Universidade Federal do Pampa
Isabel Boaventura Pereira

Modelagem de processos de tratamento de incidentes de segurança da informação do NTIC/UNIPAMPA

Alegrete
2013

Isabel Boaventura Pereira

Modelagem de processos de tratamento de incidentes de segurança da informação do NTIC/UNIPAMPA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciência da Computação da Universidade Federal do Pampa como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

Orientador: Cristiano Tolfo

Coorientador: Fernando Della Flora

Alegrete

2013

Isabel Boaventura Pereira

Modelagem de processos de tratamento de incidentes de segurança da informação do NTIC/UNIPAMPA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciência da Computação da Universidade Federal do Pampa como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

Trabalho de Conclusão de Curso defendido e aprovado em 24 de Outubro de 2013.

Banca examinadora:

Cristiano Tolfo
Orientador

Fernando Della Flora
Coorientador
(Unipampa)

Márcia Cristina Cera
(Unipampa)

Sam da Silva Devincenzi
(Unipampa)

Agradecimentos

Agradeço a DEUS por cada pessoa, oportunidade, e por ser meu eterno guia.

Agradeço a minha família pelo apoio e presença constante.

Agradeço aos amigos por serem companheiros e estarem presentes, ajudando e apoiando. Em especial a Amanda Caricatti Estrela e Miguel Moura Anchieta, por serem estes amigos irmãos.

Agradeço ao meu orientador, professor Doutor Cristiano Tolfo e ao coorientador, Coordenador de Segurança da Informação Fernando Della Flora. Em especial ao professor Tolfo pela infinita paciência em cada momento da 'construção' e 'destruição' deste trabalho e do artigo resultante do mesmo. Ainda tenho dificuldades na escrita, mas graças ao professor Tolfo, reconheço que com mais prática e 'n' refinamentos é possível surgir algo entendível.

A todos, obrigada. Muito Obrigada.

"Todos estes que aí estão
Atravancando o meu caminho,
Eles passarão.
Eu passarinho!"
(Mário Quintana)

Resumo

O avanço tecnológico exige que as organizações disponibilizem suas informações em formato digital. Entretanto, há a necessidade de meios adequados para se manter estas informações seguras e de oferecer suporte ao controle de acesso as informações priorizando a segurança. Visualizar os processos que demonstram como esta segurança é realizada, pode permitir um melhor entendimento, outra forma de examina-las, assim como um possível ganho de produtividade. Este trabalho de conclusão de curso tem como objetivo a modelagem e otimização de processos que envolvem o tratamento de incidentes de segurança da informação ocorridos nesta instituição pública de ensino superior. Será utilizada a abordagem de gestão de processos de negócio para otimizar os processos de tratamento de incidentes de segurança da informação ocorridos nesta instituição, alguns representados neste trabalho, para exemplificar como este processo pode ser reproduzível, utilizando a notação BPMN na modelagem dos processos para atender aos objetivos almejados. As modelagens serão validadas pela equipe responsável pelo tratamento de incidentes desta natureza da instituição. Com a modelagem e otimização realizada pretende-se: conceber uma forma padronizada de tratar destes incidentes, possibilitar a diminuição do retrabalho economizando recursos da organização e identificar se há meios de implementar alternativas para aprimorar o gerenciamento dos processos de tratamento deste tipo de incidentes. Neste trabalho são apresentados os resultados das modelagens dos processos de tratamento de incidente de segurança da informação que demonstraram-se viável. Assim demonstrando os trabalhos realizados e a viabilidade da proposta de padronização dos processos de tratamento de incidentes de segurança da informação tratados pela equipe de segurança desta instituição. E propondo melhorias para os processos atuais com a implementação de ferramentas para a automação de atividades, como geração de relatórios assim como o alerta automático de anomalias.

Palavras-chave: Segurança da informação; Modelagem de processos; BPMN.

Abstract

Technological advancement requires that organizations make available your information in digital format. However, there is the need for appropriate measures to keep this information secure and support the access control information prioritizing safety. View the processes that demonstrate how this security is held, may allow a better understanding, otherwise examine them, as well as a possible productivity gain. This course conclusion work aims at modeling and optimizing of processes involving the handling of information security incidents occurred in this public institution of higher education. Will be used to approach management of business processes to optimize the treatment processes of information security incidents occurred in this institution, some represented in this work, to illustrate how this process can be reproducible using the BPMN notation for modeling processes to meet the desired goals. The modeling will be validated by the team responsible for handling such incidents of the institution. With the modeling and optimization performed aims to: develop a standardized way to deal with these incidents , enabling the reduction of rework saving resources of the organization and identify whether there are ways to implement alternatives to improve the management of treatment processes such incidents. This paper presents the results of modeling of treatment processes for information security incident that demonstrated to be feasible. Thus demonstrating the work and feasibility of the proposed standardization of the treatment processes of information security incidents handled by the security staff of this institution. And proposing improvements to current processes with the implementation of tools for automating activities such as reporting, as well as the automatic alarm anomalies.

Key-words: Information Security, Process modeling, BPMN.

Lista de ilustrações

Lista de tabelas

Lista de siglas

2PTISI Processo Padrão de Tratamento de Incidente de Segurança da Informação

3PTISI Provável Processo Padrão de Tratamento de Incidente de Segurança da Informação

AIRT *Aplication for Incident Response Teams*

BPM *Business Process Management*

BPMN *Business Process Management Notation*

CAIS Centro de Atendimento de Incidentes de Segurança

CERT.br Centro de Estudos Respostas e Tratamento de Incidentes de Segurança no Brasil

CORE Coordenadoria de Redes Infraestrutura e Suporte

CERT *Computer Emergency Response Team*

CSI/NTIC Coordenador de Segurança em Informação do Núcleo de Tecnologia em Informação e Comunicação

CSIRT *Computer Security Incident Response Team*

DBIR *Data Breach Investigations Report*

DDA Dispositivo de Detecção Automática

ER Engenharia de Requisitos

ERS Equipe de Rede e Suporte

IDS *Intrusion Detection System*

ISI Incidente de Segurança da Informação

JANET *Academic Computer Network Emergency Response Team Joint*

NTIC Núcleo de Tecnologia da Informação e Comunicação

PSS Sistema de Produto-Serviço

PTISI Processo de Tratamento de Incidente de Segurança da Informação

RISI Repositório de Incidente de Segurança da Informação

RISK *Research Intelligence Solutions Knowledge*

RT *Request Tracker*

RTIR *Request Tracker for Incident Respost*

SDIEs Sistema de Detecção de Intrusão de Estações

SDIRs Sistema de Detecção de Intrusão de Redes

SIMPEP Simpósio de Engenharia de Produção

STIC Setores de Tecnologia da Informação e Comunicação

TCC Trabalho de Conclusão de Curso

TISI Tratamento de Incidente de Segurança da Informação

UNIPAMPA Universidade Federal do Pampa

VERIS *Verizon Enterprise Risk and Incident Sharing*

Sumário

1 Introdução

O avanço tecnológico exige que as organizações disponibilizem suas informações em âmbito digital para adaptarem-se e terem como se igualar em termos de oportunidade e abrangência as demais organizações (LOPES, 2002).

Há a necessidade de oferecer suporte ao controle de acesso às informações, priorizando a segurança das mesmas, sem impedir o acesso e em determinados casos permitir que se possam fazer as alterações devidas ou quando necessário, sua exclusão, mesmo elas estando em ambiente virtual (FILHO, 2004).

Considerando que a informação seja um conjunto de dados, podendo gerar valores a organização, deve-se considerar que a perda dos mesmos possa acarretar danos ao patrimônio da organização. Portanto é necessário assegurar que as informações estejam seguras em cada momento de seu manuseio (FONTES, 2006).

A informação estando em forma virtual facilita o acesso, manuseio e distribuição, entretanto permite que possa ser interceptada por alheios, causando um incidente de segurança. A partir da virtualização das informações elas agora podem ser acessadas de qualquer parte do mundo desde que se tenha acesso a equipamentos adequados e permissão de acesso a estas informações. Com tantas facilidades as políticas para a segurança das informações devem garantir que as mesmas estejam disponíveis, integras e confiáveis.

Visualizar os processos que demonstram a realização desta segurança pode permitir um melhor entendimento e até mesmo outra forma de examinar estes processos de segurança assim como um possível ganho de produtividade.

1.1 Motivação

Havendo o tratamento de incidentes de segurança da informação no Núcleo de Tecnologia da Informação e Comunicação (NTIC) pertencente à Universidade Federal do Pampa (UNIPAMPA), e não havendo uma definição dos processos que envolvem o tratamento deste tipo de incidentes faz-se necessário a modelagem destes processos.

Sendo um dos requisitos solicitados por Flora (2010), que podem ser observados na Tabela 1 referente aos requisitos e ferramentas necessárias para o aprimoramento da segurança da informação nesta instituição.

Na Tabela 1 a coluna **Prioridade** faz uma classificação das tarefas de acordo com a prioridade de implementação para o aprimoramento da segurança da informação.

Nesta tabela quanto mais baixo for o valor (zero ou próximo do zero), maior grau

Tabela 1 – Check-list de Requisitos e Ferramentas.

Tarefas	**Prioridade**
Instalação de um servidor central para armazenar os logs	0
Implantação de Sistemas para monitorar sistemas críticos e anormalidades	1
Reformulação da rede da Universidade incluindo a troca do NAT por IP válido	2
Criação de grupo de Resposta e Tratamento de Incidentes de Segurança	3
Implantação de sistema para gerenciar tarefas e incidentes de segurança	4
Definição do processo de Tratamento de Incidentes de Segurança	5
Definição da Política de Segurança da Informação	6
Definição da Política de Uso Aceitável	7
Criação de outras normas e procedimentos de segurança	8
Implantação de sistemas de detecção	9

Fonte: Adaptado de Flora (2010).

de importância a atividade terá para o aprimoramento do Tratamento de Incidente de Segurança da Informação (TISI) Flora (2010).

A motivação para a definição deste trabalho é a possibilidade de poder contribuir com a instituição de ensino que faço parte. Tendo como possibilidade a definição de um Processo Padrão de Tratamento de Incidente de Segurança da Informação (2PTISI) para a equipe do NTIC.

Tendo apresentado as motivações para a escolha deste tema para ser apresentado neste Trabalho de Conclusão de Curso (TCC), a próxima seção será para apresentar as metodologia e objetivo deste TCC.

1.2 Metodologia e Objetivos

Será utilizada a abordagem de gestão de processos de negócios para a otimização dos Processo de Tratamento de Incidente de Segurança da Informação (PTISI), utilizando a notação BPMN na modelagem dos processos para atender aos objetivos almejados.

Um dos objetivos que se tenciona realizar com este TCC é a modelagem de processos que envolvem o TISI ocorridos nesta instituição pública de ensino superior.

Outro objetivo deste trabalho é suprir à necessidade existente para a definição de um 2PTISI.

Com a definição deste 2PTISI possibilitar a socialização do conhecimento entre a equipe responsável pelo TISI, novos membros desta equipe, assim como não membros. Como por exemplo em casos que se tenham de explicar o trabalho realizado para pessoas de fora desta equipe.

Possibilitar a diminuição do retrabalho pela equipe. Assim possibilitando uma economia de recursos para a organização.

E ainda pode ser citada a possibilidade de identificar se há meios para implementar alternativas para aprimorar o gerenciamento dos PTISI.

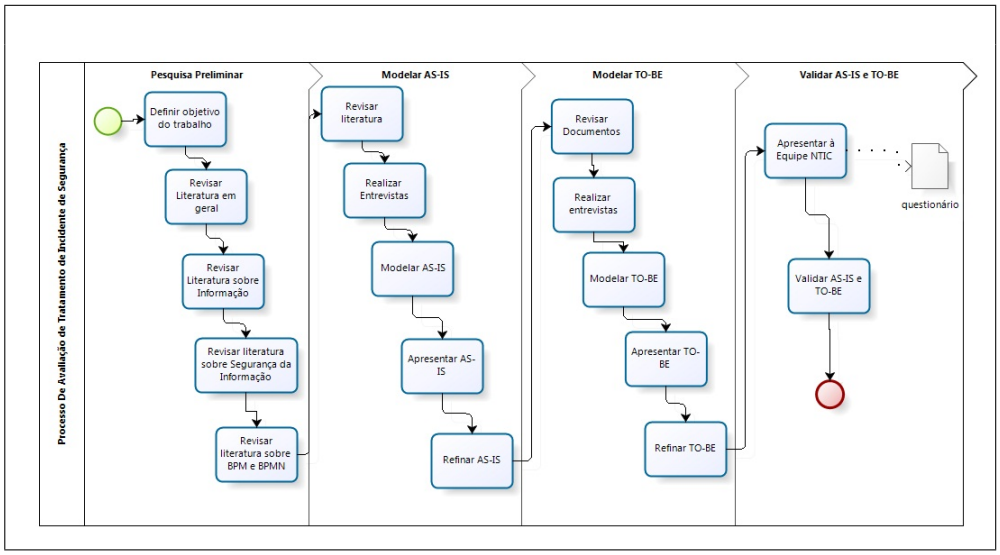
Para que estes objetivos sejam atingidos serão realizadas entrevistas com os responsáveis pelo TISI, e pesquisa a documentações de tratamento deste tipo de incidente.

Será observado como a informação esta sendo manuseada no contexto da segurança no NTIC, da UNIPAMPA, localizado no campus Alegrete. E a partir do estudo deste tratamento, gerar a modelagem do Provável Processo Padrão de Tratamento de Incidente de Segurança da Informação (3PTISI) e conforme aprovação e validação obter o 2PTISI.

1.3 Fluxo de atividades

Este TCC será realizado com a divisão do mesmo em quatro etapas distintas que pode ser vista na Figura 1.

Figura 1 – Cronograma das atividades realizadas.



Fonte: autoria própria.

Como pode ser observado na Figura 1 as quatro etapas definidas, assim na primeira etapa será realizada as pesquisa preliminares referente aos assuntos abordados neste TCC.

Na segunda etapa será realizada os processos necessários para a realização da modelagem AS-IS. Na terceira etapa será realizado os processos para a modelagem TO-BE, e na quarta etapa os processos necessários para a validação destas modelagens.

1.4 Estrutura

A apresentação deste TCC esta divido em capítulos, onde serão descritas a introdução e os conceitos dos princípios envolvidos para o desenvolvimento deste TCC, assim

como as tecnologias utilizadas para o desenvolvimento deste trabalho.

No capítulo 2 é abordado o conceito sobre segurança da informação, incidente de segurança da informação, exemplos destes incidentes, repositórios de incidentes de segurança e alguns sistemas de detecção de intrusos.

No capítulo 3 há a introdução da a abordagem *Business Process Management* (BPM) e da modelagem BPMN. O capítulo 4 apresenta trabalhos relacionados ao estudo de BPM e BPMN.

O capítulo 5 apresenta as modelagens dos processos de tratamento de incidentes de segurança que ocorrem no NTIC UNIPAMPA.

O capítulo 6 apresenta os resultados desta modelagem e o capítulo 7 apresenta as conclusões deste trabalho de conclusão de curso.

2 Segurança da Informação

O conceito de segurança da informação é dado por Sêmola (2003, p. 43) como: "[...] uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

Já Fontes (2006, p. 11) define a segurança da informação como sendo um "[...] conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão alcançada.

Garantir que uma informação esteja segura significa que a mesma segue requisitos mínimos de segurança, que possam evitar que ela possa ser danificada, alterada, interceptada entre outras ações que a tornam pouco confiáveis.

Autores como Sêmola (2003) e Fontes (2006) citam três principais requisitos que uma informação deve possuir para que seja considerada segura:

- Disponibilidade: garantia da disponibilidade da informação, quando solicitada.
- Integridade: garantia de que a informação esteja com seu conteúdo intacto e correto.
- Confidencialidade: garantia de que a informação esteja disponível apenas aqueles que tenham autorização ao mesmo.

A informação estar disponível, estar integra e ser confiável são atributos fundamentais de uma informação segura, mas não são os únicos. Sêmola (2003) as caracteriza como sendo os principais atributos de segurança da informação, as bases, e a partir destas bases haverem outros atributos que garantem que as informações sejam mantidas ou consideradas seguranças. Um destes atributos é o **não repúdio** ou **irretratabilidade** que é a garantia de que quem teve acesso, alterou, excluiu ou criou uma informação, não o possa negar. Outro atributo mencionado por Sêmola (2003) é a **Legalidade**, uso da informação de acordo com as regras da organização a que pertence assim como da legislação vigente.

Com a evolução da tecnologia, e o aumento gradativo da dependência a mesma, cada vez mais as organizações tendem a tirar proveito das vantagens tecnológicas. Entretanto há a necessidade de manter as informações, disponíveis, integras e confiáveis em ambiente virtual. Ambiente este que pode ser acessado de qualquer lugar independente de suas fronteiras, podendo ser pensado como um mundo sem lei (NÓBREGA, 2013).

