiares de similaridade compreendidos entre 100% e 75%, não

Tabela 2 – Resultado de precisão do método K-fold para pesos $w = 1$.

k-NN	1	2	3	4	5
Sim (%)	Precisão (%)				
100	NaN	NaN	NaN	NaN	NaN
95	0,00	NaN	NaN	NaN	NaN
90	0,00	0,00	0,00	0,00	0,00
85	0,00	0,00	0,00	0,00	0,00
80	0,00	0,00	0,00	0,00	0,00
75	0,00	0,00	0,00	0,00	0,00
70	50,00	50,00	50,00	50,00	50,00
65	87,50	87,50	83,33	81,25	80,00
60	87,50	84,38	88,89	83,33	80,00
55	82,35	79,41	78,43	73,53	70,59
50	82,35	79,41	78,43	73,53	70,59

Fonte: Autoria própria.

há resultados para os valores de precisão. Portanto, para estes limiares, não há casos na base de casos que possuam um correspondente cujo grau de similaridade entre ambos esteja nestes limiares. Ademais, observa-se que embora os casos em geral possuam similaridade abaixo de 70% entre si, o grau de precisão para limiares de 65% a 50% são considerados satisfatórios. Observa-se também bons resultados quando utiliza-se mais de um vizinho mais próximo para o cálculo.

A Tabela 3 demonstra os resultados de precisão quando utilizado o método *Leave-one-out Cross Validation* sem ponderação de atributos, isto é, quando todos os pesos w dos atributos são ajustados para $w = 1$. O número de partições p utilizados é p = 10, o número de vizinhos k = 5 e o limiar de similaridade (Sim) entre 100% e 50%.

Observa-se que entre 95% e 70% são encontrados poucos casos que satisfazem estes limiares. Observa-se também valores de precisão inferiores aos calculados pelo método K-fold que sofrem um decréscimo acentuado quando avalia-se mais de um vizinho mais próximo.

Tendo sido apresentados os resultados de precisão para quando não utiliza-se ponderação de atributos, com a finalidade de obtenção de uma melhora nos resultados, são apresentados a seguir os valores para quando é realizado o ajuste de pesos pelo especialista, no qual ele pôde dar maior importância aos atributos que o mesmo considerava relevantes.

A Tabela 4 demonstra os resultados de precisão quando utilizado o método *K-Fold Cross Validation* com a ponderação de atributos realizada pelo especialista. O número de partições p utilizados é p = 10, o número de vizinhos k = 5 e o limiar de similaridade (Sim) entre 50% e

Tabela 3 – Resultado de precisão do método LOOCV para pesos $w = 1$.

k-NN	1	2	3	4	5
Sim (%)	Precisão (%)				
100	NaN	NaN	NaN	NaN	NaN
95	66,67	33,33	50,00	0,00	0,00
90	66,67	33,33	33,33	25,00	0,00
85	50,00	33,33	33,33	25,00	20,00
80	50,00	33,33	33,33	25,00	20,00
75	50,00	33,33	33,33	25,00	20,00
70	59,26	63,89	71,11	76,92	75,38
65	78,74	78,93	78,45	76,96	75,83
60	78,18	75,59	74,16	73,90	73,73
55	77,55	75,11	72,82	71,79	71,45
50	75,20	72,11	69,87	68,45	68,52

Fonte: Autoria própria.

100%.

Tabela 4 – Resultado de precisão do método KFOLD para pesos ponderados por especialista.

k-NN	1	2	3	4	5
Sim (%)	Precisão (%)				
100	NaN	NaN	NaN	NaN	NaN
95	93,33	90,00	95,24	91,67	90,00
90	82,35	79,41	83,33	78,57	77,14
85	82,35	79,41	83,33	78,13	75,00
80	82,35	79,41	83,33	78,13	75,00
75	82,35	79,41	78,43	73,53	70,59
70	75,00	70,00	68,33	63,75	61,00
65	75,00	70,00	68,33	63,75	61,00
60	75,00	70,00	68,33	63,75	61,00
55	75,00	70,00	68,33	63,75	61,00
50	75,00	70,00	68,33	63,75	61,00

Fonte: Autoria própria.

Observa-se um aumento substancial na similaridade entre os casos comparando-se com quando não utiliza-se ponderação, chegando a um limiar máximo de 95%. Os valores de precisão mantém-se em um bom nível inclusive para quando utiliza-se para o cálculo mais de um vizinho mais próximo.

A Tabela 5 demonstra os resultados de precisão quando utilizado o método *Leave-one-out Cross Validation* com a ponderação de atributos realizada pelo especialista. O número de

partições p utilizados é p = 10, o número de vizinhos k = 5 e o limiar de similaridade (Sim) entre 100% e 50%.

Tabela 5 – Resultado de precisão do método LOOCV para pesos ponderados por especialista.

k-NN	1	2	3	4	5
Sim (%)	Precisão (%)				
100	100,00	NaN	NaN	NaN	NaN
95	85,44	88,42	90,45	93,37	94,93
90	79,34	77,49	77,48	77,49	77,78
85	78,31	75,52	73,95	74,67	76,42
80	78,40	75,52	73,78	73,40	75,57
75	77,47	75,00	73,33	71,72	73,25
70	77,34	74,31	72,18	70,37	71,03
65	77,04	74,02	71,90	70,10	70,35
60	76,74	73,84	71,71	69,96	70,08
55	76,74	73,84	71,71	69,96	70,08
50	76,74	73,84	71,71	69,96	70,08

Fonte: Autoria própria.

Para o método LOOCV com ponderação de atributos, nota-se um aumento discreto na similaridade entre os casos quando comparando-se com o mesmo método sem ponderação. Porém, em relação aos valores de precisão, nota-se um aumento mais acentuado, sendo que os valores obtidos são majoritariamente superiores do que quando não utiliza-se a ponderação de atributos, inclusive para quando utiliza-se mais de um vizinho mais próximo.

Desta forma, percebe-se que a ponderação de atributos pelo especialista é algo fundamental para o aumento da similaridade entre os casos e também para melhorar a precisão do sistema ao recomendar soluções para incidentes de segurança.

5.3 RETENÇÃO E REÚSO DO CONHECIMENTO

A retenção e reúso do conhecimento são aspectos importantes quando se tem o intuito de utilizar as lições aprendidas por uma organização para a resolução de novos problemas. O conhecimento deve ser passível de ser armazenado e reutilizado de forma a resolver novos problemas satisfatoriamente.

Para que fosse possível avaliar a correta recuperação do conhecimento do especialista em resolver incidentes de segurança computacionais, desenvolveu-se um experimento complementar ao experimento (i), no qual foram recuperados aleatoriamente cinco incidentes dos quais