Sendo assim, é necessário que haja regulamentos (políticas, regras ou normas) de como proteger estas informações, minimizando possíveis ocorrências de incidentes de

segurança da informação. Fontes (2006, p. 3) argumenta sobre as vantagens para a organização em se ter estes regulamentos e o uso destas informações de uma forma estruturada, pois "[...] possibilita que o negócio não seja prejudicado por um mau uso da informação: seja por erro ou por acidente".

Tendo conceituado segurança da informação na sequência é descrito o conceito de incidente de segurança da informação e apresentado alguns dos componentes que estão envolvidos em um incidente desta natureza.

2.1 Incidente de Segurança da Informação

Um incidente de segurança da informação é definido pelo CERT.br (1998) como sendo: "Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores".

Semelhante a isto Sêmola (2003, p. 50) define como: "[...] fato (evento) decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação [...]".

Desta forma para atender ao objetivo deste trabalho, será utilizado um esquema visual de incidente de segurança da informação. Este esquema é apresentado no *framework Verizon Enterprise Risk and Incident Sharing* (VERIS) produzido pela Verizon.

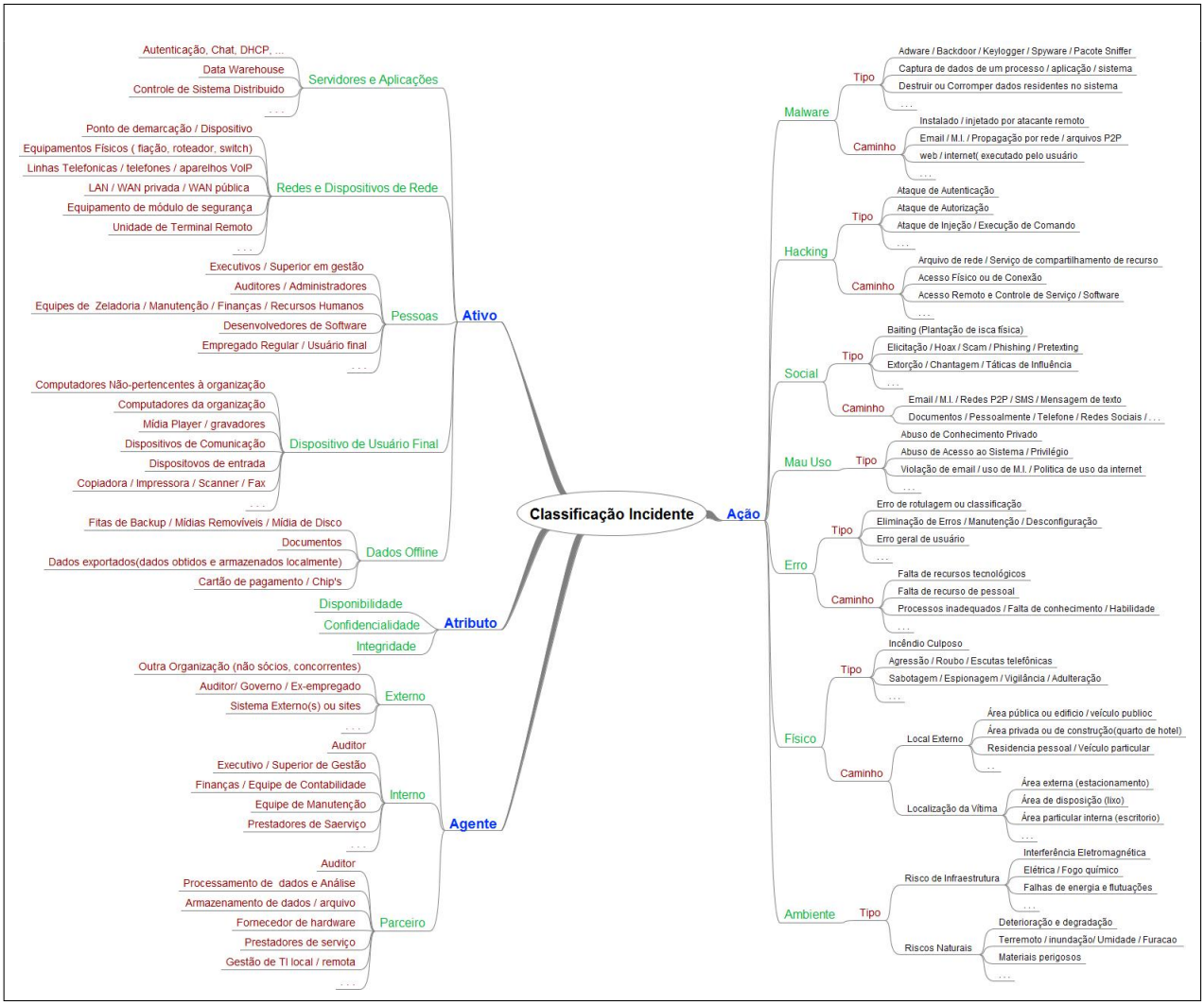
A *Verizon Communications* é uma companhia americana líder global no fornecimento de inovação em comunicação, informação e entretenimento, especializada em telecomunicações, sediada em Nova Iorque. Constituída em 2000 com a fusão da *Bell Atlantic Corp* e *GTE Corp Verizon*, duas grandes marcas internacionais na prestação de serviço. A Verizon tem mais de cem milhões de clientes espalhados por todo o mundo, incluindo o Brasil. No Brasil atua a partir da Terramark sua mais nova subsidiária. (VERIZON, 2012), (VERIZON, 2013) e (EVEF, 2012).

A equipe de segurança da Verizon, *Team Research Intelligence Solutions Knowledge (RISK)*, precisava analisar e avaliar os milhões de registros de violação de dados produzidos a cada ano, com o intuito de produzir o seu *Data Breach Investigations Report* (DBIR) - Relatório de Investigações de Violação de Dados. Assim em 2010 a Verizon desenvolveu o seu quadro de métricas VERIS. Este quadro VERIS permite que os dados dos contribuintes da comunidade VERIS, com informações sobre incidentes de segurança possam ser agregados e analisados no mesmo formato. Esta estrutura usa uma linguagem comum e um processo estruturado e repetitivo permitindo que as organizações classifiquem com objetivos definidos os incidentes de segurança. O VERIS desde o seu lançamento foi constantemente modificado e aperfeiçoado até a sua versão atual, que hoje é utilizado para o compartilhamento de dados de incidentes de segurança (BRUMFIELD, 2013).

Portanto VERIS (2010) é um conjunto de métricas projetadas para fornecer uma linguagem comum para descrever incidentes de segurança da informação em empresas, de uma forma estruturada e reproduzível.

A Figura 2 é um mapa mental resumido do VERIS de maio de 2012.

Figura 2 – Classificação de Incidente de Segurança da Informação.



Fonte: Adaptado de VERIS (2010).

A Figura 2 demonstra esta interação entre os quatro elementos, A ação e suas classificações principais, os principais atributos de segurança da informação, agente e suas 3 categorias e o ativo e suas classificações. No anexo deste trabalho, a Figura 36 representa o VERIS, de maio de 2012, este quadro de classificação de incidente de segurança da informação, representa a classificação dos incidentes, como o da Figura 2 entretanto com maior número de detalhamento em suas classificações e uma maior especificação de elementos.

O domínio de incidentes de segurança da informação pode ser representado visu-

almente com o quadro de intersecção das ameaças, ativos, ações e atributos. A versão de maio de 2012 do VERIS, proporciona a visualização do incidente relacionado com estes quatro elementos. Neste TCC este mapa será utilizado para auxiliar na compreensão de como as partes envolvidas em um incidente de segurança da informação normalmente estão interligadas.

No decorrer deste trabalho haverá uma breve descrição destes quatro elementos envolvidos em um incidente de segurança da informação e seus papeis nele.

- Atributo - qual o atributo da organização sera afetado pela ação.
- Agente - cujas as ações afetam o ativo de uma organização.
- Ativo - propriedade da organização que é afetado pela ação.
- Ação - incidente em si, que afeta o ativo da organização.

Com a utilização deste quadro de classificação pode-se classificar incidentes simples ou complexos, e o mesmo incidente podendo gerar um ou mais quadro de classificações dependendo da classificação feita pelos seus elementos. Assim sendo necessária uma melhor classificação destes elementos para futuras classificações.

2.1.1 Atributo

Esta ramificação, do quadro de classificação de incidentes, denominada **Atributo** refere-se aos princípios básicos que uma informação deve possuir para que seja garantida a classificação de informação segura: **Confidencialidade**, **Integridade** e **Disponibilidade**.

Apesar da importância dos mesmos, apenas eles não são suficiente, Sêmola (2003), agrega a eles outros princípios como a **Autenticidade**, garantia de quem esta manipulando a informação, a **Legalidade**, estar de acordo com as regras da organização e das leis vigentes, assim como: **Autorização**, **Auditoria**, **Autenticidade**, **Irretratabilidade** e outras.

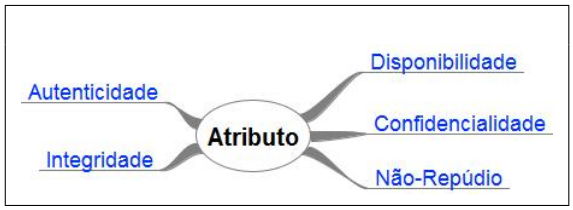
A Figura 3 é uma representação de alguns destes atributos, conceitos básicos da segurança da informação, que definem que uma informação esteja segura.

Como demonstrado na Figura 3 foi visto a classificação do atributo de uma informação em uma organização. Na próxima seção será comentado sobre o elemento agente.

2.1.2 Agente

Em um incidente de segurança da informação, obrigatoriamente haverá um agente. O **Agente** refere-se a entidade(s) ou indivíduo(s) que causaram ou contribuíram para

Figura 3 – Atributos de segurança da Informação.



Fonte: Adaptado de VERIS (2010).

que o incidente ocorra independente de ser voluntariamente ou não. Podendo haver mais de um agente envolvido em qualquer incidente. O papel do agente pode ser malicioso, intencional ou acidental, direto ou indireto. VERIS (2010) reconhece três categorias principais de agentes de ameaça: **externo**, **interno** e **parceiro**.

A identificação de qual o tipo especifico do agente, ajuda a avaliar os recursos, capacidade e tendências do mesmo e os recursos que o mesmo tem como atingir em relação à organização. Sendo que cada uma das categorias do elemento agente inclui sub categorias.

2.1.2.1 Agente Externo

Agentes externos compõem as ameaças provenientes de fontes externas à organização e sua rede de parceiros. São exemplos destes agentes externos desde *hackers*, grupos criminosos organizados, entidades governamentais, assim como eventos ambientais, como clima e terremotos. Sua principal característica seria que de forma normal e aceitável, nenhuma confiança ou privilégio seriam designadas a estes agentes. Uma descrição de como o agente contribuiu para o incidente, pode distinguir entre atos deliberados ou não-intencionais e entre ação direta ou indireta sobre a parte do agente.

No VERIS, onde há uma estrutura com maior nível de detalhes, pode se apresentar a origem e/ou local (origem geográfica) do agente externo.

2.1.2.2 Agente Interno

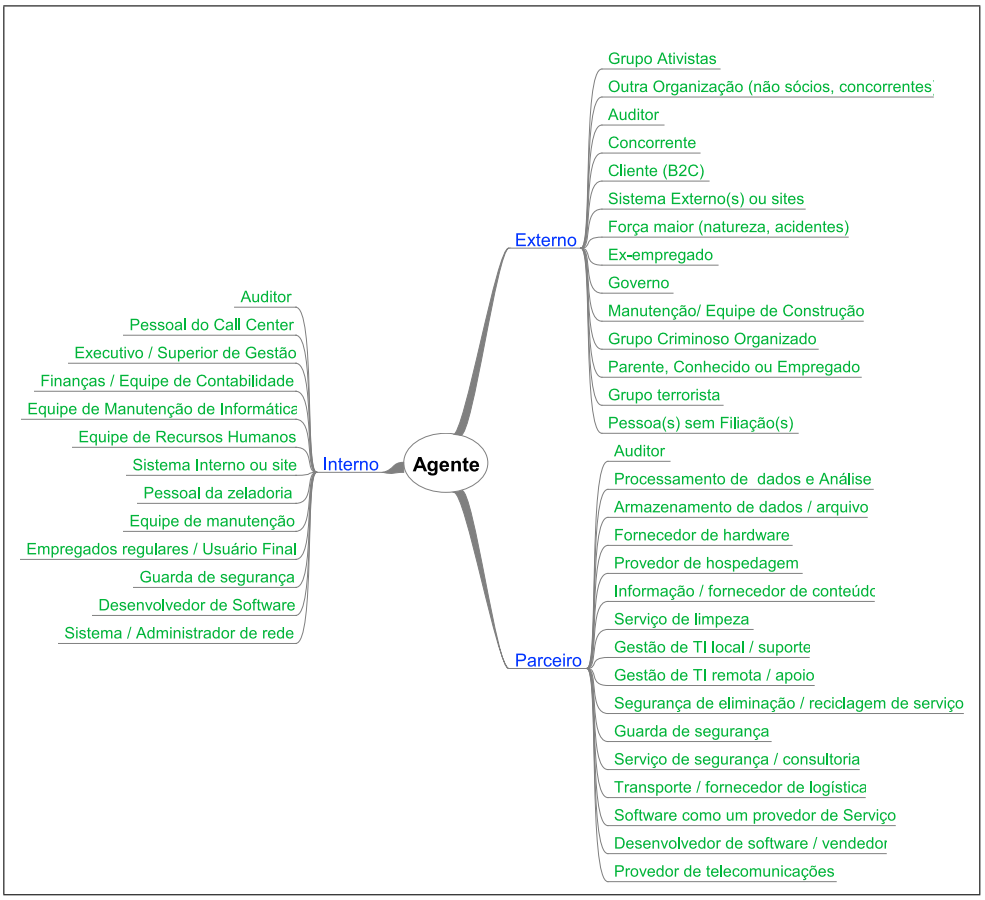
Agentes internos são ameaças originárias de dentro da organização. Não apenas funcionários como todos aqueles que possuem acesso à organização assim como as informações a qual ela abrange, independente do seu nível de liberdade. São exemplos destes casos, os executivos da empresa, funcionários, contratados independentes (terceirizados), estagiários e outros. Na categoria de agente interno, cabe ainda, de não menos importância, os sistemas internos da organização.

2.1.2.3 Agente Parceiro

O **agente parceiro** definido por pessoas ou grupos que tem uma relação de negócios com a organização. Exemplos destes agentes são os fornecedores, vendedores, fornecedores de hospedagem, suporte de TI terceirizados, e outros. Geralmente há níveis de segurança implícito entre parceiros de negócios. Identificar o tipo específico do parceiro (ou do serviço prestado) envolvido em um incidente de segurança da informação ajuda a avaliar e gerenciar riscos em lidar com terceiros.

A Figura 4 é uma representação desta classificação, tendo o agente como centro desta classificação e sua divisão realizada com seus sub elementos (agentes parceiros, internos e externos).

Figura 4 – Classificação de Agente



Fonte: Adaptado de VERIS (2010).

Como pode ser observado na Figura 4 foi realizada a classificação do agente de um incidente. Esta classificação é definida pela relação que o agente tem com a organização. Por exemplo, o auditor, que neste exemplo aparece tanto como agente interno, externo e parceiro, um único cargo, dependendo da relação que a organização tem com o mesmo. Entretanto, independente de qual tipo de agente seja este auditor, em teoria, o agente

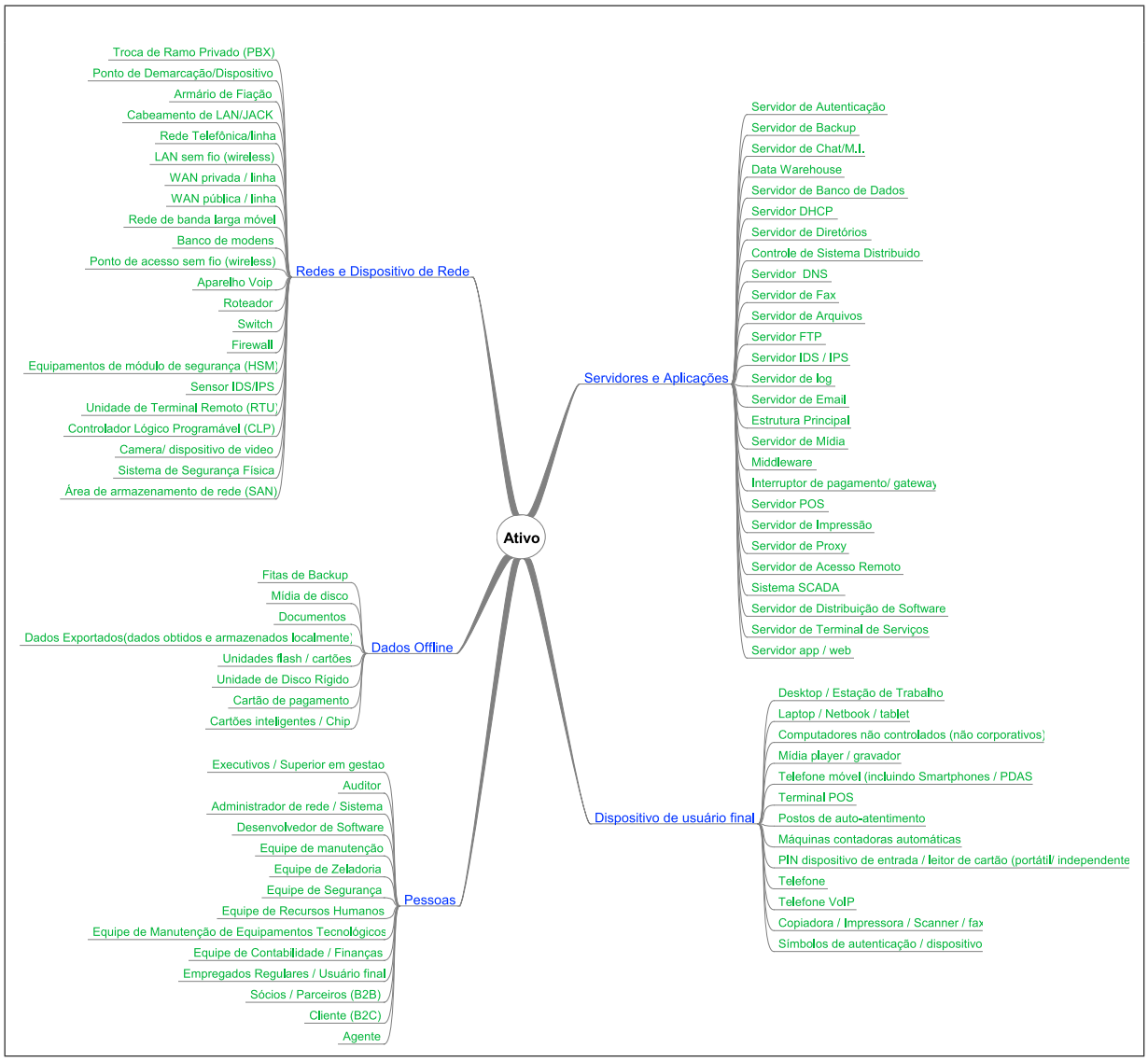
auditor, tem direito a acesso ao mesmo nível de informação. Na próxima seção há o resumo do ativo.

2.1.3 Ativo

Ativo são as posses e responsabilidades da organização que sofre com o incidente, podendo ser classificado desde objetos, como fios e equipamentos como também seus funcionários, responsabilidade da organização de inegável importância e valor.

A Figura 5 demonstra esta classificação.

Figura 5 – Ativo



Fonte: Adaptado de VERIS (2010)

Como pode ser observado na Figura 5 a classificação de ativo de uma organização está dividida em 5 classes: Servidores e Aplicações; Redes e Dispositivos de Redes; Dados

Offline; Dispositivos de Usuários finais, os produtos da organização e Pessoas, responsabilidades da organização. Na próxima seção será comentado sobre o elemento ação.

2.1.4 Ação

A **Ação** descreve o que o agente da ameaça fez, ou contribui, para causar a violação de alguma das propriedades de segurança da informação. Normalmente existem várias ações durante um cenário de violação. VERIS (2010) utiliza sete classificações de ações, para cada classificação há divisões das mesmas em sub elementos podendo variar desde o tipo, especificação do caminho que ela percorreu para atingir a organização, ou outras classificações relevantes.

Abaixo uma breve descrição das sete principais ações que ameaçam uma organização: ***Malware***, ***Hacking***, **Engenharia Social**, **Uso Indevido**, **Física**, **Erro** e **Ambiental**.

Malware Software ou código desenvolvido com a finalidade de comprometer ou prejudicar outros softwares sem o consentimento, até mesmo o conhecimento, do proprietário (CERT.BR, 1998). Exemplos destes incluem vírus, *worns*, *spyware*, *keyloggers*, *backdoors*, entre outros. Eles podem ser classificados de diversas maneiras, VERIS (2010) observa a distribuição do *malware* (seu caminho) e qual sua função.

A classificação de alguns destes *Malware* é descrita por CISCO (2006, p. 3) como sendo:

> Normalmente, os vírus, *worms* e *spyware* introduzem-se numa empresa por correio eletrônico ou aplicações de mensagens instantâneas, por transferências *Web* ou por transferências de ficheiros, embora possam ocorrer ataques sofisticados por meio de serviços móveis sem fios ou serviços de sistema operativo

Hacking Atividade de *hackear* sistemas com o objetivo de vasculhar a procura de falhas e vulnerabilidades para tirar proveito das mesmas (WENDT; JORGE, 2012).

Engenharia Social Qualquer organização é composta por seres humanos, e seres humanos estarão sempre necessitando de outros seres humanos, esta relação pode ser o elo frágil da organização. Podendo ser a partir desta **socialização** entre seres humanos pode as vezes acarretar em perigo a segurança da informação da organização. Pois o conjunto de técnicas com o propósito de induzir a vítima de modo que a mesma forneça dados pessoais ou execute tarefas ou aplicativos de interesse de outros é definido como engenharia social (WENDT; JORGE, 2012).

Uso Indevido Sendo que seres humanos trabalham nas organizações, deve se ter regras e regulamentos para a manipulação das informações, mas nem sempre estes regulamentos

são bem estabelecidos ou estão claros e ao alcance de todos. Podendo ser de uso de material ou informação da organização, podendo ser um descarte incorreto ou um mau uso de equipamento.

Físico Refere-se a ações visíveis e/ou táteis, que podem colocar em risco a segurança da informação.

Erro Refere-se ao não seguimento dos regulamentos da organização por não se ter conhecimento ou por equivoco.

Ambiental São ações que não podem ser evitadas ou previstas. Entre estes está a perda de informações devido a chuvas e inundações. Esta classificação resumida dos elementos da ação e seus sub elementos pode ser observada na Figura 6.

Na Figura 6 pode se observar os elementos da ação, em sua maioria divididos entre o tipo e o caminho que esta ação teve ao se infiltrar na organização. Diferenciando apenas na ação de Mau Uso, onde se diferencia apenas pelo seu tipo.

Na próxima seção será apresentado exemplos de como esta classificação dos elementos ajuda na classificação de incidentes de segurança da informação.

2.2 Exemplos de Classificação de Incidentes de segurança da Informação

Alguns exemplos usando o quadro de classificação de incidentes de segurança da informação podem ser observados em VERIZON (2010), onde há exemplos de como esta classificação é realizada. Na sequência dois destes exemplos.

Furto de Fitas de *Backup* Este exemplo trata de um incidente de segurança da informação que envolve o furto de fitas de *backup* contendo informações de uma organização. O mapa deste incidente de segurança pode ser observado na Figura 7, onde se vê as interações que ocorre entre a ação, o atributo, o ativo e o agente neste incidente.

Neste exemplo prático da classificação de um incidentes de segurança da informação mostrado na Figura 7, onde há a classificação de um incidente de segurança da informação envolvendo o furto de fitas de *backup* contendo o histórico hospitalar. Ocorreu quando um administrador de TI de um hospital da América do Norte, estava a caminho das instalações externas da instituição, com o intuito de entregar as fitas de backup do dia, porém, com fome, decidiu parar em uma lanchonete. Este estacionou seu carro e entrou no estabelecimento, ao voltar para o veículo, constatou que uma das janelas estava quebrada, e as fitas que continham os prontuários de cerca de 60.000 pacientes, desaparecidas.

Figura 6 – Ação

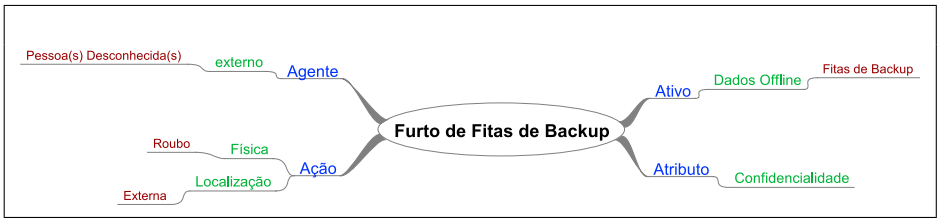
Fonte: Adaptado de VERIS (2010).

Neste mapa apresentado na Figura 7 mostra as interações que ocorre entre a ação, o atributo, o ativo e o agente deste incidente. Onde pode-se observar a participação de agente(s) externo(s) desconhecido(s) que participaram direta e deliberada na subtração do ativo da organização. Rompendo com um dos principais atributos da segurança da informação: a **confidencialidade**.

Outro exemplo de classificação de incidente de segurança da informação é definido em Ataque de Injeção SQL.

Ataque de Injeção SQL Este exemplo de classificação de incidente de segurança da informação descreve um ataque estrangeiro ao sistema de uma organização. Neste exemplo foi descrito que vários ataques de Injeção SQL foi realizada a uma aplicação *web* voltados

Figura 7 – Furto de Fitas de *Backup*.

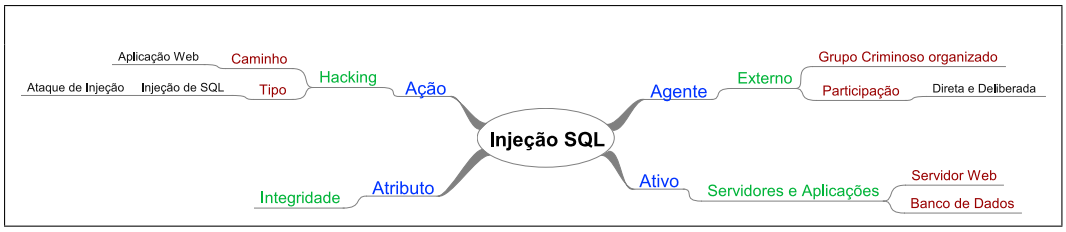


Fonte: Adaptado de VERIZON (2010).

ao público. Com os ataques foi possível introduzir *Keyloggers* e *sniffers* nos sistemas internos da empresa alvo. Os *keyloggers* capturaram várias credenciais de domínio, que os atacantes utilizaram para se infiltrar na rede corporativa. Com os pacotes *sniffers* os dados foram capturados por vários meses, em que o atacante recolhia periodicamente as informações armazenadas.

Neste incidente é possível a modelagem de 3 mapas utilizando o modelo do VERIS (2010), a Figura 8 mostra o mapa deste incidente de segurança da informação pela perspectiva de uma ação por *Hacking* e a quebra do atributo de integridade.

Figura 8 – Injeção de SQL



Fonte: Adaptado de VERIZON (2010).

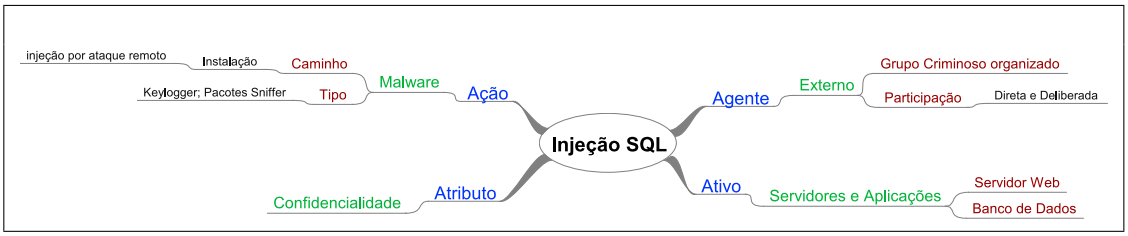
Na Figura 8 , pode se observar a interação entre os elementos do incidente. Esta ação, um ataque de injeção de SQL, com agentes externos, organização criminosa estrangeira, tendo uma participação direta e deliberada, para prejudicar a organização em questão. Os ativos, servidores e aplicações, tiveram sua integridade abalada.

Na Figura 9 observa-se este mesmo incidente de segurança da informação, tendo em foco a ação que provocou o incidente como: *Hacking* e o atributo atingido: a confidencialidade.

Já a Figura 10 mostra uma outra fase deste mesmo incidente de segurança da informação.

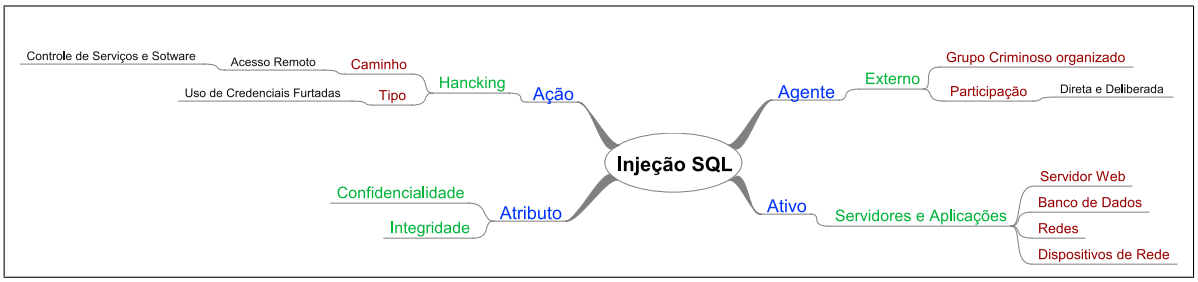
Como pode ser observado nas Figuras 8, 9 e 10 que demonstram que um único incidente de segurança da informação, dependendo do incidente, pode ser causado por diversas ações, ter vários atributos de segurança quebrados, danificar diversos ativos, mesmo tendo o mesmo agente que o provocou.

Figura 9 – Injeção de SQL: Ação Hacking



Fonte: Adaptado de VERIZON (2010).

Figura 10 – Injeção de SQL. Atributos



Fonte: Adaptado de VERIZON (2010).

Uma vantagem de se ter um quadro de métricas de incidentes de segurança da informação, além da visualização da interligação destes elementos, e a descoberta do caminho das ações percorridas pelo(s) agente(s) causador(es) da ação. Com este quadro se pode ter uma base de ações para prevenir futuros incidentes como os ocorridos ou ainda definição de ações para parar o incidente de segurança da informação.

Tendo apresentado os elementos envolvidos em incidentes de segurança da informação e exemplos da classificação destes incidentes, na próxima seção será apresentado alguns métodos de detecção automática destes incidentes e alguns repositórios que auxiliam as equipes que tratam deste tipo de incidente a encontrar soluções para os mesmos.

2.3 Repositórios de incidentes de segurança da informação

Esta seção tem como foco a apresentação de conceitos que envolvem um Repositório de Incidente de Segurança da Informação (RISI). Um RISI geralmente são constituídos de algum aplicativo *web* e um banco de dados. Nesta seção será apresentado alguns destes RISI.

2.3.1 Best Pratical

A organização *Best Pratical Solutions LLC* é a criadora do *Request Tracker* (RT). Definido por Bone (2006) "[...] RT é um conjunto de ferramentas de topo de linha cus-

tomizável para qualquer número de tarefas e fluxos de trabalho com um núcleo baseado na idéia de rastrear qualquer coisa". Assim como o *Request Tracker for Incident Respost* (RTIR) é definido como sendo "[...] um produto especialmente concebido para componentes computacionais para auxiliar nas resposta a incidentes de segurança da informação usando as ferramentas fornecidas pelo RT".

Best Pratical foi fundada para agregar valor a base dos usuários de RT, fornecendo desenvolvimento personalizado e suporte aos usuários. Esta organização fundada em outubro de 2001 por Jesse Vincent, autor do RT esta localizada em Somerville, Massachusetts, Estados Unidos (BEST, 2002).

No site do BEST (2002) há a descrição do seu programa como sendo "[...]RT para Resposta a Incidentes ajuda aos Centro de Estudos Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br) ou *Computer Security Incident Response Team* (CSIRT) a controlar eficientemente incidentes de segurança de informação. Projetado em colaboração com equipes de resposta a incidentes de topo, o RTIR foi construído com base no RT para ajudar a gerenciar todo o fluxo de trabalho a partir de relatório de incidente para investigação e suas resoluções."

Esta ferramenta surgiu pela necessidade de se trabalhar com um volume cada vez mais crescente de notificações de incidentes de segurança, a exigência de uma triagem destes incidentes, assim como um incremento automático do número destes incidentes (BEST, 2002).

Nesta ferramenta o fluxo de trabalho inicia-se com a triagem dos recebimentos dos relatórios de incidente, ligando-os com incidentes já relatados ou criando um novo tópico. Cada incidente é projetado para manter o controle de tudo o que é necessário saber para resolver o problema. Podendo ser acompanhado os procedimentos realizados para resolver o incidente (BEST, 2002).