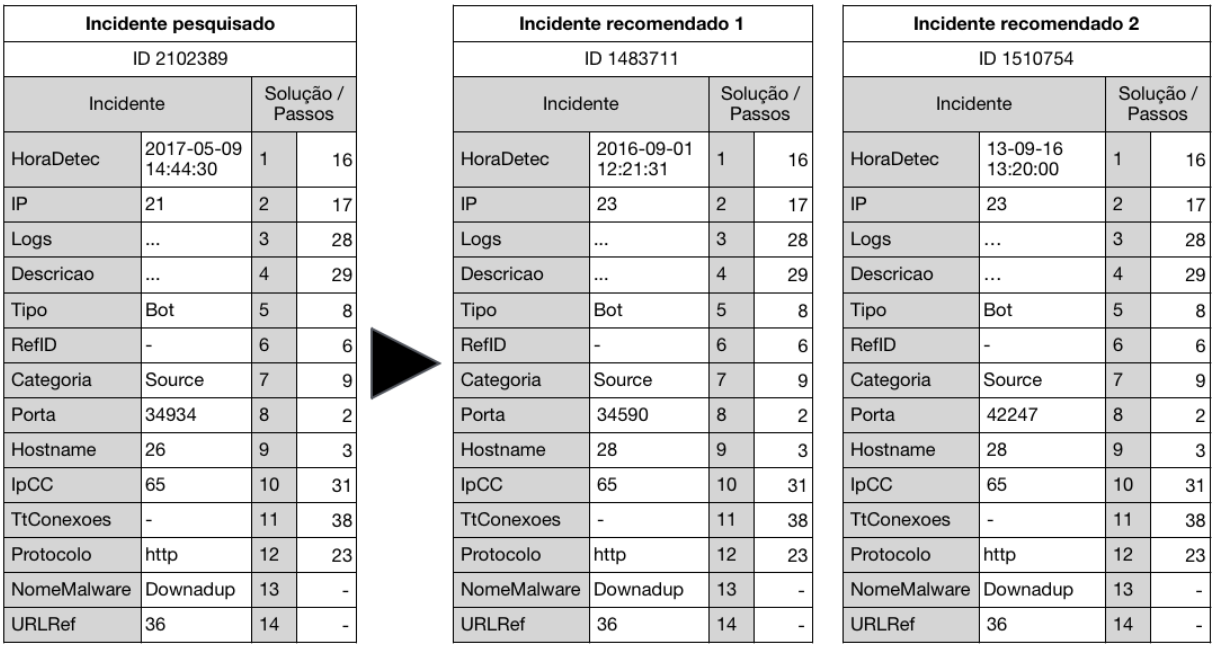
utilizou-se para pesquisa na base de casos apenas a parte do problema (o incidente sem sua solução) e, para cada um deles, recuperou-se os dois incidente mais similares, avaliando-se então de forma prática, se as soluções dos problemas recuperados eram susceptíveis de serem aplicadas aos casos previamente selecionados de forma aleatória.

Foram selecionados os incidentes 2102389, 2261674, 966062, 1746148 e 845538. A seguir são detalhados os incidentes que serviram como pesquisa juntamente com os dois incidentes mais semelhantes recomendados pelo protótipo desenvolvido. É importante ressaltar que alguns campos como endereços de IP e $URLs$ foram codificadas para manter o sigilo das informações.

São apresentados os incidentes com os seus respectivos planos para que fosse possível a comparação entre eles. Quando o plano do incidente que serviu como pesquisa é exatamente igual ao plano do incidente que foi recuperado, entende-se que o mesmo pode ser aplicado para a resolução do problema. Porém quando o plano gerado é diferente, necessita-se de uma análise mais minuciosa para identificar se os passos gerados poderiam resolver o problema de forma correta.

A Figura 10 apresenta o incidente 2102389 que serviu como pesquisa, e os incidentes 1483711 e 1510754 que foram recuperados pelo sistema (incidente recomendado). O incidente pesquisado e ambos incidentes recuperados são do tipo Bot. Os dois incidentes recuperados foram gerados com quinze dias de diferença entre eles, e com alguns meses de diferença em relação ao incidente pesquisado, provavelmente pelo mesmo *botmaster*, pois os três possuem o mesmo endereço de IP de origem do controlador ($IpCC$ do *botmaster*). Ambos incidentes recuperados possuem o mesmo plano de tratamento do incidente pesquisado, e portanto pode-se dizer que o sistema obteve sucesso na recuperação de dois casos cujas soluções poderiam ser aplicadas ao incidente pesquisado, demonstrando que o conhecimento do especialista foi retido e é passível de ser reutilizado.

Figura 10 – Incidentes 2102389, 1483711 e 1510754.



Incidente pesquisado			
ID 2102389			
Incidente		Solução / Passos	
HoraDetec	2017-05-09 14:44:30	1	16
IP	21	2	17
Logs	...	3	28
Descricao	...	4	29
Tipo	Bot	5	8
RefID	-	6	6
Categoria	Source	7	9
Porta	34934	8	2
Hostname	26	9	3
IpCC	65	10	31
TtConexoes	-	11	38
Protocolo	http	12	23
NomeMalware	Downadup	13	-
URLRef	36	14	-

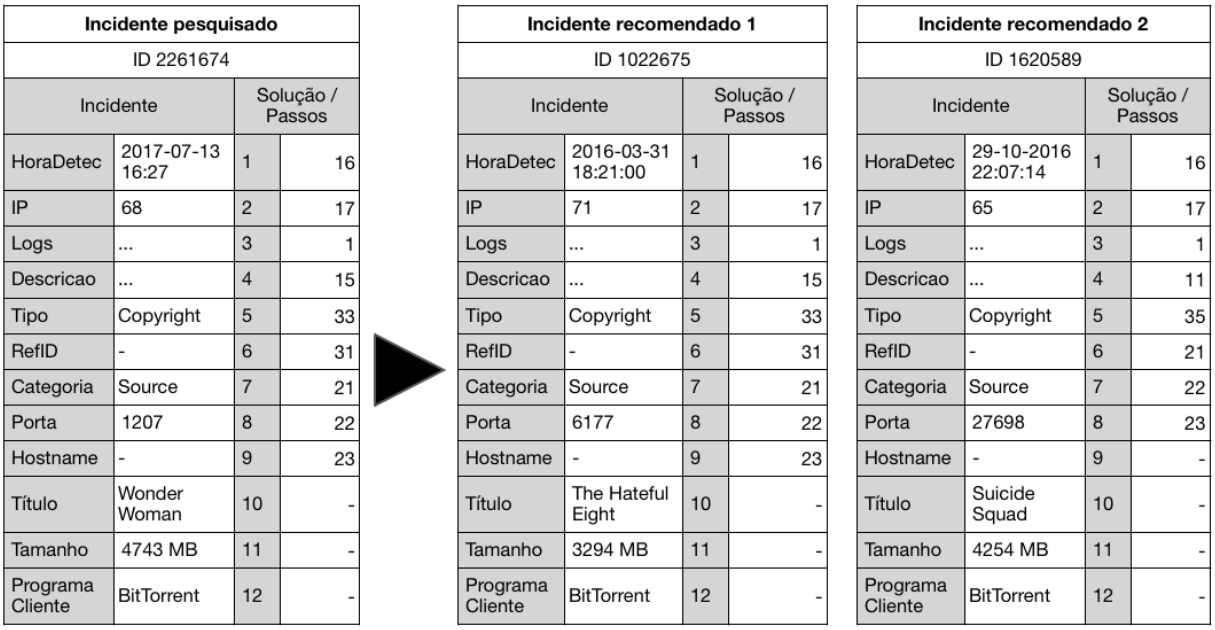
Incidente recomendado 1			
ID 1483711			
Incidente		Solução / Passos	
HoraDetec	2016-09-01 12:21:31	1	16
IP	23	2	17
Logs	...	3	28
Descricao	...	4	29
Tipo	Bot	5	8
RefID	-	6	6
Categoria	Source	7	9
Porta	34590	8	2
Hostname	28	9	3
IpCC	65	10	31
TtConexoes	-	11	38
Protocolo	http	12	23
NomeMalware	Downadup	13	-
URLRef	36	14	-

Incidente recomendado 2			
ID 1510754			
Incidente		Solução / Passos	
HoraDetec	13-09-16 13:20:00	1	16
IP	23	2	17
Logs	...	3	28
Descricao	...	4	29
Tipo	Bot	5	8
RefID	-	6	6
Categoria	Source	7	9
Porta	42247	8	2
Hostname	28	9	3
IpCC	65	10	31
TtConexoes	-	11	38
Protocolo	http	12	23
NomeMalware	Downadup	13	-
URLRef	36	14	-

Fonte: Autoria própria.

Para o incidente 2261674 que serviu como pesquisa, e os incidentes 1022675 e 1620589 que foram recuperados pelo sistema, a Figura 11 demonstra que ambos incidentes recuperados e o incidente pesquisado são do tipo $Copyright$ representando o compartilhamento indevido de filmes por meio de um programa de $BitTorrent$. Em relação ao plano de tratamento, apenas o incidente 1022675 possui o mesmo plano de tratamento do que o incidente pesquisado, e portanto poderia ser diretamente utilizado para sanar o problema. Porém o incidente 1620589 possui um plano de tratamento ligeiramente distinto, o que demanda uma análise mais detalhada dos passos a fim de se verificar se a solução do mesmo resolveria o problema apresentado pelo incidente pesquisado (2261674).