Características desta ferramenta Algumas das importantes características desta ferramenta podem ser encontradas em BEST (2002):

- A informação crítica estar disponível e em um só lugar. Depois do RT estar instalado, pode ser acessado de qualquer dispositivo, pois é uma aplicação *web*, independente de plataforma. Podendo haver interação via email com o repositório.

- Personalizável para cada organização. Os Tickets (bilhetes, códigos, chave primária, ou como for definido pela organização) podem ser definidos a escolha da organização, de forma que faça sentido para a mesma. Assim como a lógica e o fluxo do trabalho podem ser definidas pela organização, usando os tickets, ciclos de vida, campos personalizados, aprovações e extensões. Com a possibilidade de mais de 15 idiomas

e permitindo que a própria organização crie/altere algum componente para melhor gerir seu trabalho.

- Interface móvel para *iPhone*, *Android*, e dispositivos *WebOS*;
- Gráficos de relacionamento;
- Apoio PGP *Seamless* para criptografar, descriptografar, assinar e verificar emails enviados e recebidos;
- Relatórios de Incidentes. Podendo haver datas para o término do trabalho com um incidente. Os incidentes serão exibidos no painel do RTIR. Os relatórios dos incidentes ainda em aberto, sendo trabalhados, depois da data limite podem ser transformados em novos incidentes ou ligados a incidentes já existentes. Vários relatos de um mesmo incidente podem ser agrupados a um mesmo incidente, ajudando a reduzir a duplicação. Os relatórios podem ser gerados a partir de textos, HTML, ou relatórios de planilhas, podendo ser sobre o número de incidentes, seus tipos e resoluções, assim como para qualquer período de tempo;
- Toda a informação relevante do incidente está incluída automaticamente quando se inicia uma nova etapa do processo de tratamento de incidente;
- Extração automática do IP;
- Compatível com IPv4 e IPv6.

Ferramenta de Pesquisa Para a realização de pesquisa, há uma ferramenta auxiliar, a RTFM, uma ferramenta de gestão de conhecimento, integrada ao RT, que permite que a organização possa capturar e compartilhar as informações coletadas dos incidentes. Os Tickets usados para registrar os incidentes, com o RTFM eles podem abrir, categorizar e pesquisar os arquivos existentes. Podendo adicionar novas informações a Tickets já fechados e fazer consultas aos mesmos (BEST, 2002).

2.3.2 *Remedy* ARS

A ferramenta *Remedy* ARS baseada na IMAP, foi usada pela *Academic Computer Network Emergency Response Team Joint* (JANET)-*Computer Emergency Response Team* (CERT), antes de ser substituída por RTIR. Esta ferramenta não possui manutenção, e era projetada para times pequenos de tratamento de incidente, ou seja, poucas notificações de incidentes, com exigência de interação manual para cada mensagem recebida. Com suporte a poucas plataformas, e dificuldade de interação com ferramentas externas e impossibilidade de vários funcionários trabalharem em paralelo no mesmo incidente (BONE, 2006).

2.3.3 AIRT

O site AIRT (2005) define o *Aplication for Incident Response Teams* (AIRT) como sendo

> AIRT é um aplicativo *Web*, projetado e desenvolvido para suportar o dia-a-dia de uma equipe de resposta a incidentes de segurança informação. O aplicativo suporta processamento altamente automatizado de relatórios de incidentes e facilita a coordenação de vários incidentes por um centro de operações de segurança.

Este aplicativo é construído com PHP4 e o banco de dados PostgreSQL, tem como público alvo os grupos de resposta a incidentes de segurança. Desenvolvido pelo Laboratório de Informática da Universidade de Tilburg em 2005.

O lançamento da versão 20.090.221.1 foi lançada em 2009. Algumas características desta nova versão são (AIRT, 2005):

- A capacidade de fazer submissão de arquivos e anexá-las a incidentes;
- Implementar recursos de apoio;
- Incluiu a capacidade de receber emails e vinculá-lo a incidentes;
- Capacidade de receber de rede, eleitorado e informações de contato através da fila de importação;
- Ao executar em um site com SSL, é possível usar um certificado de cliente para autenticação;
- Adicionado um nome descritivo para casos; entre outras.

2.3.4 Rutgers

A RUTGERS - *State University of New Jersey* é uma das principais universidades de pesquisa nacional dos Estados Unidos, é uma preeminente instituição pública estadual de ensino superior. Rutgers é dedicada ao ensino que atende aos mais altos padrões de excelência, para a realização de pesquisas que inova, e para prestação de serviços, soluções e cuidados clínicos. Foi fundada em 1766 e foi a oitava universidade fundada nos Estados Unidos (RUTGERS, 2010).

Esta universidade utiliza o RTIR com acesso restrito aos seus membros. O acesso ao `https://rt.ips.rutgers.edu` é restrito a Runet. A Universidade Rutgers emprega um modelo de segurança distribuído o RU CIRT. O RU CIRT revisa relatórios de incidentes e os despacha para a equipe do departamento de informática para a resolução. Em outras palavras, notificação e coleta de dados são centralizados enquanto execução e resolução são descentralizadas (RUTGERS, 2010).

2.3.5 Veris

O quadro de métricas Veris, produzido pela Verizon, já comentado neste texto e utilizado para produzir os mapas de interseção entre ativo, agente, ação e atributo também é um repositório de incidente de segurança da informação. Podendo ter seus arquivos baixados e instalados, permite o compartilhamento do conhecimento das atividades para o tratamento de incidentes (VERIS, 2010).

Nesta seção foram apresentados alguns dos repositórios de incidente de segurança da informação. Na seção seguinte será apresentada alguns sistemas de detecção de intrusos, ferramenta que auxiliam sa segurança da informação.

2.4 Sistema de Detecção de Intrusos

Soriano (201?) descreve um *Intrusion Detection System* (IDS) como sendo "[...] uma espécie de sistema de gestão de segurança para computadores e redes", os IDS foram desenvolvidos em uma tentativa de diminuir os ataques em sites e redes. Os IDS consistem em um conjunto de ferramentas que analisam informações de diversas áreas dentro de um computador ou uma rede para identificar possíveis falhas de segurança, incluindo uso indevido (ataques de dentro da organização) assim como a intrusos (ataques de fora da organização) (SORIANO, 201?).

Laufer (2003) define os objetivos dos IDS como sendo "[...] para indicar que alguma tentativa de intrusão foi feita no sistema". Desta forma há dois tipos de detecção: os baseados na rede, que "[...] observam todo os dados trocados entre estações"; e os baseados na estação,"[...] monitoram os dados em uma determinada máquina".

Os IDS geralmente são classificados dependendo de onde seus dados são coletados, podendo ser pela rede, estação ou híbridos, união dos dois.

Sistema de Detecção de Intrusão de Redes Laufer (2003) os descreve como sendo "[...] pacotes são capturados e é feita uma análise em cada um deles para verificar se este está dentro de padrões pré-determinados ou não, indicando respectivamente tráfego normal ou uma tentativa de ataque".

Sistema de Detecção de Intrusão de Estação Laufer (2003) descreve os Sistema de Detecção de Intrusão de Estações (SDIEs) como tendo sido um dos primeiros sistemas de detecção de intrusão implementados. Sendo o seu objetivo o de "[...] monitorar toda a atividade existente em uma estação específica. O funcionamento desses sistemas se dá através da coleta e análise de dados originados em uma máquina que hospeda um serviço. Depois de coletados, esses dados podem ser analisados localmente ou até enviados para uma máquina remota responsável pelo exame".

Híbrida Laufer (2003) as define como sendo uma configuração que utilizaria ambos os sistemas, usando um "[...] Sistema de Detecção de Intrusão de Redes (SDIRs) para a rede local e SDIEs rodando nos servidores principais".

Algumas destes sistemas de detecção de intrusos são descritos abaixo:

HoneyPots Leobons (2012) descreve como sendo "[...] sistemas usados para enganar *hackers* expondo vulnerabilidades conhecidas deliberadamente". Atraindo possíveis intrusos com a intenção de catalogar suas investidas e assim descobrir suas ações e técnicas.

Syslog-ng ng (2013) descreve como sendo "[...] uma aplicação de código aberto para implementação de padrão de registro *syslog*. O protocolo *syslog* original permite que mensagens sejam classificadas com base apenas em prioritárias/instalação pares; *syslog-ng* adiciona a capacidade de filtrar com base no conteúdo da mensagem usando expressões regulares".

Arpwatch Madeira (2008) descreve como sendo:

> *Arpwatch* é uma ferramenta que monitora a atividade em uma rede *ethernet*, mantendo atualizada uma tabela com endereços *ethernet* (MAC) e seus respectivos endereços IP. Essa ferramenta tem a capacidade de reportar via email certas mudanças. O *Arpwatch* é uma ferramenta importante na monitoração da rede contra ataques de *Arp Poisoning* ou *Arp Spoofing* usados para realizar ataques mais sofisticados como *Man-in-the-Middle* (MITM).

Logwatch Conforme o Ubuntu (2013) "[...]*Logwatch* é uma ferramenta que irá monitorar os *logs* do seu servidor e enviar email ao administrador em uma base diária", sendo um analisador de log poderoso e versátil. *Logwatch* é projetado para dar um relatório unificado de toda a atividade em um servidor, que pode ser entregue através da linha de comando ou email.

Swatch swatch (2013) define esta ferramenta de código aberto como sendo "[...] um utilitário que monitora arquivos de *log* do sistema, filtra dados indesejados e realiza ações específicas (envio de email, a execução de um *script*, etc) com base no que ele encontra nos arquivos de *log*". Assim *Swatch* pode ser usado para configurar *snort* para enviar os alertas como email.

Snort snort (2013) define *Snort* como sendo "[...] uma rede de prevenção de intrusão de código aberto e sistema de detecção (IDS/IPS) desenvolvido pela *Sourcefire*. Combinando os benefícios de assinatura, protocolo e inspeção baseada em anomalias, *Snort* é o mais amplamente implantado IDS/IPS tecnologia em todo o mundo".

Nessus Documentation (2013) descreve que *Nessus* pode digitalizar todos os *hosts* em uma rede, e tentar determinar a lista de seus serviços e pontos fracos rodando *plugins*, pequenos programas que estão a cargo de uma única sonda. Algumas vezes comportando-se da mesma forma que *hackers*.

Tendo apresentado alguns conceitos segurança da informação, incidentes de segurança, exemplos de incidentes, exemplos de RISI e de sistemas de detecção de intrusos, na próxima seção serão apresentadas a abordagem BPM e a sua modelagem BPMN, utilizados para modelar os processos de tratamento de incidentes abordados neste TCC.

3 Modelagem de Processos de Negócios

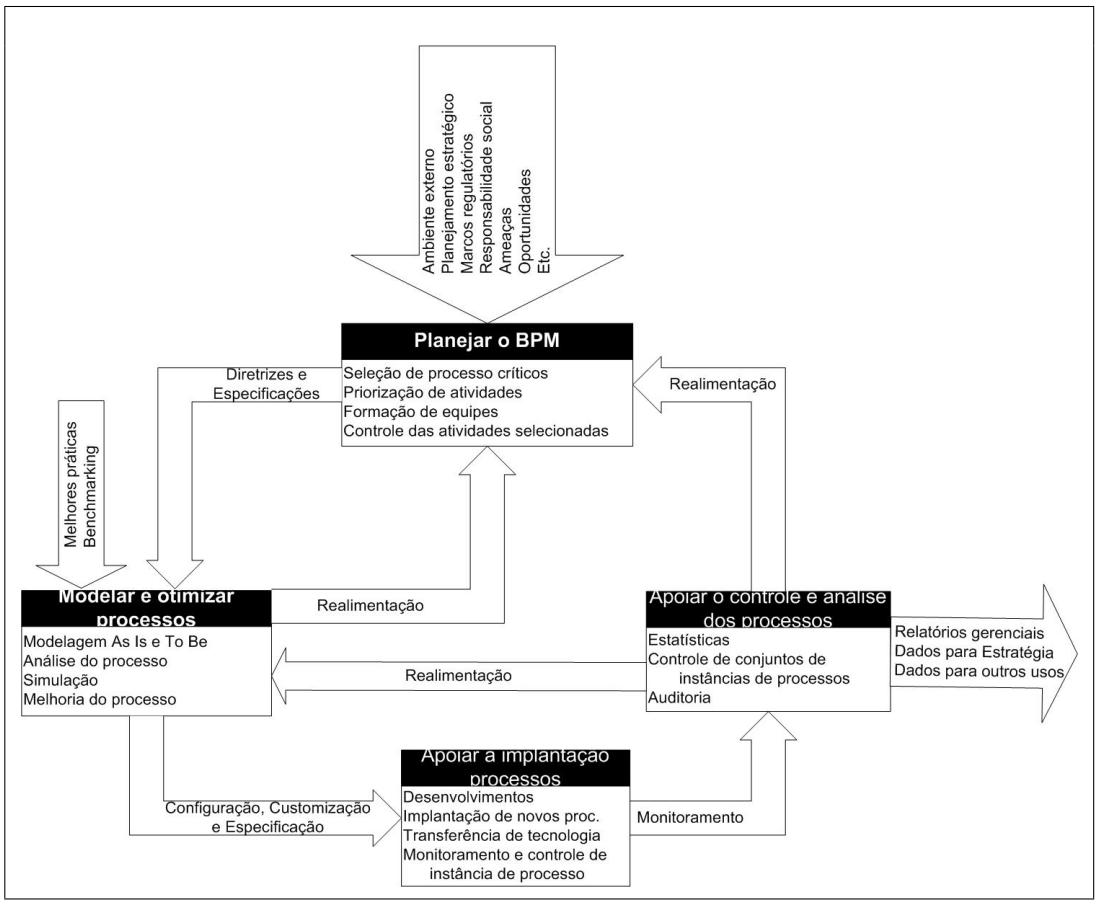
Esta seção foca na descrição de BPM e BPMN para modelar o processo de tratamento de incidentes de segurança da informação.

3.1 *Business Process Management* - BPM

CRUZ (2010, p. 66) define BPM como sendo: "[...] um conjunto de múltiplos elementos, conceitos e metodologias que existe há algum tempo com a finalidade de tratar de forma holística processos de negócios".

O Modelamento de processos de negócios BPM, tem por objetivo não só gerenciar os processos para agregar valor à organização, como também a melhoria continua dos processos, principalmente através de seu redesenho e análise.

Figura 11 – Ciclo de Gerenciamento BPM



Fonte: Adaptado de BALDAM (2009).

O conceito BPM, que une gestão de negocio e tecnologia da informação tem o

foco na otimização dos resultados das organizações por meio de melhoria dos processos de negócio. Para tal ocorrer, são utilizados métodos, técnicas e ferramentas (ABPMP, 2009) .

A Figura 11 apresentada por BALDAM (2009) contempla um ciclo de gerenciamento de BPM que, dentre as suas etapas, prevê a etapa de modelagem e de otimização de processos.

Na etapa de modelar e otimizar o processo, representada na Figura 11, uma das técnicas que podem ser utilizadas é a modelagem BPMN. Que será vista em outra seção. Entretanto, de acordo com BALDAM (2009) na metodologia BPM, pode-se dividir a modelagem de um processo em dois estados distintos. O primeiro estado é quando se busca modelar a situação em que se encontra um dado processo, mapeando e modelando assim o seu estado atual, também chamado de estado AS-IS. Tendo realizado esta modelagem é possível verificar oportunidades de melhoria no processo e definir então como pode ser uma versão otimizada do processo, modelando então o seu estado futuro – também definido como estado TO-BE.

Havendo a necessidade de modelar um processo, seus primeiros passos serão a análise do processo atual, para sua modelagem. O objetivo desta análise é criar uma visualização, juntamente com um texto pertencente ao mesmo. Assim podendo determinar as possíveis áreas de melhoria. Baseado em BALDAM (2009), algumas das atividades que estão envolvidas no AS-IS e no TO-BE estão descritas na Tabela 2.

No estado atual (AS-IS), um cenário real do processo em si, com seus erros, e também pode se projetar um cenário ideal (TO-BE), não que este seja implementado, porém o cenário atual é o ideal para uma otimização do processo.

Tabela 2 – Atividades de Modelar e Otimizar Processos.

Modelar processos para a situação Atual AS-IS	**Modelar processos para a situação Futura TO-BE**
Compreender os processos atuais (atuação, falhas, expectativas e outros); Documentar os processos; Prover dados de integração entre processos; Quando possível, comparar o modelo com melhores práticas e *benchmarking* de referência Definir e priorizar soluções para os problemas atuais;	Empregar metodologias para otimizar os processos; Fazer simulações inovações e redesenho; Definir mudanças nos novos processos; Adotar quando possível e/ou necessário, as melhores práticas e modelos de referência; Gerar especificações para a implantação, execução e controle; Realimentar o planejamento do BPM.

Fonte: Adaptado de BALDAM (2009)

Observando a Tabela 2 verifica-se alguns passos necessários para a modelagem de processos de negócio em uma organização. Na próxima seção será apresentado o conceito de BPMN bem como alguns de seus principais elementos. Uma notação que auxilia a

modelagem dos processos de negócios.