Figura 11 – Incidentes 2261674, 1022675 e 1620589.



Incidente pesquisado			
ID 2261674			
Incidente		Solução / Passos	
HoraDetec	2017-07-13 16:27	1	16
IP	68	2	17
Logs	...	3	1
Descricao	...	4	15
Tipo	Copyright	5	33
RefID	-	6	31
Categoria	Source	7	21
Porta	1207	8	22
Hostname	-	9	23
Título	Wonder Woman	10	-
Tamanho	4743 MB	11	-
Programa Cliente	BitTorrent	12	-

Incidente recomendado 1			
ID 1022675			
Incidente		Solução / Passos	
HoraDetec	2016-03-31 18:21:00	1	16
IP	71	2	17
Logs	...	3	1
Descricao	...	4	15
Tipo	Copyright	5	33
RefID	-	6	31
Categoria	Source	7	21
Porta	6177	8	22
Hostname	-	9	23
Título	The Hateful Eight	10	-
Tamanho	3294 MB	11	-
Programa Cliente	BitTorrent	12	-

Incidente recomendado 2			
ID 1620589			
Incidente		Solução / Passos	
HoraDetec	29-10-2016 22:07:14	1	16
IP	65	2	17
Logs	...	3	1
Descricao	...	4	11
Tipo	Copyright	5	35
RefID	-	6	21
Categoria	Source	7	22
Porta	27698	8	23
Hostname	-	9	-
Título	Suicide Squad	10	-
Tamanho	4254 MB	11	-
Programa Cliente	BitTorrent	12	-

Fonte: Autoria própria.

A Figura 12 apresenta os planos de tratamento dos incidentes 2261674 (pesquisado) e 1620589 (recomendado) lado a lado para avaliarmos a semelhança entre eles. Percebe-se que o incidente pesquisado possui passos mais detalhados para resolver o problema em questão do que o incidente recomendado. Os passos do incidente recomendado demonstram de maneira mais genérica como resolver o problema. Desta forma percebe-se que isto pode representar que dois especialistas diferentes resolveram estes incidentes semelhantes, porém no incidente pesquisado as informações possuem maiores detalhes. Assim se evidencia que apesar de o método desenvolvido permitir a retenção do conhecimento utilizando-se uma abordagem didática de como resolver um problema detalhando-se mais os passos, pode acontecer de o funcionário encarregado boicotar de certa forma o sistema omitindo certas informações, seja isto algo intencional ou não. Desta forma entende-se que não é possível afirmar que a solução recuperada é passível de ser utilizada para solucionar o problema, principalmente pelo fato de ela não conter os detalhes necessários para resolver o incidente pesquisado que trata do compartilhamento indevido de arquivos.

Figura 12 – Detalhamento do plano de tratamento dos incidentes 2261674 e 1620589.

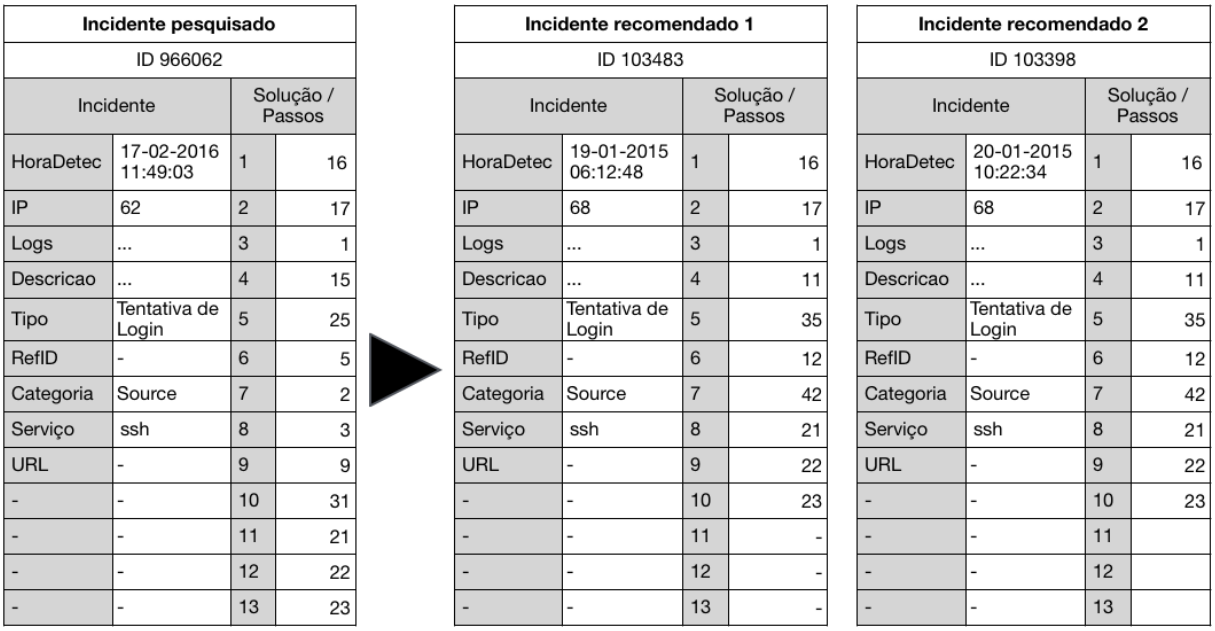
IdIncidente	2261674	1620589
Passo 1	Coleta de evidências para comprovar o problema	Coleta de evidências para comprovar o problema
Passo 2	Analizar evidências para comprovar o problema	Analizar evidências para comprovar o problema
Passo 3	Bloquear o acesso com a Internet do host contaminado no firewall de borda	Bloquear o acesso com a Internet do host contaminado no firewall de borda
Passo 4	Abrir chamada com o Centro de Apoio ao Usuário para enviar técnico ao local	Notificar o responsável pelo equipamento/host/server/ rede/página web sobre o Incidente de Segurança recebido
Passo 5	Desinstalar o programa cliente do protocolo BitTorrent	Solicitar ao responsável do equipamento/host/server para imediatamente interromper a comunicação com a rede de dados.
Passo 6	Orientar o usuário a seguir os orientações da Livro da Cartilha de Segurança para Internet https://cartilha.cert.br/	Após as correções/atualizações/resolução do incidente de segurança, solicitar o desbloqueio no firewall de borda
Passo 7	Após as correções/atualizações/resolução do incidente de segurança, solicitar o desbloqueio no firewall de borda	Após as correçoes/atualizações/resolução do incidente de segurança, desbloquear no firewall de borda
Passo 8	Após as correçoes/atualizações/resolução do incidente de segurança, desbloquear no firewall de borda	Responder sobre a resolução do incidente ao CAIS
Passo 9	Responder sobre a resolução do incidente ao CAIS	

Fonte: Autoria própria.

A Figura 13 demonstra o incidente 966062 que serviu como pesquisa, e os incidentes 103483 e 103398 que foram recuperados pelo sistema. Neste caso tratam-se de tentativas de *login* em três *hots* nos quais o serviço SSH estava disponível. Nesta situação o plano do incidente pesquisado difere-se dos planos dos incidentes recuperados que são idênticos. Assim, necessita-se de uma análise mais completa para que seja possível identificar se os diferentes planos são maneiras diferentes de resolver o mesmo problema, ou se um dos casos apresenta um plano inconsistente.