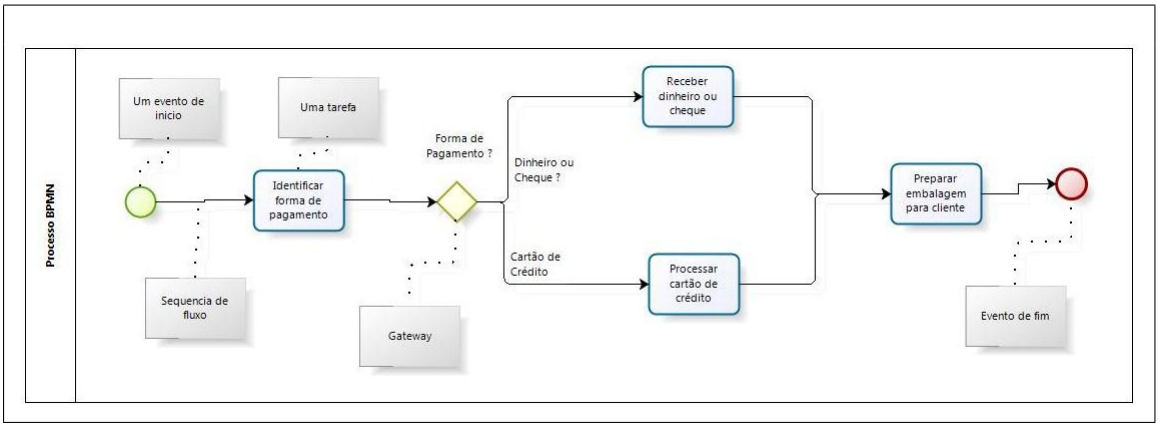
3.2 BPMN

Uma das técnicas da notação de BPM é a modelagem BPMN. O Modelo Padrão de Processo de Notações de Negócios - BPMN, desenvolvido pela *Object Management Group*, com o principal objetivo de fornecer uma notação que seja de fácil compreensão por todos os usuários de negócios. Desenvolvido a partir dos rascunhos iniciais criados pelos analistas de negócios, ate chegar aos gerentes dos negócios. Assim conforme OMG (2011) "[...] BPMN cria uma ponte padronizada entre o desenho de processo de negocio e a implementação do processo".

Conforme NETO (2009, p. 53), BPMN "[...] trata-se de uma técnica especialmente voltada para a definição e documentação de processos de negócios com padrões de notação bem definidos".

Alguns dos principais elementos da notação BPMN são os eventos de início e de fim do processo e as tarefas que são interligadas por fluxos de sequência e *gateways*, conforme pode ser verificado na Figura 12.

Figura 12 – Notação de Modelagem de Negócios



Fonte: Adaptado de VALLE e OLIVEIRA (2009).

Na figura 12, há um exemplo de um diagrama de processo definido pela notação BPMN (CAMPOS, 2013), (GARCIA; CUVILLIER, 2009) e (CRUZ, 2010). As atividades são representadas por retângulos e as decisões por losângulos. Os círculos, preenchido e vazio, representam, respectivamente o início e o fim de processos, assim como as setas representam o fluxo, destas atividades um "vai para onde".

Com foco na notação BPMN, que conforme VALLE e OLIVEIRA (2009) trata-se de "[...] uma técnica de definição e documentação de processos de negócios com padrões

definidos", tenciona-se apresentar o estado atual da segurança da informação do NTIC, e o estado esperado, depois de sua otimização.

Na próxima seção há exemplos deste estudos de casos referentes a modelagem de processos utilizando a notação BPMN.

4 Trabalhos Relacionados

Este capítulo abordara alguns trabalhos que vieram validar a pesquisa realizada. A pesquisa foi realizada por trabalhos relacionados na modelagem de processo utilizando a notação BPMN. Alguns destes trabalhos estão descritos abaixo.

4.1 Aplicação da Modelagem de Processos de Negócios em Sistemas Produto-Serviço

Um artigo apresentado no XVII- Simpósio de Engenharia de Produção (SIMPEP), escrito por BARROS, FERREIRA e TOLFO (2010), relata um estudo de caso que utilizou a modelagem BPMN para a representação dos processos de negócios que formam um Sistema de Produto-Serviço (PSS).

BARROS, FERREIRA e TOLFO (2010) descrevem o PSS como sendo "[...] um modelo de economia onde a produção e o consumo estejam voltados para a redução de utilização de materiais e prevaleçam modelos de negócio que focam o comércio da utilização de produtos ao invés da aquisição do mesmo".

Este estudo de caso foi baseado em uma empresa, líder de mercado, de produção e venda de eletrodomésticos.

Esta empresa criou um modelo de negócio no qual o purificador de água não é mais vendido e sim instalado na casa do consumidor mediante o pagamento de uma assinatura mensal pela utilização do mesmo.

Com este modelo de negócio, a empresa e o cliente constroem um vínculo, onde a empresa fornece atendimento perante um chamado do cliente. Como pode ser observado na Figura **??**.

Na Figura **??** é apresentado os passos desde o momento em que a empresa recebe o chamado do cliente, até a finalização deste do atendimento a este cliente.

O trabalho teve êxito em seu propósito sendo concluído como BARROS, FERREIRA e TOLFO (2010) descrevem "[...] adoção de uma visão por processos em modelos de negócios PSS representa uma alternativa para a análise de questões técnicas e econômica destes empreendimentos"sendo um dos principais motivos de aceitação desta modelagem neste tipo de processo "[...] possibilitar a integração dos processos de negócios com a tecnologia de informação".

4.2 Estudo exploratório utilizando BPMN em um processo de Engenharia de Requisitos

Esta apresentação de monografia escrita por SOARES e INSFRAN (2011), relata a utilização da notação BPMN nas fases dos projetos de Engenharia de requisitos. Desenvolvido a partir do estudo de um problema de um dos departamentos do instituto de ensino superior ao qual os autores pertencem. O problema relacionado ao processo de alocação de salas de aula para o semestre, processo este que não era completamente automatizado.

Neste trabalho uma das questões a serem respondidas sobre a viabilidade da proposta levantadas por SOARES e INSFRAN (2011) era se "[...] o BPMNpoderia modelar de forma precisa o processo de alocação de salas de aula ... nas distintas fases iniciais do processo de engenharia de requisitos?". Assim levantando a questão se "[...] a notação BPMN constitui um instrumento capaz de auxiliar as fases de engenharia de requisitos por meio dos cenários AS-IS e TO-BE".

Na etapa AS-IS deste trabalho pretendia-se organizar o processo de alocação de salas de aula para entendimento e futuro aperfeiçoamento do processo atual. Ao final do trabalho era esperado um aperfeiçoamento deste processo, ou seja, a modelagem TO-BE. Para obter os resultados esperados foram realizados levantamento iniciais do processo, identificação dos processos envolvidos, das atividades, e rotinas de trabalho por meio de entrevistas e reuniões.

Como resultado deste estudo obteve-se as modelagens AS-IS, a qual pode se observar na Figura 13, e a modelagem TO BE.

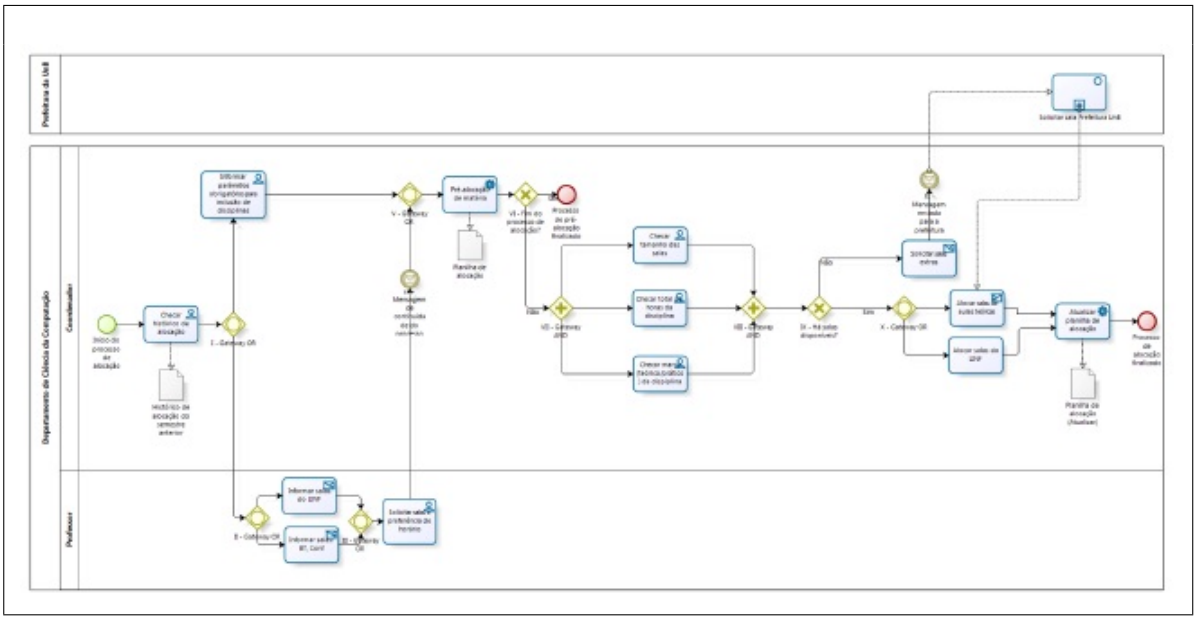
Na Figura 13 pode se observar como a alocação das salas é gerada a partir do coordenador, o mesmo tem como base para a organização das salas o histórico de anos ou semestre anteriores, assim como as requisições de cada matéria e de cada professor. Com base nestes e outros parâmetros tenciona-se a melhor alocação de salas por semestre.

O processo de alocação de salas foi modelado com êxito nas etapas AS-IS e TO-BE. Assim como foi abordada as fases do processo de Engenharia de Requisitos (ER). Sendo apontado como tendo mais relações com o BPMN as fases de elicitação, de análise de requisitos e de especificação. A tecnologia utilizada, no caso a notação BPMN, não influência na primeira etapa do processo de ER, o estudo de viabilidade.

Foi concluído neste estudo de caso que 4 das 5 etapas da ER foram abrangidas pela notação BPMN. Sendo por meio da notação BPMN que foi realizada a validação do processo de ER. Assim como o fato desta notação retratar de forma fiel o processo de alocação de salas de aula.

Abordado dois exemplos da utilização da modelagem BPMN e sua viabilidade, na

Figura 13 – Processos de alocação de salas de aula.



Fonte: Adaptado de SOARES e INSFRAN (2011).

próxima seção será demonstrado como foram realizadas as modelagens dos processos de tratamento de incidente da segurança da informação na instituição base de estudo.

5 Modelagem de Processos de Tratamento de Incidentes de Segurança da Informação do NTIC/UNIPAMPA.

Este trabalho envolve a modelagem de processos de tratamento de incidentes de segurança da informação do NTIC da UNIPAMPA. Nas seções seguintes será apresentado uma descrição do NTIC, equipe que trata dos incidentes de segurança da informação que ocorrem na UNIPAMPA. E em seguida os processos que envolvem o tratamento destes incidentes.

5.1 Núcleo de Tecnologia da Informação e Comunicação

Conforme NTIC (2010) o NTIC da UNIPAMPA é um órgão suplementar da Reitoria da universidade. O NTIC tem por objetivo, segundo seu regimento, "[...] criar e manter condições para o funcionamento sistêmico das atividades ligadas à tecnologia da informação e comunicação na Universidade, a fim de dar suporte ao desenvolvimento do ensino, pesquisa, extensão, gestão e serviços à comunidade".

É de competência do NTIC, o planejamento, a organização e controle das atividades que tenham relação com tecnologia da informação e comunicação. O NTIC possui a responsabilidade de manter e dar suporte aos sistemas de comunicação, como rede de dados e telefonia da universidade proporcionando assim, a infraestrutura de TI necessária para o desenvolvimento da universidade (UNIPAMPA, 2011).

Também compete a este órgão, a orientação dos setores de Setores de Tecnologia da Informação e Comunicação (STIC) das unidades universitárias e a aplicação das políticas da área de tecnologia da informação e comunicação da universidade (UNIPAMPA, 2011).

Conforme NTIC (2011) descreve "[...] ficam sob orientação do NTIC os STIC das Unidades quanto à aplicação das políticas, normas, padronizações e planejamento referente à área de Tecnologia da Informação e Comunicação da instituição". Ainda conforme NTIC (2011) "[...] os STIC's têm como principal finalidade planejar, organizar e executar as atividades necessárias ao atendimento das demandas locais de suporte e infraestrutura de tecnologia".

O NTIC desta instituição está fisicamente instalado junto ao prédio administrativo do campus de Alegrete, onde iniciou usa operação em 2007. Havendo planejamento para a construção de um prédio com estrutura suficiente para abrigar a infraestrutura

de servidores da universidade, assim como a equipe de trabalho, além de laboratório de pesquisa para testes e desenvolvimentos de novas tecnologias e sistemas (FLORA, 2010) .

Entre as atividades de suporte e infraestrutura de tecnologia, de responsabilidade do NTIC encontra-se a de prevenção e de tratamento de incidentes de segurança da informação.

Depois de ter sido realizado um breve relato da instituição UNIPAMPA e da equipe responsável pelo tratamento de incidentes de segurança da mesma, o NTIC, neste TCC será apresentado o tratamento de alguns incidentes de segurança da informação.

5.2 Tratamento de Incidentes

Sendo uma das atribuições do NTIC a prevenção e o tratamento de incidentes de segurança da informação. São relatado neste TCC as formas como o NTIC trata destes incidentes. Baseado em um estudo realizado por Flora (2010) e complementado por pesquisas e entrevistas realizadas junto ao grupo de segurança da informação, nesta seção é apresentada uma versão do PTISI realizado nesta instituição.

Com base nestes estudos preliminares pretende-se modelar o 2PTISI para o estado atual (AS-IS) e a partir deste, a otimização das atividades permitindo o desenvolvimento do 2PTISI do estado futuro (TO-BE) .

No decorrer deste estudo foram obtidos dois resultados, um mapa e a modelagem deste incidente, que serão mostrados no decorrer desta seção.

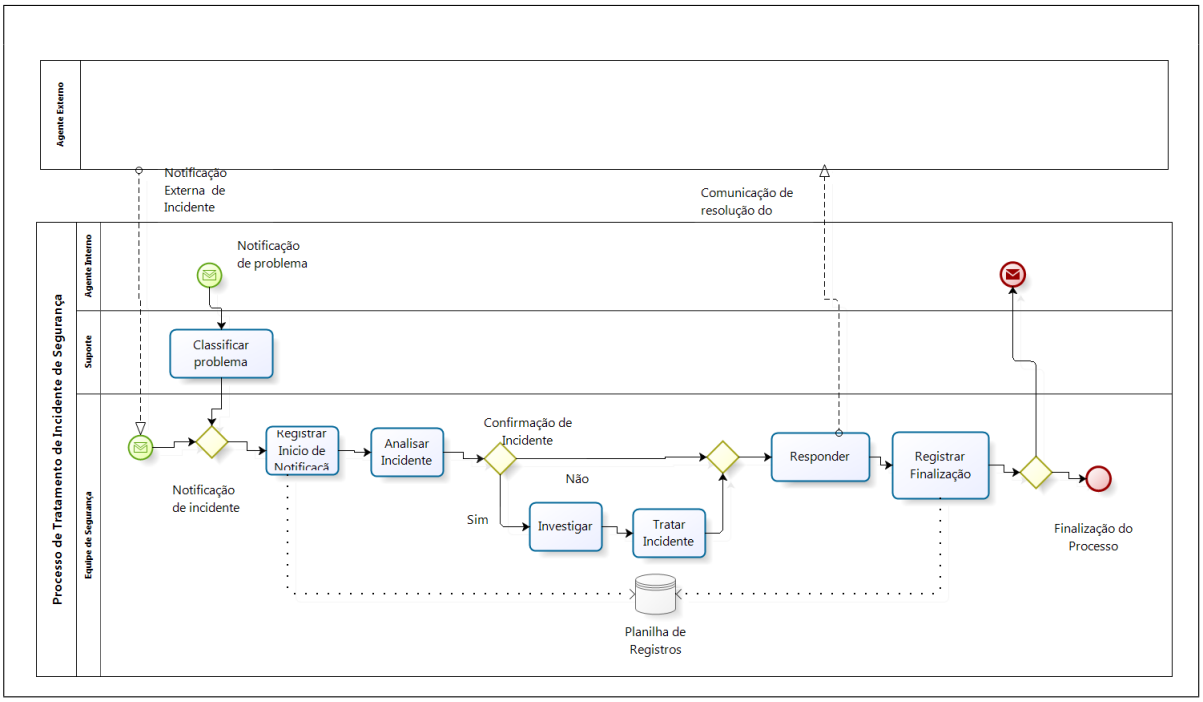
Fundamentado em Flora (2010), onde o mesmo descreve o TISI de Violação de *Copyrights*, que neste trabalho será descrito como Violação de Direitos Autorais. A equipe responsável pelo TISI da instituição objeto de estudo, que de agora em diante neste trabalho, será denominada apenas como equipe de segurança. A equipe de segurança ao receber o email com a comunicação do Centro de Atendimento de Incidentes de Segurança (CAIS) indicando a ocorrência deste incidente de segurança, começa a trabalhar neste incidente para que possa provar ou refutar sua ocorrência.