A Figura 14 apresenta os passos dos incidentes lado a lado para avaliarmos a semelhança entre eles. Percebe-se que no incidente 966062 os passos são realizados de forma mais detalhada do que nos incidente 103483 e 103398, mas que porém o plano dos incidentes recuperados demonstra-se suscetível de ser aplicado ao caso pesquisado. De acordo com um dos especialistas responsáveis pela resolução destes incidentes no CPD da UFSM, a diferença entre os dois planos se deve ao fato de que o *host* do incidente 966062 encontra-se fisicamente alocado no próprio CPD, enquanto os *hosts* pertencentes aos outros dois incidentes encontram-se em prédios externos. Assim, o primeiro incidente pôde ser resolvido pela equipe do próprio CPD, enquanto os incidentes 103483 e 103398 foram resolvidos pelo responsável pelo equipamento. Desta forma, entende-se que neste caso o conhecimento do especialista que foi recuperado é susceptível de resolver o incidente pesquisado.

Figura 13 – Incidentes 966062, 103483 e 103398.



Incidente pesquisado			
ID 966062			
Incidente		Solução / Passos	
HoraDetec	17-02-2016 11:49:03	1	16
IP	62	2	17
Logs	...	3	1
Descricao	...	4	15
Tipo	Tentativa de Login	5	25
RefID	-	6	5
Categoria	Source	7	2
Serviço	ssh	8	3
URL	-	9	9
-	-	10	31
-	-	11	21
-	-	12	22
-	-	13	23

Incidente recomendado 1			
ID 103483			
Incidente		Solução / Passos	
HoraDetec	19-01-2015 06:12:48	1	16
IP	68	2	17
Logs	...	3	1
Descricao	...	4	11
Tipo	Tentativa de Login	5	35
RefID	-	6	12
Categoria	Source	7	42
Serviço	ssh	8	21
URL	-	9	22
-	-	10	23
-	-	11	-
-	-	12	-
-	-	13	-

Incidente recomendado 2			
ID 103398			
Incidente		Solução / Passos	
HoraDetec	20-01-2015 10:22:34	1	16
IP	68	2	17
Logs	...	3	1
Descricao	...	4	11
Tipo	Tentativa de Login	5	35
RefID	-	6	12
Categoria	Source	7	42
Serviço	ssh	8	21
URL	-	9	22
-	-	10	23
-	-	11	
-	-	12	
-	-	13	

Fonte: Autoria própria.

Figura 14 – Detalhamento do plano de tratamento dos incidentes 966062, 103483 e 103398.

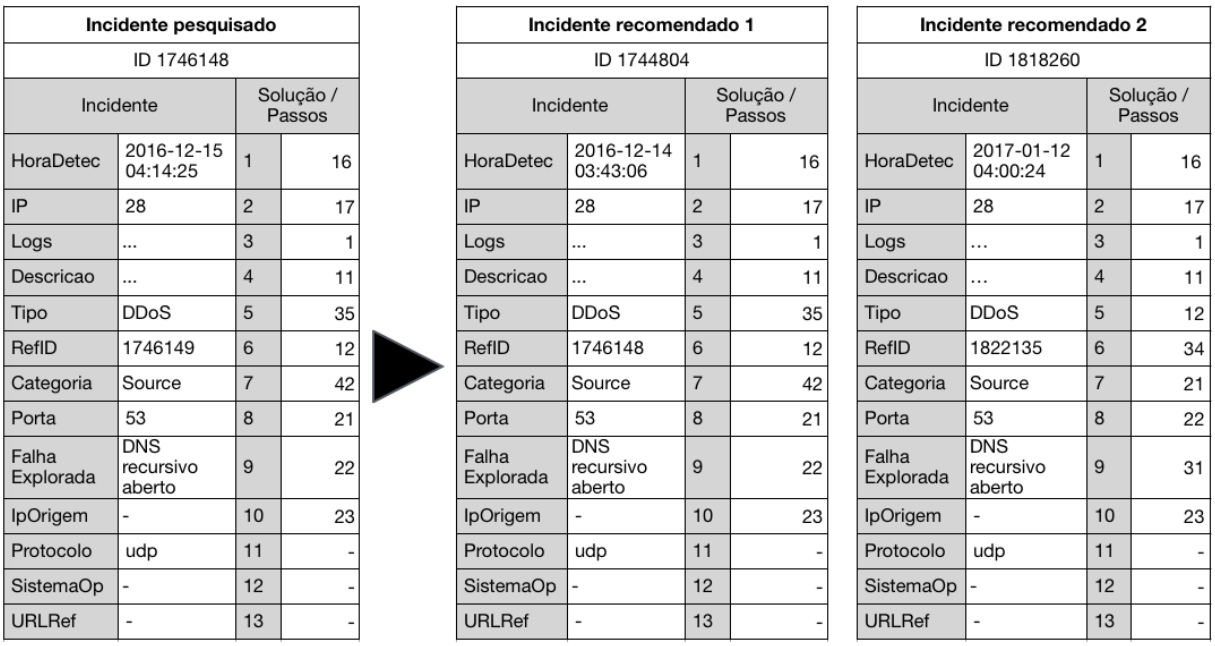
IdIncidente	966062	103483 e 103398
Passo 1	Coleta de evidências para comprovar o problema	Coleta de evidências para comprovar o problema
Passo 2	Analizar evidências para comprovar o problema	Analizar evidências para comprovar o problema
Passo 3	Bloquear o acesso com a Internet do host contaminado no firewall de borda	Bloquear o acesso com a Internet do host contaminado no firewall de borda
Passo 4	Abrir chamada com o Centro de Apoio ao Usuário para enviar técnico ao local	Notificar o responsável pelo equipamento/host/server/rede/página web sobre o Incidente de Segurança recebido
Passo 5	Investigar o Incidente, coletar e examinar evidências digitais	Solicitar ao responsável do equipamento/host/server para imediatamente interromper a comunicação com a rede de dados.
Passo 6	Reinstalar Sistema Operacional	Solicitar ao responsável do equipamento/host/server para corrigir o problema
Passo 7	Atualizar o Sistema Operacional	Comunicar o CPD/UFSM sobre a resolução do incidente de segurança
Passo 8	Ativar firewall no host/equipamento	Após as correções/atualizações/resolução do incidente de segurança, solicitar o desbloqueio no firewall de borda
Passo 9	Instalar/Atualizar o antivirus com as últimas definições de vírus	Após as correçoes/atualizações/resolução do incidente de segurança, desbloquear no firewall de borda
Passo 10	Orientar o usuário a seguir os orientações da Livro da Cartilha de Segurança para Internet https://cartilha.cert.br/	Responder sobre a resolução do incidente ao CAIS
Passo 11	Após as correções/atualizações/resolução do incidente de segurança, solicitar o desbloqueio no firewall de borda	-
Passo 12	Após as correçoes/atualizações/resolução do incidente de segurança, desbloquear no firewall de borda	-
Passo 13	Responder sobre a resolução do incidente ao CAIS	-

Fonte: Autoria própria.

A Figura 15 demonstra a comparação entre o incidente 1746148 que serviu como pes-

quisa e os incidente 1744804 e 1818260 que foram recuperados. Os três incidentes dizem respeito a uma tentativa de ataque $DDoS$ realizada no mesmo *host* com um dia de diferença e exploram a falha de DNS recursivo "aberto". Ambos incidentes recuperados possuem o mesmo plano de tratamento que o incidente pesquisado e portanto o conhecimento do especialista pode ser reutilizado para resolver o problema.

Figura 15 – Incidentes 1746148, 1744804 e 1818260.