Baseado neste relato de Flora (2010) sobre o TISI foi desenvolvido o primeiro protótipo do 3PTISI representado na Figura 14.

Neste protótipo do 3PTISI há duas entradas: uma entrada é vinda do agente externo, que encaminha para a equipe de segurança a notificação através de email; a outra entrada é vinda a partir de um agente interno da instituição, que faz um chamado para a equipe de suporte, esta classifica é reencaminha para a equipe de segurança para o devido procedimento.

Sendo um dos intuitos deste trabalho a socialização do conhecimento entre os membros da equipe de segurança, assim como não membros. Portanto esta duplicidade

Figura 14 – Notificação Dupla de Incidentes.



Fonte: autoria própria.

de início de eventos, poderia causar dúvidas ao entender este 3PTISI. Além do que, os autores consultados neste estudo recomendam que um processo usualmente tem apenas um evento de início.

Portanto após refinamentos e entrevistas, ficou estabelecido que apenas um 3PTISI não era viável. Sendo constituído então dois 3PTISI: um para as notificações externas de ISI, realizadas por um agente externo, geralmente o CAIS; o outro para as notificações internas de ISI, podendo ser realizada por qualquer membro da instituição, agente interno (professores, alunos, funcionários, e outros).

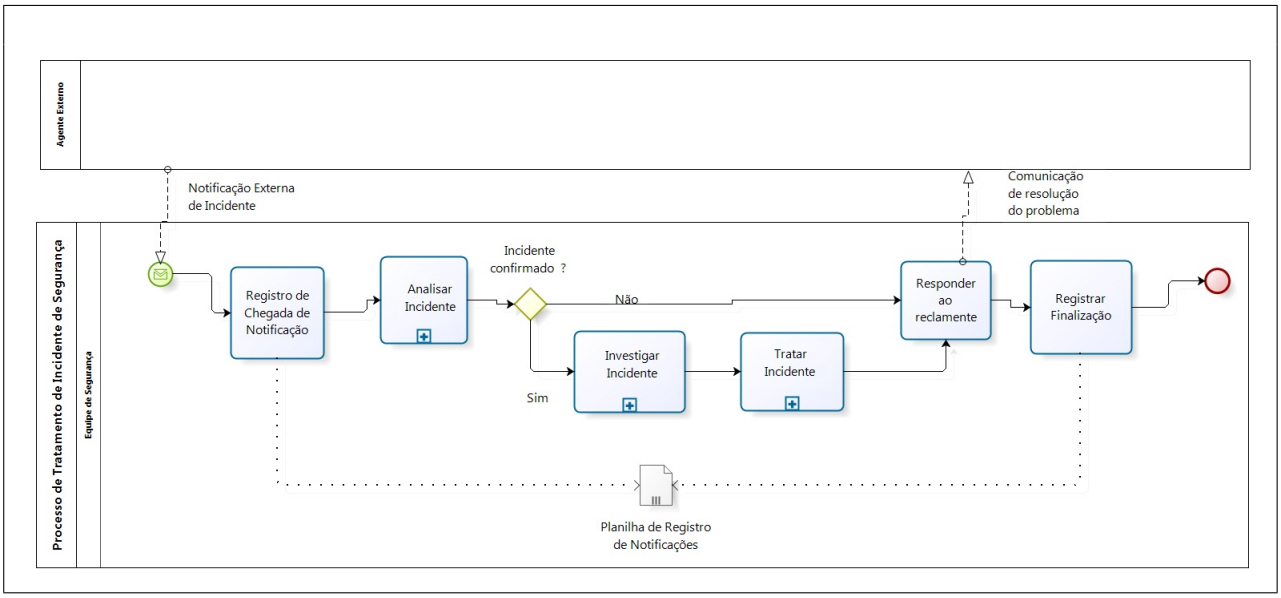
Assim sendo realizada as duas modelagens 2PTISI, na Figura 15 visualiza-se a modelagem realizada para notificações de incidentes por agentes externo à instituição.

Observando a Figura 15 nota-se que diferente da Figura 14 há apenas um elemento de início. Demonstrando que o processo inicia ao chegar um email vindo de um agente externo. Após a chegada da notificação, o fluxo do processo continua como no processo da Figura 14.

Na Figura 16 é apresentada a modelagem realizada para a notificação Interna de incidente de segurança. Novamente apontando como diferença o início do processo.

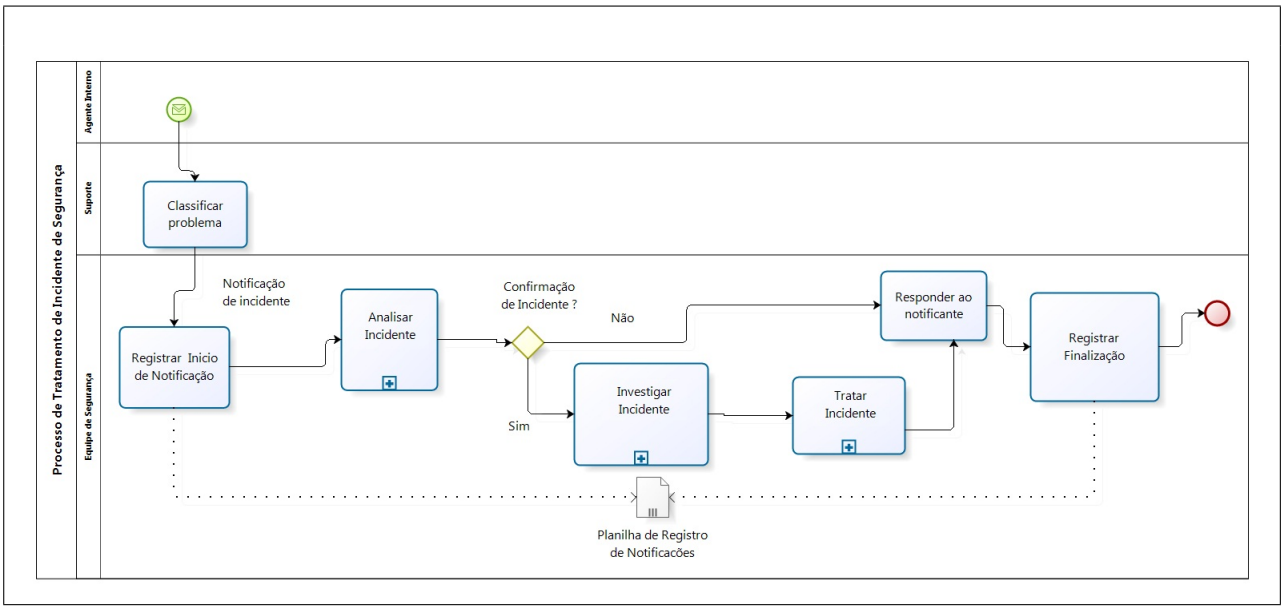
Após o recebimento da notificação, a equipe de segurança trata ambas as notificações da mesma maneira. Assim é realizado o registro da chegada da informação, em uma planilha eletrônica, que serve para a equipe como um registro de suas atividades.

Figura 15 – Notificação Externa da Modelagem AS-IS.



Fonte: autoria própria.

Figura 16 – Notificação Interna da Modelagem AS-IS.



Fonte: autoria própria.

Depois deste registro, a notificação passa para a etapa de **Análise de incidente**, onde será verificado se a notificação procede ou não. Caso não proceda é encaminhada uma resposta negativa ao agente que notificou o possível incidente de segurança, que neste trabalho será denominado de **reclamante**.

Caso na análise de incidente, as evidências vindas com o email, sejam provenientes da instituição, estas evidências são encaminhadas para a atividade de **Investigação do incidente**, onde se procurará descobrir mais evidências que possam refutar ou compro-

var este incidente. Se o mesmo é comprovado, as evidências coletadas na análise e na investigação do incidente passam para a atividade de **Tratamento de incidente**, onde se procurará formas de frear e/ou extinguir o incidente em si.

A fase de tratamento, assim que é finalizada, o responsável pelo tratamento do incidente gera um relatório do incidente, onde constará os passos realizados e os resultados obtidos. Depois da geração deste relatório é realizada a resposta ao reclamante, e a atualização da planilha de registro de notificação, que neste trabalho será denominada apenas como planilha, finalizando o PTISI.

Tendo como base o trabalho de Flora (2010), usar-se-á a notificação externa de incidente de violação de direitos autorais para descrever este processo com suas atividades e sub-processos. No trabalho base é descrito que uma notificação do CAIS chega à equipe de segurança via email, onde constam dados que serão úteis na identificação do possível responsável pelo provável incidente. Estes dados constantes no email referem-se ao *host*, equipamento computacional, identificado pelo número IP, data e hora do possível incidente, título, tamanho e URL proveniente do conteúdo, instituição que apontou o possível incidente, o reclamante. São com estes dados que a equipe de segurança terá de confirmar ou refutar o possível incidente.

Assim para testar o 3PTISI, foi utilizado o Processo de Violação de Direitos Autorais, que utilizará a modelagem já gerada que pode ser observado na Figura 15.

Utilizando-se a Figura 15 para a modelagem do 3PTISI pode-se agregar a esta modelagem as atividades que a equipe de segurança realizou desde a chegada do email, até a conclusão da investigação, sendo finalizada com resposta ao reclamante, com cópia anexa para o CAIS. Ao receber a notificação, neste caso uma notificação externa, a equipe de segurança registra na planilha os dados de chegada da notificação, assim como o responsável pela análise, investigação, tratamento e de resposta e os dados de finalização de registro da notificação.

Após o registro da notificação passa-se para a atividade de análise do incidente, neste caso, esta análise é realizada pela verificação se o IP que consta na notificação consta na IPTables da instituição.

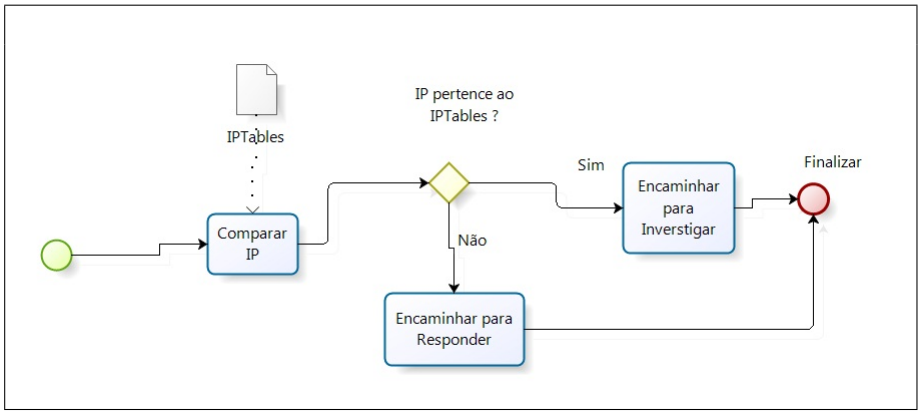
A instituição utiliza a técnica NAT, *Network Address Translation*, que é uma técnica que consiste em reescrever os endereços IP de origem, de dentro da rede, um IP inválido, por um endereço válido. Para assim poder fazer requisições para endereços da internet. Ao fazer a troca de IP válidos por inválidos e de IP inválidos por válidos, esta técnica armazena os IP em sua tabela, IPTable, que de agora em diante neste trabalho será chamada apenas de Tabela de IP's. Com este armazenamento, possibilita que NAT, saiba qual máquina fez uma requisição, para qual porta, data e horário.

No email proveniente do comunicante do possível incidente, consta o nome do

reclamante, a indicação de qual host (endereço IP), e qual violação cometeu, assim como as evidências de data, hora, nome do arquivo, tamanho, URL de onde fez o *download*, a solicitação de verificação do incidente, pedido de investigação, tomada de providências e resposta ao reclamante assim como cópia para o próprio CAIS.

A Figura 17 demonstra a comparação entre os dois IP's. Caso o IP notificado não conste na Tabela de IP's da instituição, a Análise do Incidente é encerrada comprovando a negação do incidente notificado.

Figura 17 – Notificação Externa - Sub-Processo de Análise de Incidente

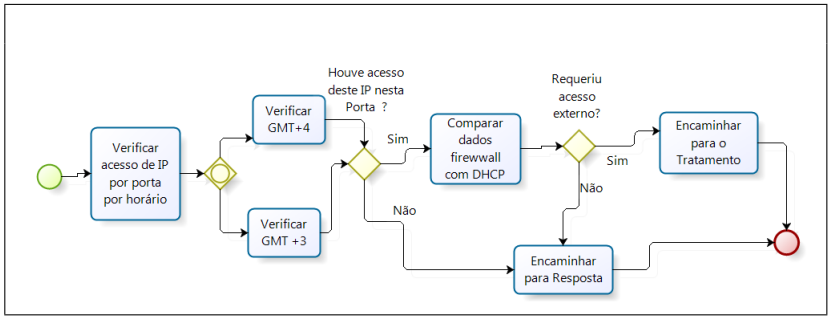


Fonte: autoria própria.

Na Figura 17 demonstra a comparação feita entre os IP's, o que consta no email do comunicante e algum que conste no Tabela de IP da instituição. Caso a comparação entre ambos resulte negativa, passa-se para a atividade de **Responder ao reclamante**, caso o contrário, esta informação é encaminhada para a atividade de investigação.

A Figura 18 demonstra como esta investigação foi realizada neste caso.

Figura 18 – Sub-Processo de Investigação de Incidente.



Fonte: autoria própria.

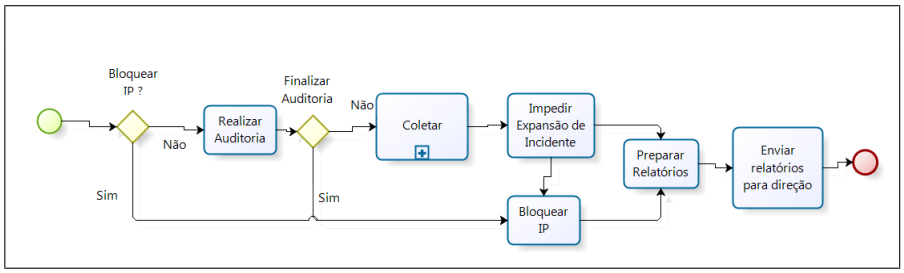
Na Figura 18 há a demonstração de como a investigação deste incidente foi realizada. Resultando na análise que o IP da notificação pertence ao IPTable da instituição faz-se necessária a Investigação do Incidente, onde se investigará outros dados constantes

na notificação para se comprovar o possível incidente. A verificação se o IP obteve acesso externo na porta indicada e no horário indicado são evidências que devem ser obtidas.

Neste caso, foi necessário verificar qual o horário GMT, o servidor da instituição estava trabalhando. O horário que consta na notificação do CAIS, esta em GMT 0, os servidores da instituição trabalham em GMT+3, horário normal e GMT+4, horário de verão. A confirmação obteve resultado positivo. Caso não tivesse havido acesso deste IP, nesta porta, em nenhum dos horários do servidor, a investigação seria finalizada e o processo encaminhado para a resposta ao reclamante com cópia ao comunicante. Entretanto houve confirmação de acesso externo realizado pelo IP, na porta indicada e no horário indicado, confirmado pelo servidor DHCP da instituição.

Com as evidências coletadas, assume-se que houve o incidente notificado. Agora com a confirmação do incidente a equipe de segurança precisa tomar as providências necessárias para o Tratamento do mesmo. Na Figura 19 há a demonstração das atividades seguidas pela equipe de segurança para o Tratamento deste incidente.

Figura 19 – Sub-Processo de Tratamento de Incidente.

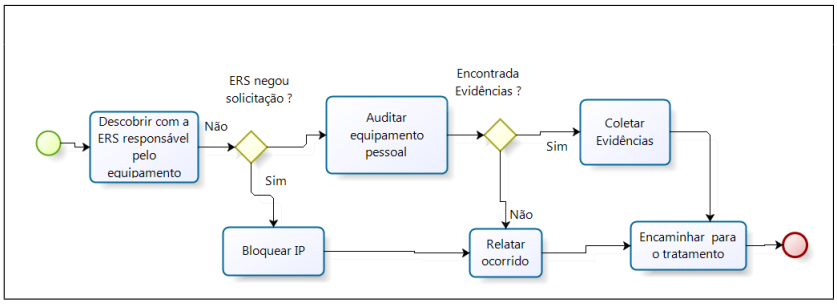


Fonte: autoria própria.

Conforme pode ser observado na Figura 19, a equipe de segurança teve a escolha de bloquear o IP causador do incidente. Com o propósito de realizar uma auditoria no equipamento registrado para este IP, a equipe de segurança preferiu não bloquear o IP. O não bloqueio foi o meio escolhido para não alertar o responsável, evitando que o mesmo pudesse eliminar qualquer evidência que pudesse estar armazena em seu equipamento, eliminando a possível coleta de evidências no equipamento de uso pessoal. A auditoria é realizada na busca de evidências que podem ser encontradas apenas no equipamento que foi utilizado no incidente. A Figura 20 demonstra as atividades realizadas na coleta de evidências no equipamento pessoal.

Na Figura 20 é demonstrada a interação entre a equipe de segurança e a Equipe de Rede e Suporte (ERS), é esta equipe que tem sob sua responsabilidade a tabela onde consta qual agente interno da instituição (aluno, funcionário, professor, e outros) tem acesso a qual IP da instituição. No decorrer das investigações e com a ajuda da ERS descobriu-se que um funcionário da instituição (agente interno) era o responsável pelo equipamento que utilizava o IP deste incidente em questão. Após obter o nome do res-

Figura 20 – Sub-Processo de Coleta de Evidência em Equipamento Pessoal.



Fonte: autoria própria.

ponsável pelo equipamento com a ERS, passa-se a auditar o equipamento do mesmo em busca de evidências que confirmem a autoria do incidente de segurança.

Foram realizadas as coletas de evidências no equipamento pessoal deste agente interno, e tomadas as devidas providências para que o impedimento da expansão do incidente, evitando que os dados que foram baixados sem autorização não fossem passado para outros. Neste momento ocorre o bloqueio do IP até que o responsável pelo equipamento tenha eliminado o conteúdo que obteve sem a devida permissão e, caso necessário, os softwares que utilizou para o mesmo. As atividades realizadas após a coleta de evidências no equipamento pessoal e bloqueio do IP do responsável, são internas a equipe de segurança: o preparo do relatório, seu envio para a direção e a resposta ao reclamante, com cópia ao comunicante (CAIS). Finalizando o processo com o registro na planilha do encerramento deste incidente de segurança da informação.

O agente interno da organização, ao baixar um conteúdo sem a devida autorização, violou o atributo de integridade da organização proprietária dos direitos autorais deste conteúdo. Neste caso o ativo de uma outra organização estava sendo manuseado. O atributo de integridade de outra organização foi corrompida, entretanto esta infração das regras internas, compromete também o atributo de confiabilidade da organização do caso de estudo.

A confiabilidade na organização de estudo deve ser protegida assim como a integridade de outras organizações, esta importância é salientada por Flora (2010) ao observar a importância da resposta ao reclamante "[...] dar credibilidade à Universidade, como uma organização comprometida com a segurança da Informação".

A Figura 21 é a representação do mapa deste incidente onde há a demonstração de uma Ação de Mau uso de softwares da organização, quando um agente interno foi o causador de um incidente de segurança da informação.

Como pode ser observado na Figura 21 há a interação entre o agente interno, que causou o incidente; o atributo de confiabilidade desta instituição; o ativo, o conteúdo que foi baixado; e a ação de Mau uso, a qual obteve caminho por software *peer-to-peer*. Este

Figura 21 – Mapa da ação de Violação de Direitos Autorais

Fonte: autoria própria.

mapa de classificação tem como objetivo a demonstração visual de como cada componente teve sua participação neste incidente.

Com base neste incidente de segurança da informação a modelagem AS-IS do processo de tratamento de notificação Externa foi validada para este incidente. Entretanto faz-se necessário para que o 2PTISI seja validado a mesma modelagem deve ser replicável para todos os PTISI da instituição. Assim sendo a próxima seção tratará de uma notificação interna de incidente de segurança sendo modelado pelo 3PTISI de notificação Interna.

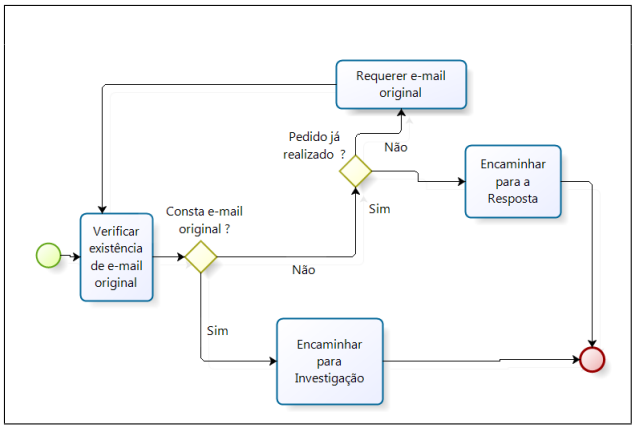
5.2.1 Notificação Interna

Com o propósito de validar as modelagens dos 3PTISI, para a modelagem AS-IS de notificação interna, foi modelado um exemplo de notificação interna de incidente de segurança de SPAM, para validação desta modelagem. A Figura 16 demonstra como esta modelagem foi realizada.

Observando a Figura 16 nota-se que esta notificação origina-se de um agente interno da instituição, o qual abre um chamado para a equipe de suporte via email, a equipe confere a natureza do email e encaminha o mesmo para a equipe de segurança. Quando esta notificação chega a equipe de segurança, esta notificação recebe o mesmo tratamento de uma notificação externa. A notificação irá ser processada por cada uma das atividades e sub-processos que seria realizada em uma notificação externa. A Figura 22 mostra como esta notificação de incidente é tratada no sub-processo de Análise de incidente.

As Figuras 22 e 17 demonstram o TISI no sub-processo de Análise de incidente. Por se tratarem de incidentes diferentes, estes sub-processos também são diferentes. Na Figura 22 nota-se que é verificado se no email que notificou o possível incidente havia o email original do mesmo. Caso não houver o email original o responsável pela Análise do incidente encaminhara um email ao comunicante pedindo o email original. Caso este pedido já tenha sido realizado, e ainda não constar o email original, o incidente será encaminhado para a resposta e o encerramento. Caso houver o email original na notificação do incidente, esta notificação será encaminhada para a Investigação, encerrando o sub-processo de Análise de incidente. Na Figura 23 é apresentado como esta investigação é

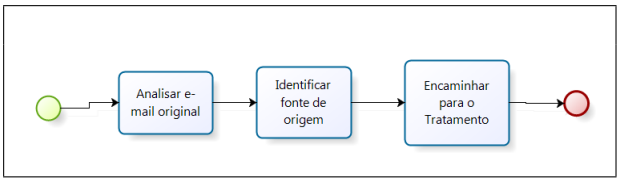
Figura 22 – Sub-Processo de Análise de Notificação de SPAM



Fonte: autoria própria.

realizada.

Figura 23 – Sub-Processo de Investigação de SPAM



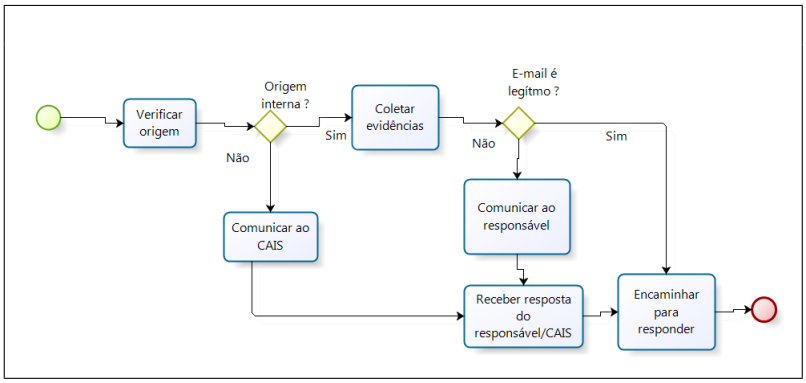
Fonte: autoria própria.

Como pode ser observado na Figura 23, este é um dos sub-processos com menos atividades a serem realizadas. Neste sub processo é necessário ser analisado o email original, identificar neste email a sua fonte de origem, e encaminhar estas evidências para o processo de Tratamento. Novamente por se tratar de incidentes diferentes o processo de Investigação de incidente demonstrado na Figura 18 e na Figura 23, apesar de se tratar do mesmo sub-processo de Investigação de incidente, tem suas atividades diferentes. E assim será para casa sub-processo de diferentes tipos de incidentes.

Como pode ser observado na Figura 24 que demonstra o processo de Tratamento de incidente da notificação de SPAM.

Comparando o processo da Figura 19 com o processo da Figura 24, ambos representando o mesmo sub-processo de Tratamento de Incidente, nota-se não se tratar das mesmas atividades. Na Figura 24 há a atividade de verificar qual a origem do email original, se interna (da instituição) ou não. Caso seja uma origem interna, a equipe de segurança busca por evidências que servirá de prova se este email se caracteriza ou não por ser um SPAM, provas de que o email é legítimo. Caso o email seja legítimo encaminha para a resposta. Caso contrário comunica ao responsável, aguarda uma resposta do mesmo e encaminha para a resposta. Caso este email, notificado como sendo um SPAM

Figura 24 – Sub-Processo de Tratamento de incidente de SPAM



Fonte: autoria própria.

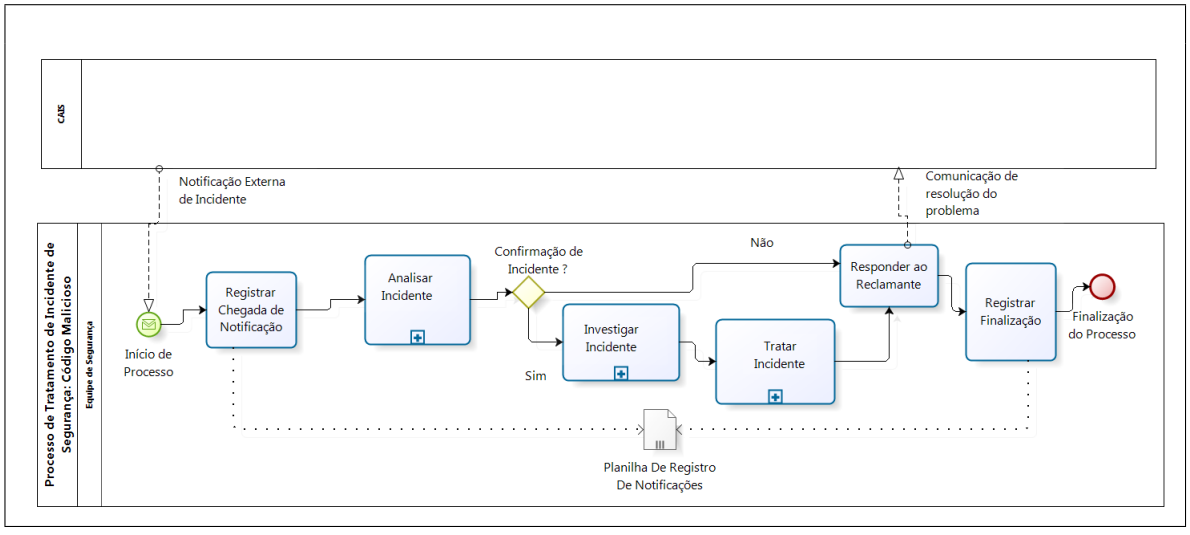
seja de origem externa a equipe de segurança comunica o ocorrido ao CAIS com todas as evidências coletadas. E aguardará pela resposta do CAIS sobre o ocorrido.

Da mesma forma como em uma notificação de violação de direitos autorais, este PTISI só será encerrado depois da ser passada uma resposta ao comunicante da notificação e realizado o devido registro na planilha.

Com a modelagem do 3PTISI para a notificação interna de incidente, no caso uma notificação de SPAM, foi validado junto com entrevistas a validação deste modelo.

Uma outra modelagem foi realizada para uma notificação externa de código malicioso, para obter a validação do 3PTISI. Na Figura 25 nota-se que houve uma notificação realizada por um agente externo, CAIS via email, para a equipe de segurança da instituição.

Figura 25 – Notificação Externa de Código Malicioso.

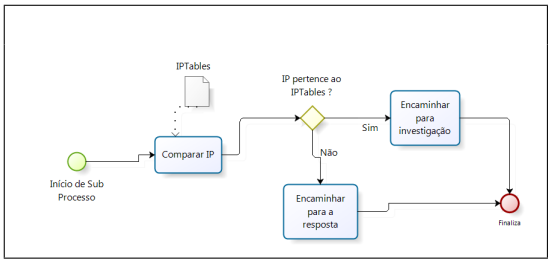


Fonte: autoria própria.

Como pode-se notar na Figura 25 usa-se o 3PTISI de notificação externa para

modelar este PTISI. Demonstrando que o 3PTISI é um processo reproduzível para as notificações tanto internas como externas. Sendo que as mudanças de uma notificação para outra se dará nos sub-processos de cada notificação.

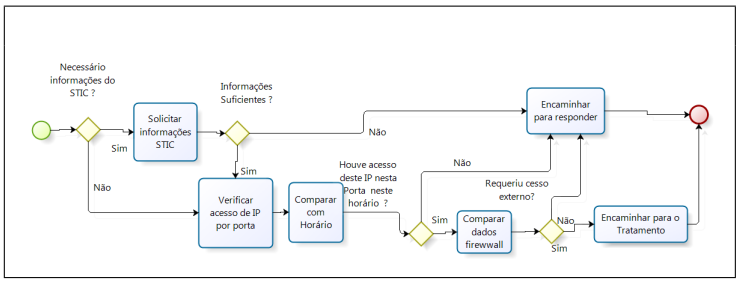
Figura 26 – Sub-Processo de Análise de Incidente de Código Malicioso.



Fonte: autoria própria.

Observando a Figura 26 observa-se a repetição da existência dos mesmo sub-processos, neste caso em particular o sub-processo de Análise de incidente será idêntico como no incidente de violação de direitos autorais. Sendo modificado neste caso o sub-processo de Investigação de incidente que é apresentado na Figura 27.

Figura 27 – Sub-Processo de Investigação de Código Malicioso.

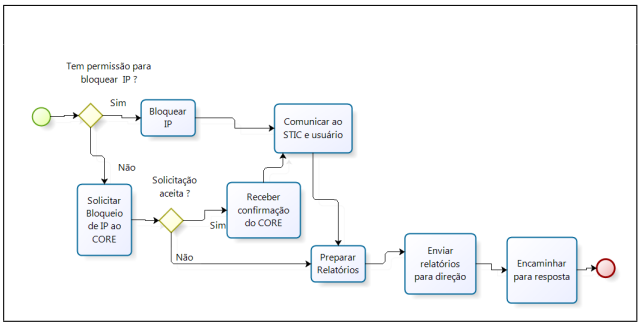


Fonte: autoria própria.

Na Figura 27 observa-se que a equipe de segurança solicita ao STIC informações adicionais, para investigar a notificação. E na Figura 28 é introduzido a Coordenadoria de Redes Infraestrutura e Suporte (CORE) que será responsável por permitir ou não o bloqueio de um determinado IP.

Juntamente com a Figura 28 e as demais foi demonstrado que as modelagem AS-IS são viáveis e replicáveis para vários tipos de PTISI. Após entrevista com membros do NTIC foi verificada a validação das modelagens AS-IS para notificações internas e notificações externas de TISI. Tendo apresentado as modelas AS-IS para as notificações internas e externas de tratamentos de incidentes de segurança da informação. Apresentado sua viabilidade e a possibilidade de replicações, torna-se necessário a modelagem TO-BE deste tipo de incidentes, para possibilitar a otimização dos processos já existentes.

Figura 28 – Sub-Processo de Tratamento de incidentes de Código Malicioso.



Fonte: autoria própria.

5.3 Modelagem TO-BE dos Incidentes de Segurança da Informação

Após a modelagem do estado atual, faz-se necessário a modelagem do estado futuro. Alguns dos requisitos adicionais para o estado futuro (TO-BE) são encontrados em Flora (2010), onde é mencionado algumas das melhorias que poderiam ser realizadas para ajudar nos PTISI.