Incidente pesquisado			
ID 1746148			
Incidente		Solução / Passos	
HoraDetec	2016-12-15 04:14:25	1	16
IP	28	2	17
Logs	...	3	1
Descricao	...	4	11
Tipo	DDoS	5	35
RefID	1746149	6	12
Categoria	Source	7	42
Porta	53	8	21
Falha Explorada	DNS recursivo aberto	9	22
IpOrigem	-	10	23
Protocolo	udp	11	-
SistemaOp	-	12	-
URLRef	-	13	-

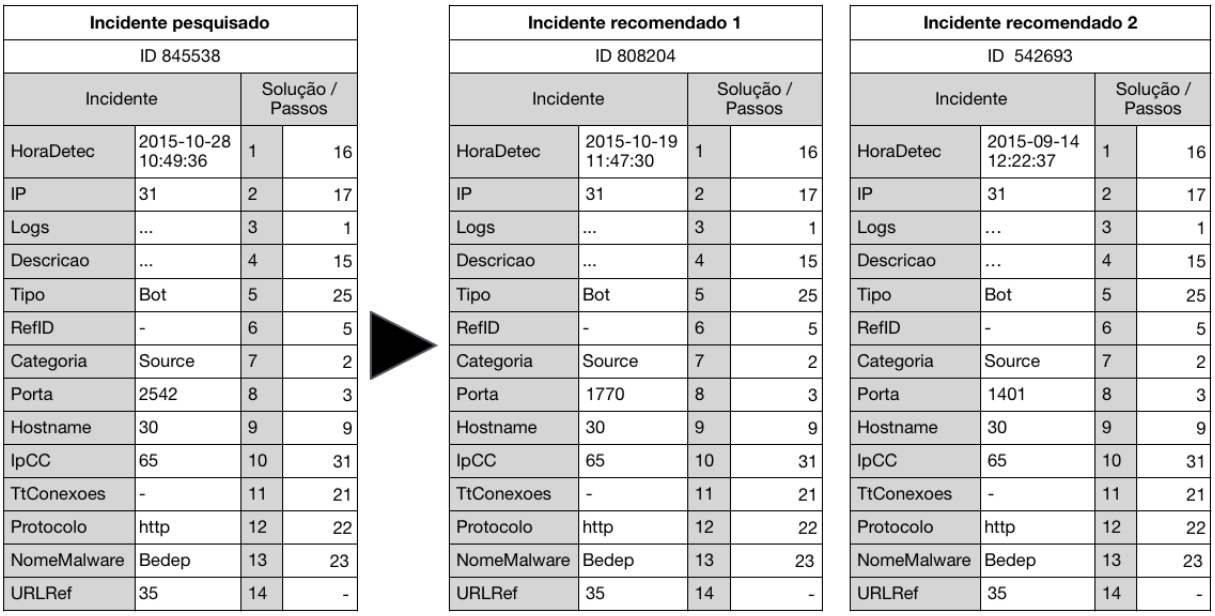
Incidente recomendado 1			
ID 1744804			
Incidente		Solução / Passos	
HoraDetec	2016-12-14 03:43:06	1	16
IP	28	2	17
Logs	...	3	1
Descricao	...	4	11
Tipo	DDoS	5	35
RefID	1746148	6	12
Categoria	Source	7	42
Porta	53	8	21
Falha Explorada	DNS recursivo aberto	9	22
IpOrigem	-	10	23
Protocolo	udp	11	-
SistemaOp	-	12	-
URLRef	-	13	-

Incidente recomendado 2			
ID 1818260			
Incidente		Solução / Passos	
HoraDetec	2017-01-12 04:00:24	1	16
IP	28	2	17
Logs	...	3	1
Descricao	...	4	11
Tipo	DDoS	5	12
RefID	1822135	6	34
Categoria	Source	7	21
Porta	53	8	22
Falha Explorada	DNS recursivo aberto	9	31
IpOrigem	-	10	23
Protocolo	udp	11	-
SistemaOp	-	12	-
URLRef	-	13	-

Fonte: Autoria própria.

A Figura 16 demonstra a comparação entre os incidentes 845538, que serviu como pesquisa, e os incidentes 808204 e 542693. Os três incidentes dizem respeito a ataques do tipo Bot que foram realizados entre setembro e outubro de 2015, pelo no mesmo ip. Ambos incidentes recuperados possuem o mesmo plano de tratamento que o incidente pesquisado e portanto conclui-se que conhecimento do especialista pode ser reutilizado para resolver o problema.

Figura 16 – Incidentes 845538, 808204 e 542693.



Incidente pesquisado			
ID 845538			
Incidente		Solução / Passos	
HoraDetec	2015-10-28 10:49:36	1	16
IP	31	2	17
Logs	...	3	1
Descricao	...	4	15
Tipo	Bot	5	25
RefID	-	6	5
Categoria	Source	7	2
Porta	2542	8	3
Hostname	30	9	9
IpCC	65	10	31
TtConexoes	-	11	21
Protocolo	http	12	22
NomeMalware	Bedep	13	23
URLRef	35	14	-

Incidente recomendado 1			
ID 808204			
Incidente		Solução / Passos	
HoraDetec	2015-10-19 11:47:30	1	16
IP	31	2	17
Logs	...	3	1
Descricao	...	4	15
Tipo	Bot	5	25
RefID	-	6	5
Categoria	Source	7	2
Porta	1770	8	3
Hostname	30	9	9
IpCC	65	10	31
TtConexoes	-	11	21
Protocolo	http	12	22
NomeMalware	Bedep	13	23
URLRef	35	14	-

Incidente recomendado 2			
ID 542693			
Incidente		Solução / Passos	
HoraDetec	2015-09-14 12:22:37	1	16
IP	31	2	17
Logs	...	3	1
Descricao	...	4	15
Tipo	Bot	5	25
RefID	-	6	5
Categoria	Source	7	2
Porta	1401	8	3
Hostname	30	9	9
IpCC	65	10	31
TtConexoes	-	11	21
Protocolo	http	12	22
NomeMalware	Bedep	13	23
URLRef	35	14	-

Fonte: Autoria própria.

5.4 CONSIDERAÇÕES PARCIAIS

Este Capítulo abordou a validação da solução proposta. Foram utilizados métodos de validação cruzada para aferir a precisão do sistema. Pôde ser observado nos experimentos que a ponderação dos atributos, isto é, a atribuição de pesos garantiu uma significativa melhora na precisão do sistema, refletindo o conhecimento do especialista em relação aos atributos de maior relevância para os cálculos de similaridade.

Em relação a retenção do conhecimento, nota-se que as lições aprendidas puderam ser reutilizadas na maioria dos casos para sanar problemas similares. Isto demonstra a aplicabilidade da solução na resolução de incidentes de segurança com a utilização do conhecimento retido de forma satisfatória.

Cabe ressaltar que a solução apresentada é flexível, podendo ser adaptada a diferentes contextos. A flexibilidade diz respeito aos ajustes que podem ser efetuados pelo especialista como a ponderação dos atributos, adição e remoção de passos contidos na biblioteca de ações, e a possibilidade de adição e remoção de atributos conforme necessidade do ambiente.

6 CONSIDERAÇÕES FINAIS

As organizações são vulneráveis à perda do conhecimento o qual está contido na mente dos especialistas, sendo que isto também acontece no contexto de resolução de incidentes computacionais. Todos os dias os funcionários podem deixar definitivamente o ambiente de trabalho, levando consigo o conhecimento de como resolver estes problemas, fazendo com que as empresas estejam vulneráveis a perda deste ativo intelectual.

Como solução para o problema de perda de conhecimento, este trabalho propõe uma metodologia para IRS que explora a automatização de recomendações de planos de resposta à incidentes de segurança com a utilização de um padrão de dados e ponderação de atributos de RBC. A principal contribuição deste trabalho é uma metodologia que permite às equipes dos CSIRTs o reúso do conhecimento relativo à resolução de incidentes de segurança através do uso de técnicas de RBC. Desta forma, a empresa passa a ser detentora do conhecimento, que fica retido na base de casos, possibilitando a outros funcionários utilizarem-se deste conhecimento para apoio na resolução de incidentes de segurança. Este trabalho difere-se dos demais trabalhos encontrados na literatura pela utilização da metodologia de RBC a qual explora o padrão de representação atualmente adotado por CSIRTs (o IODEF), um ciclo de refinamento de casos de incidente/solução, bem como a ponderação de atributos dos casos.

Foi desenvolvida uma memória de resolução de incidentes com o auxílio do RBC, o qual funciona como um *framework* para a aquisição e reúso do conhecimento. Foi utilizado o protocolo padrão de representação de incidentes IODEF que foi desenvolvido para ser utilizado por CSIRTs, possibilitando a comunicação entre ambientes heterogêneos. Posteriormente foram selecionados e modelados os atributos que serviram para a representação dos incidentes de segurança, sendo que os mesmos foram mapeados para o padrão IODEF. A ponderação de atributos de RBC foi utilizada para refletir o conhecimento do especialista em relação à importância dos atributos que foram selecionados, sendo que o mesmo pode também indexar ou não os atributos que achar necessário. Por último foram explorados e modelados o planos de tratamento que são sugeridos de forma automatizada com o auxílio do RBC, visando apoiar o especialista na resolução de incidentes, utilizando para isso o conhecimento retido na base de casos.

A avaliação da solução utilizou-se de dois experimentos. O primeiro evidencia a importância da ponderação dos atributos, permitindo que o especialista utilize de seu conhecimento

tácito para realizar um balanceamento dos pesos visando a melhoria de desempenho do sistema. O desempenho foi medido pela precisão do sistema utilizando-se dois métodos de validação cruzada. Os resultados deste experimento demonstraram que a precisão obteve uma melhora significativa quando o especialista realizou a ponderação. Outra constatação relacionada a esta avaliação é de que a base de casos utilizada possui uma boa qualidade, pois os incidentes possuem uma boa representatividade, mesmo quando não é utilizada a ponderação dos atributos, o que é evidenciado pelos bons valores de precisão. O segundo experimento buscou avaliar se o conhecimento fica efetivamente retido e se pode ser realmente reutilizado para apoiar a decisão do especialista. Este experimento expôs a viabilidade da solução proposta, pois foi possível resolver os incidentes pesquisados através dos planos de tratamento recuperados pelo sistema.

Cabe ressaltar algumas dificuldades encontradas na realização deste trabalho. A falta de bases de dados abertas sobre incidentes de segurança computacionais fez com que tivéssemos algumas dificuldades na obtenção dos incidentes que formaram a nossa base de casos. Esta dificuldade impediu que pudéssemos realizar avaliações em diferentes bases de casos. Felizmente, por mais que houvesse dificuldades na obtenção dos casos, foi conseguido um número suficiente destes para que pudéssemos desenvolver as validações necessárias, pois as metodologias de validação cruzada utilizadas permitem que seja realizado o particionamento dos dados em conjuntos de treinamento e testes sem que seja haja perda significativa na capacidade de modelagem e testes realizados (SENI; ELDER, 2010). Outro ponto a ser destacado é que nesta abordagem pode ocorrer de o especialista boicotar o sistema por algum motivo, mas que mecanismos de autenticação e/ou validação por duas pessoas pode minimizar este risco.

Ao término deste trabalho, é possível então identificar que os objetivos traçados no início da pesquisa foram alcançados e comprovados com êxito. Novos funcionários podem assim se beneficiar de recomendações construídas com base no conhecimento fornecido por outros especialistas, melhorando com isto a retenção do conhecimento nas organizações, aumentando assim sua competitividade no contexto atual.

6.1 TRABALHOS FUTUROS

Como trabalhos a serem realizados em complemento a esta dissertação, podem ser desenvolvidas os tópicos a seguir:

a) Explorar a automatização de respostas: a automatização de respostas pode ser explorada,

fazendo com que algumas das respostas para incidentes mais triviais possam ser executadas de maneira automática, sem que o profissional de segurança necessite interferir nisso. Um bloqueio temporário no *firewall*, por exemplo, pode ser executado em estações de trabalho para que posteriormente os profissionais responsáveis possam tratar do incidente de forma mais detalhada, permitindo antes disso que a ameaça seja neutralizada até que o problema seja resolvido. A automatização pode também ser aplicada no processo de construção de casos, os quais não necessitariam de uma revisão e adição de informações pelo especialista. Desta forma um novo incidente seria inserido na base de casos de forma automática;

b) Utilizar ponderação com métodos de aprendizagem para a atribuição de pesos: a atribuição de pesos pode ser realizada de forma automática com a utilização de técnicas de aprendizagem. Desta forma pode-se otimizar a precisão do sistema, pois isto permite que sejam testados diferentes pesos de forma automática buscando-se assim os melhores pesos possíveis;

c) Atribuição de pesos dinâmica: a atribuição de pesos pode ser realizada de forma dinâmica por classe para que o especialista possa determinar pesos diferentes de acordo com a pesquisa a ser realizada. Desta forma ao pesquisar um incidente do tipo $Copyright$, por exemplo, pode-se dar maior importância ao atributo $Titulo$ e assim recuperar mais incidentes que possuam este atributo;

d) Verificação de similaridade nos campos de texto: apesar de neste trabalho os atributos de campos de texto ($Logs$ e $Descricao$) não terem sido indexados, isto é, não considerados para pesquisa, pode-se, com a utilização de algoritmos específicos, verificar a semelhança entre as descrições textuais afim de se computar a similaridade destes campos (indexar).

REFERÊNCIAS

AHMAD, A.; HADGKISS, J.; RUIGHAVER, A. Incident response teams – Challenges in supporting the organisational security function. **Computers and Security**, [S.l.], v.31, n.5, p.643 – 652, 2012.

AHMAD, A.; MAYNARD, S. B.; SHANKS, G. A case analysis of information systems and security incident responses. **International Journal of Information Management**, [S.l.], v.35, n.6, p.717 – 723, 2015.

ANUAR, N. B. et al. An investigation and survey of response options for Intrusion Response Systems (IRSs). In: INFORMATION SECURITY FOR SOUTH AFRICA, 2010. **Anais...** [S.l.: s.n.], 2010. p.1–8.

ARKKO, J.; BRADNER, S. O. **IANA Allocation Guidelines for the Protocol Field**. [S.l.]: RFC Editor, 2008. n.5237. (Request for Comments).

BEJTLICH, R. **The Practice of Network Security Monitoring**: understanding incident detection and response. San Francisco, CA, USA: No Starch Press, 2013.

CAPUZZI, G.; SPALAZZI, L.; PAGLIARECCI, F. IRSS: incident response support system. In: CTS. **Anais...** IEEE Computer Society, 2006. p.81–88.

CARPENTER, B. E.; JIANG, S. **Transmission and Processing of IPv6 Extension Headers**. [S.l.]: RFC Editor, 2013. n.7045. (Request for Comments).

CERTBR. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Acessado em: 22-06-2017, https://www.cert.br/stats/incidentes/.

DALKIR, K.; LIEBOWITZ, J. **Knowledge Management in Theory and Practice**. [S.l.]: MIT Press, 2011.

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

HOVE, C.; TARNES, M. **Information security incident management**: an empirical study of current practice. 2013. Dissertação (Mestrado em Ciência da Computação) — Norwegian University of Science and Technology, Trondheim, Norway.

INAYAT, Z. et al. Intrusion response systems: foundations, design, and challenges. **Journal of Network and Computer Applications**, [S.l.], v.62, p.53 – 74, 2016.

ISO-27035. **Information technology - Security techniques - Information security incident management**. Geneva, CH: International Organization for Standardization, 2011. Standard.

JIANG, F. et al. Case Retrieval for Network Security Emergency Response Based on Description Logic. In: INTELLIGENT INFORMATION PROCESSING. **Anais...** Springer, 2014. p.284–293. (IFIP Advances in Information and Communication Technology, v.432).

KHURANA, H. et al. Palantir: a framework for collaborative incident response and investigation. In: SYMPOSIUM ON IDENTITY AND TRUST ON THE INTERNET, 8., New York, NY, USA. **Proceedings...** ACM, 2009. p.38–51. (IDtrust '09).

KIM, H. K.; IM, K. H.; PARK, S.-C. DSS for computer security incident response applying CBR and collaborative response. **Expert Syst. Appl.**, [S.l.], v.37, n.1, p.852–870, 2010.

KOHAVI, R. et al. A study of cross-validation and bootstrap for accuracy estimation and model selection. In: ACM. **Anais...** [S.l.: s.n.], 1995.

KOLODNER, J. **Case-based Reasoning**. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1993.

LAMIS, T. A Forensic Approach to Incident Response. In: INFORMATION SECURITY CURRICULUM DEVELOPMENT CONFERENCE, 2010., New York, NY, USA. **Anais...** ACM, 2010. p.177–185. (InfoSecCD '10).

LEMAY, A.; LEBLANC, S. P.; JESUS, T. de. Lessons from the Strategic Corporal: implications of cyber incident response. In: ACM SIGMIS CONFERENCE ON COMPUTERS AND PEOPLE RESEARCH, 2015., New York, NY, USA. **Proceedings...** ACM, 2015. p.61–66. (SIGMIS-CPR '15).

MANSAR, S. L.; MARIR, F.; REIJERS, H. A. Case-based reasoning as a technique for knowledge management in business process redesign. **Electronic Journal on Knowledge Management**, [S.l.], v.1, n.2, p.113–124, 2003.

METZGER, S.; HOMMEL, W.; REISER, H. Integrated Security Incident Management – Concepts and Real-World Experiences. In: SIXTH INTERNATIONAL CONFERENCE ON IT SECURITY INCIDENT MANAGEMENT AND IT FORENSICS, 2011., Washington, DC, USA. **Proceedings...** IEEE Computer Society, 2011. p.107–121. (IMF '11).

NONAKA, I.; TAKEUCHI, H. **The Knowledge-creating Company**: how japanese companies create the dynamics of innovation. [S.l.]: Oxford University Press, 1995. (Everyman's library).

PHILLIPS, A.; DAVIS, M. **Tags for Identifying Languages**. [S.l.]: IETF, 2006. (Request for Comments).

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–V11–340.

PROSISE, C.; MANDIA, K.; PEPE, M. **Incident Response &Amp; Computer Forensics, 2Nd Ed.** 2.ed. New York, NY, USA: McGraw-Hill, Inc., 2003.

RAHIMLI, A. Knowledge Management and Competitive Advantage. In: INFORMATION AND KNOWLEDGE MANAGEMENT. **Anais...** [S.l.: s.n.], 2012. p.37–43.

RAJNOVIC, D. **Computer Incident Response and Product Security**. Indianapolis, IN, USA: Cisco Press, 2011.

REFAEILZADEH, P.; TANG, L.; LIU, H. Cross-validation. In: **Encyclopedia of database systems**. [S.l.]: Springer, 2009. p.532–538.

RICHTER, M. M.; WEBER, R. O. **Case-Based Reasoning**: a textbook. [S.l.]: Springer Publishing Company, Incorporated, 2013.

SENI, G.; ELDER, J. **Ensemble Methods in Data Mining**: improving accuracy through combining predictions. [S.l.]: Morgan and Claypool Publishers, 2010.

TAKAHASHI, T. et al. **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. **NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium**, [S.l.], p.949–954, 2016.

TøNDEL, I. A.; LINE, M. B.; JAATUN, M. G. Information security incident management: current practice as reported in the literature. **Computers and Security**, [S.l.], v.45, p.42 – 57, 2014.

WANGENHEIM, C. von; WANGENHEIM, A. von. **Raciocínio baseado em casos 2 Ed.** [S.l.]: Manole, 2013.

WIIG, K. M. Knowledge management: an introduction and perspective. **Journal of knowledge Management**, [S.l.], v.1, n.1, p.6–14, 1997.

ZHANG, Z. **Static and Dynamic Feature Weighting in Case-Based Reasoning (CBR)**. 1997. Dissertação (Mestrado em Ciência da Computação) — Simon Fraser University, Burnaby, Canada.

ANEXOS

ANEXO A – Protótipo Desenvolvido para Inserção e Preenchimento dos Incidentes

Como mencionado no texto principal, foi desenvolvido um protótipo para inserção e preenchimento dos dados advindos de incidentes. A Figura 17 representa uma tela onde é possível fazer o *upload* de arquivos IODEF para inserção na base de casos. Assim a cada novo incidente recebido é possível atualizar a base de casos. Para que este incidente seja corretamente inserido, é feita uma verificação da sintaxe XML que deve corresponder ao modelo apresentado na Figura 5 do Capítulo 4.2.1.

Figura 17 – Tela de envio do documento IODEF para inserir o incidente na base de casos.

A Figura 18 apresenta a tela onde é possível exibir os incidentes cadastrados na base de casos.

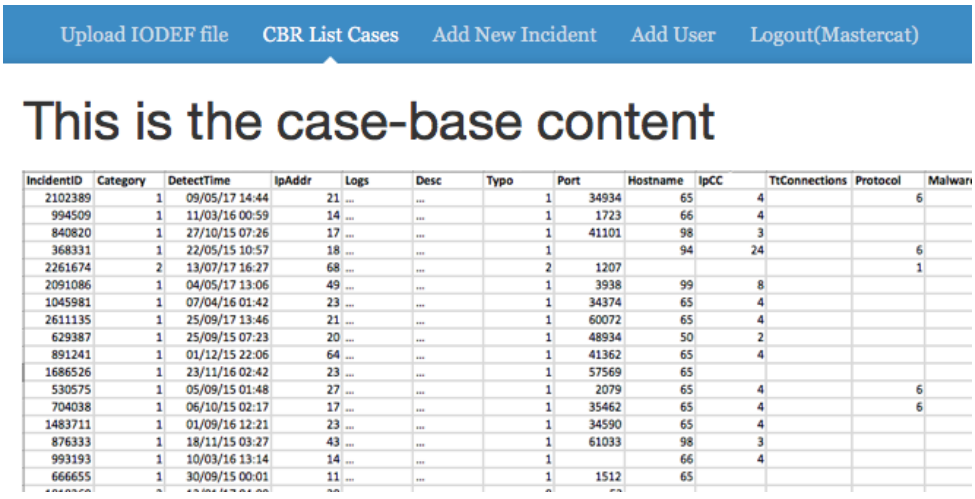


Figura 18 – Tela de exibição dos incidentes da base de casos.

A Figura 19 apresenta a tela de cadastro de um novo incidente na qual pode-se escolher um dos tipos de incidentes a ser inserido. O sistema esconde e mostra campos de acordo com o que deve ser preenchido para determinado tipo.

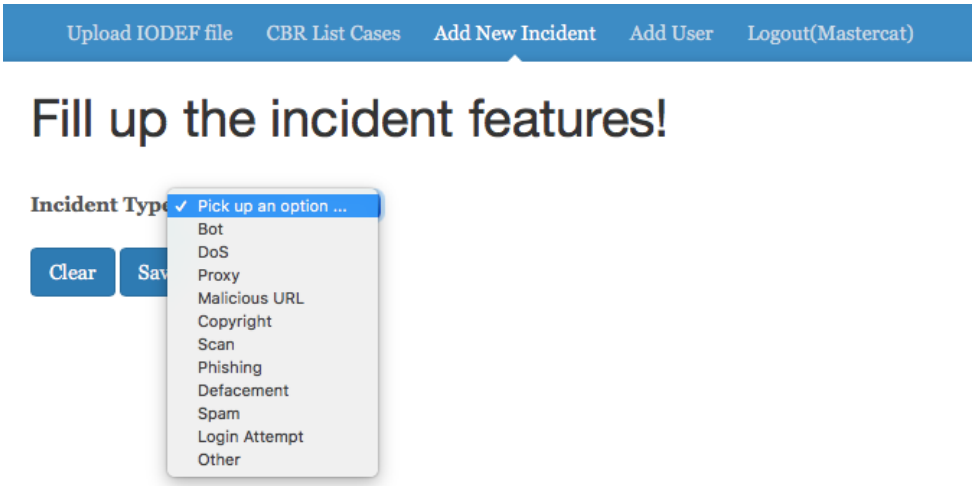


Figura 19 – Tela de registro de um novo incidente na qual é permitido escolher o tipo de incidente.

A Figura 20 apresenta a tela de preenchimento de um incidente do tipo Bot, onde os campos estão ajustados para receber informações específicas deste tipo de incidente.

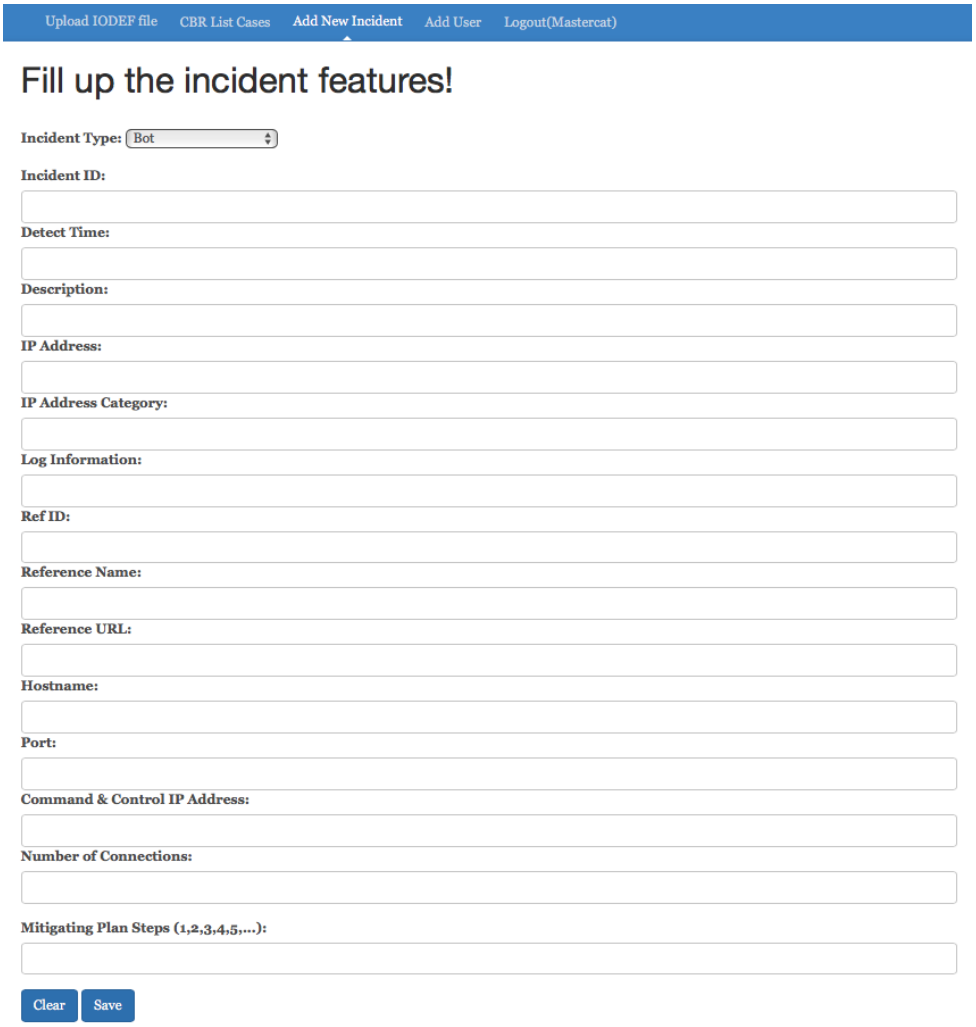


Figura 20 – Tela para preenchimento de um incidente do tipo Bot.

A Figura 20 apresenta a tela de preenchimento de um incidente do tipo $Spam$, onde os campos estão ajustados para receber informações específicas deste tipo de incidente.

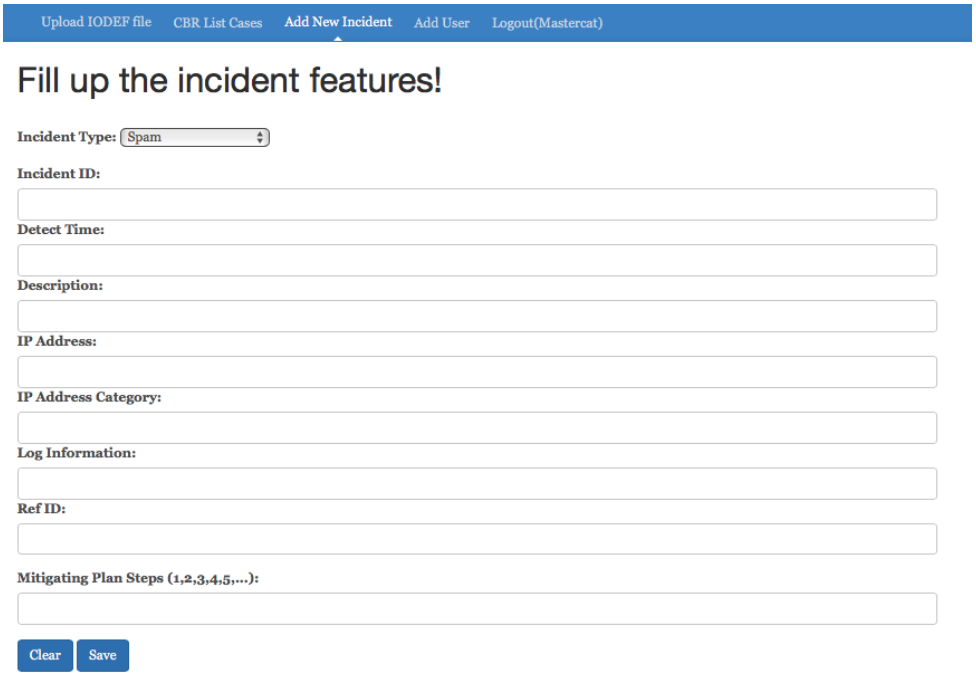


Figura 21 – Tela para preenchimento de um incidente do tipo $Spam$.

Por fim, a Figura 20 apresenta a tela de cadastro de um novo usuário do sistema.

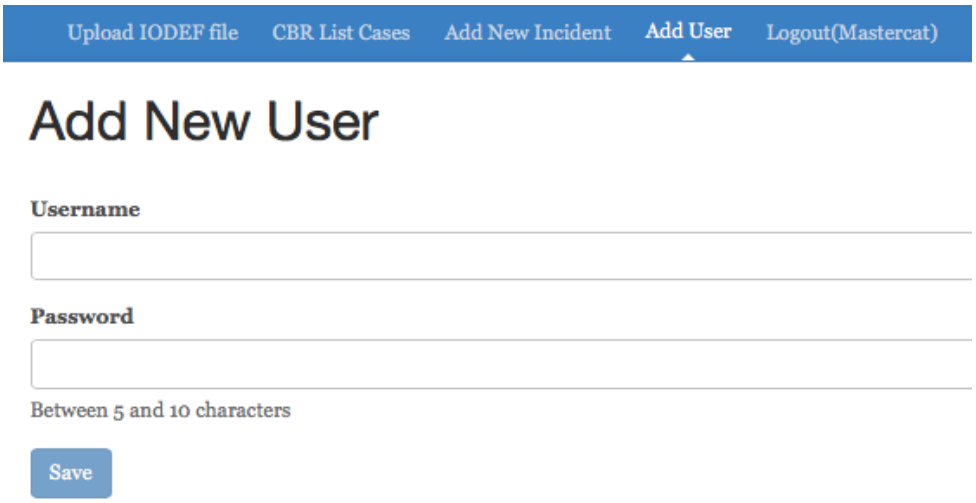


Figura 22 – Cadastro de novo usuário para utilizar o sistema.