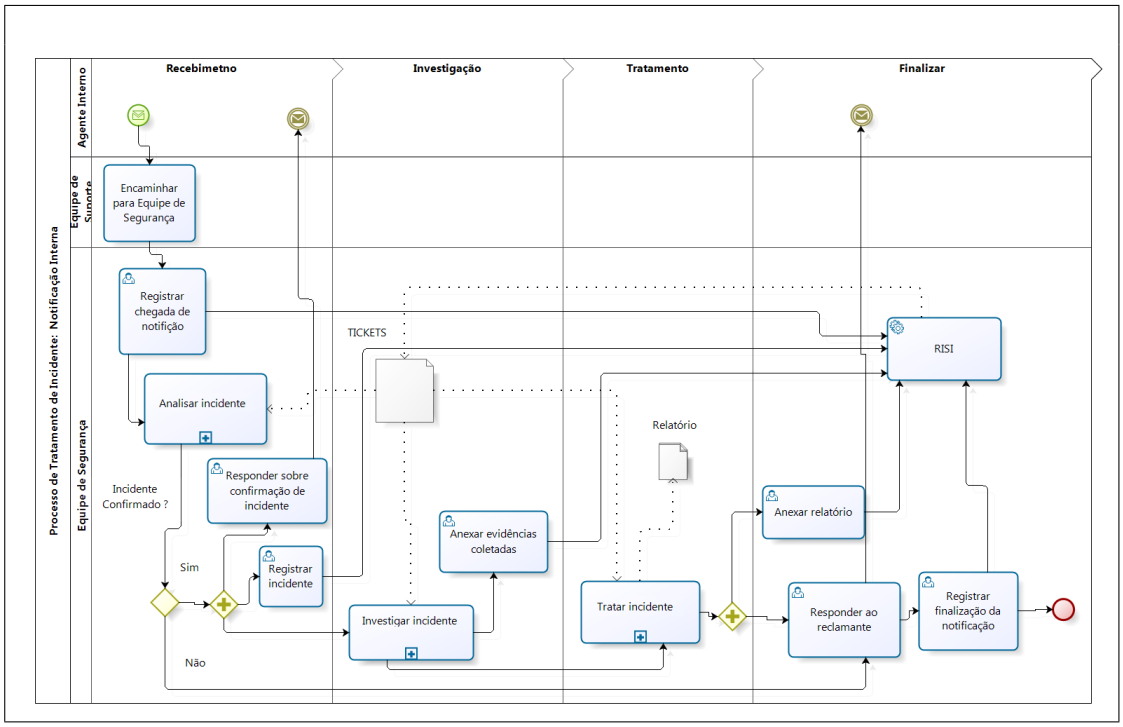
Sendo um dos requisitos para esta melhoria, a utilização de Dispositivos de Detecção Automática, como salienta Flora (2010) que

> a maioria dos incidentes identificados internamente ocorreu por constatação visual, ou seja, por indisponibilidade de um serviço ou na inspeção de rotina realizada por um membro da equipe ... é muito importante contar com dispositivos capazes de detectar a ocorrência de incidentes de segurança ou atividades suspeitas de forma automática, pois esta detecção pode evitar danos maiores à instituição.

Flora (2010) salienta ainda outra melhoria que poderia ser implementada no PTISI, que seria a implementação de "[...] um sistema ou base de dados para armazenar as informações relativas a cada incidente tratado". A implementação do mesmo se daria pelo fato de que a não existência de um sistema ou base de dados dificulta tanto a consulta sobre um incidente como também a geração de relatórios estatísticos sobre os incidentes de segurança da informação.

Com base nestes requisitos, apresentação e entrevista a partir de um questionário com membros de NTIC, que pode ser observado no anexo B deste trabalho, e entrevistas com o Coordenador de Segurança em Informação do Núcleo de Tecnologia em Informação e Comunicação (CSI/NTIC) Fernando Della Flora, obteve para a modelagem de estado TO-BE, três novas modelagens. A Figura 29 referente a modelagem de Notificação Interna dos incidentes de segurança da informação. A modelagem de Notificação Externa de incidente de segurança da informação representada pela Figura 34 e a modelagem de Dispositivo de Detecção Automático que consta na Figura 35.

Figura 29 – Modelagem TO-BE de Notificação Interna.



Fonte: autoria própria.

Observando a Figura 29 pode ser constatado diferenças entre esta e a Figura 16 da modelagem AS-IS. Na modelagem do estado futuro pode se constatar que uma divisão da modelagem referente ao tempo foi adicionado, portanto agora há tempos para o recebimento, investigação, tratamento e finalização do processo. A esta modelagem foi adicionado um RTIR, que funciona como um repositório para receber, armazenar e servir de consulta para as atividades que envolvem o PTISI, portanto no texto quando houver menção a repositório, será ao RTIR que trata este trabalho.

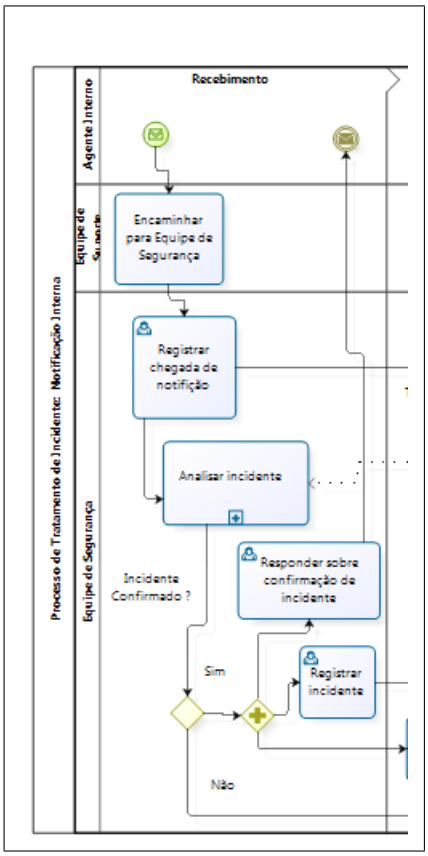
O RTIR, assim como dispositivo de detecção automático será melhor descrito mais a frente neste texto.

A Figura 30 refere-se a apenas ao tempo relacionado com o recebimento da notificação desde a equipe de suporte, passando pela chegada da notificação pela equipe de segurança, a realização da análise. Dependendo da resposta da análise passando para outra linha de tempo podendo ser a de finalização ou a de investigação.

Quando chega um email para a equipe de segurança com a notificação de um possível incidente, a equipe de segurança registra esta chegada de notificação de incidente. Diferente da modelagem AS-IS, este registro não mais será realizado em uma planilha eletrônica e sim em um repositório. Este repositório a partir do registro de uma notificação, ele gera um Ticket (um código referente a notificação realizada), contendo todas as informações que foram atualizadas nele que haviam no email de notificação. Este Ticket

é enviado para a Análise de incidente.

Figura 30 – Modelagem TO-BE - Divisão por tempo: Recebimento



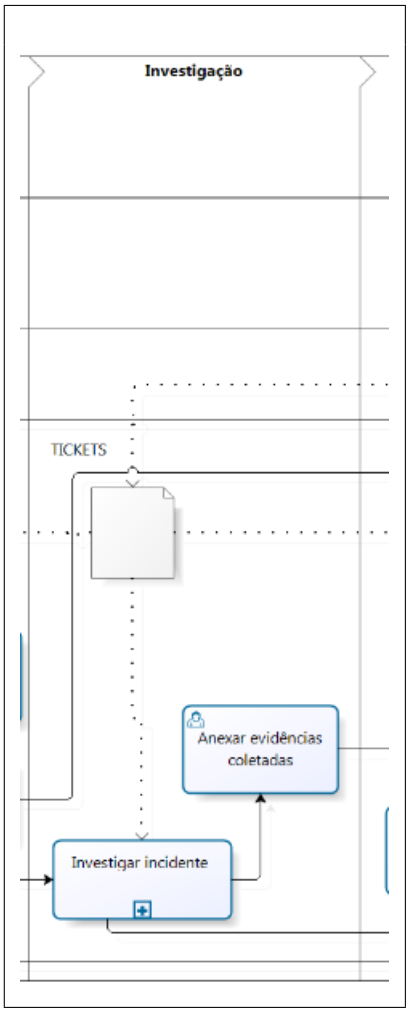
Fonte: autoria própria.

Nesta Figura 30 também há o acréscimo da atividade sobre "Responder sobre confirmação do incidente", atividade esta que foi adicionada para evitar o reenvio por parte do comunicante da mesma notificação. Foi acrescentada a atividade "Registrar incidente"devido ao acréscimo do repositório, sendo necessário a atualização do mesmo. As atividades existentes são marcadas para que se saiba de quem será a responsabilidade de cada tarefa, ou seja, definido entre tarefa do usuário, equipe de segurança, ou tarefa de sistema, algum software instalado.

Na Figura 31, onde as tarefas são desenvolvidas a partir das respostas obtidas na atividade Análise de Incidente que irão atualizar o repositório, e o mesmo gerara um Ticket com o mesmo número do anterior, entretanto tendo as informações obtidas a partir da análise do incidente. Neste período de tempo há duas atividades a serem realizadas. O sub-processo de investigação de incidente e a atividade de anexar as evidências coletadas no sub-processo de investigação ao repositório.

Como mostrado na Figura 31, o sub-processo investigar utiliza as informações vindas do repositório para obter as informações necessárias para a investigação, e possíveis consultas. Este processo também atualiza o repositório com as evidências que esta

Figura 31 – Modelagem TO-BE - Divisão por tempo: Investigação.



Fonte: autoria própria.

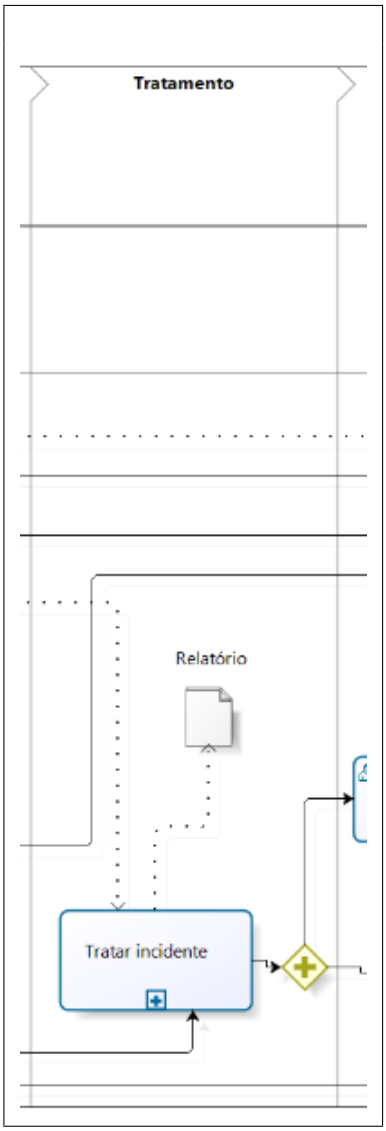
investigação coletou.

Na Figura 32 referente ao tempo de tratamento do PTISI há apenas o sub-processo de tratamento. Este sub-processo recebe do repositório, o Ticket contendo o número original (gerado no momento do registro da notificação) e todo o conteúdo, desde o registro da notificação até as evidências coletadas na investigação.

Este sub-processo que é representado na Figura 32, após realizar as suas atividades de tratamento do incidente, gera um relatório sobre o ocorrido. Na divisão de tempo denominada de Finalização, este relatório será anexado ao repositório, como pode ser observado na Figura 33.

A Figura 33 demonstra as atividades que ocorrem na divisão de tempo da finalização. Nesta etapa de tempo ocorrerá o anexo do relatório gerado na atividade de tratamento ao repositório, haverá também a atividade de responder ao comunicante, assim como haverá a atividade de registrar a finalização desta notificação ao repositório.

Figura 32 – Modelagem TO-BE - Divisão por tempo: Tratamento.



Fonte: autoria própria.

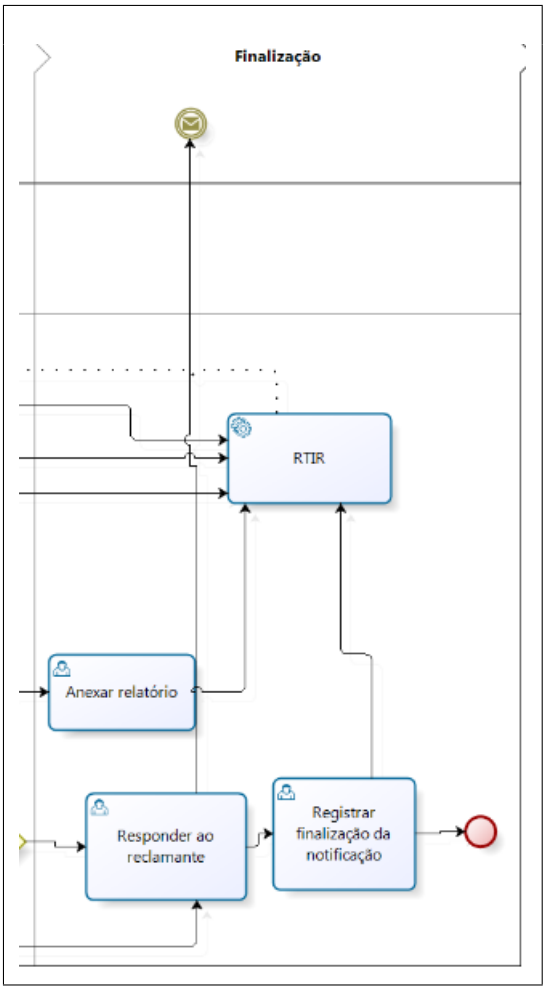
5.3.1 Notificação Externa

Assim como há a notificação Interna na modelagem TO-BE, também há a notificação Externa nesta modelagem. A Figura **??** representa esta modelagem.

Como pode ser observado na Figura 34, ao receber uma notificação por um agente externo à organização por meio de um email. A partir do momento que este email chega a equipe de segurança, na notificação externa da modelagem AS-IS era realizado o registro de chegada em uma planilha eletrônica. Na modelagem TO-BE, este registro é realizado no repositório.

Do momento em que é realizado o registro no repositório as atividades realizadas na modelagem TO-BE para notificação interna são idênticas as atividades realizadas na modelagem TO-BE para as notificações externas.

Figura 33 – Modelagem TO-BE - Divisão por tempo: Finalização.



Fonte: autoria própria.

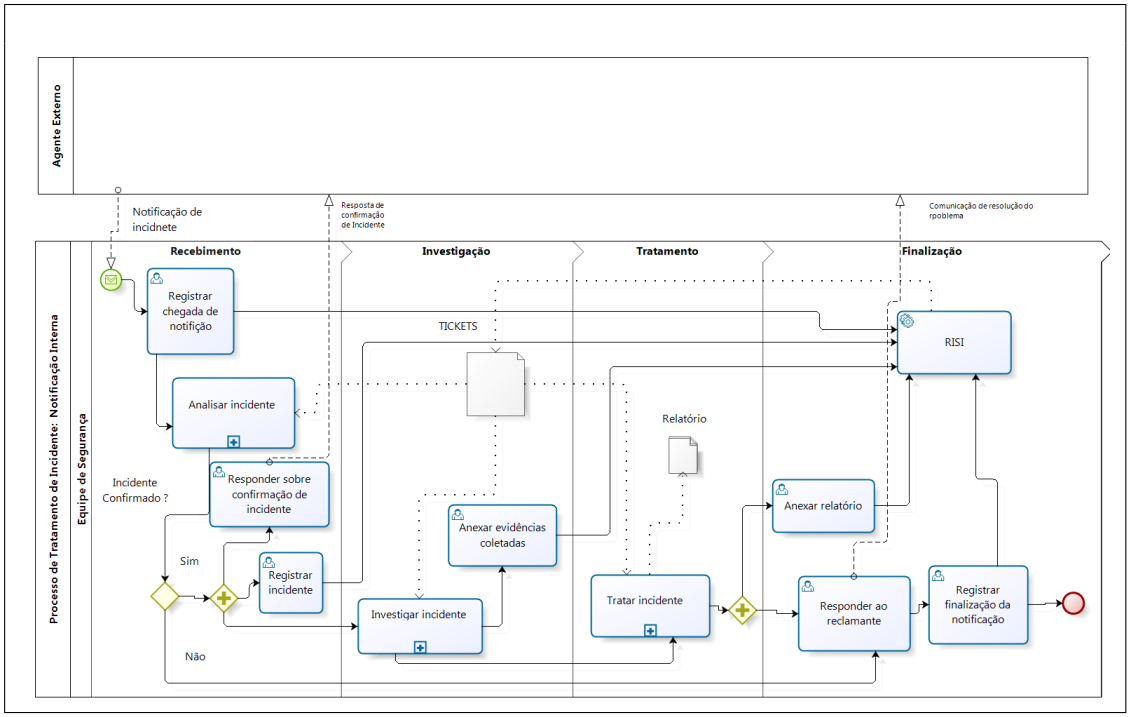
5.3.2 Dispositivo de Detecção Automático

A terceira notificação da modelagem TO-BE é realizada a partir de um Dispositivo de Detecção Automático. A Figura 35 mostra a modelagem realizada para esta notificação.

Observando a Figura 35 nota-se uma imagem de alarme, esta imagem esta representando um Dispositivo de Detecção Automática (DDA). Este dispositivo tem como finalidade o monitoramento da rede, e assim que o mesmo perceber alguma anomalia na rede, automaticamente informa a equipe de segurança da informação, via email, para que a equipe possa tratar do incidente.

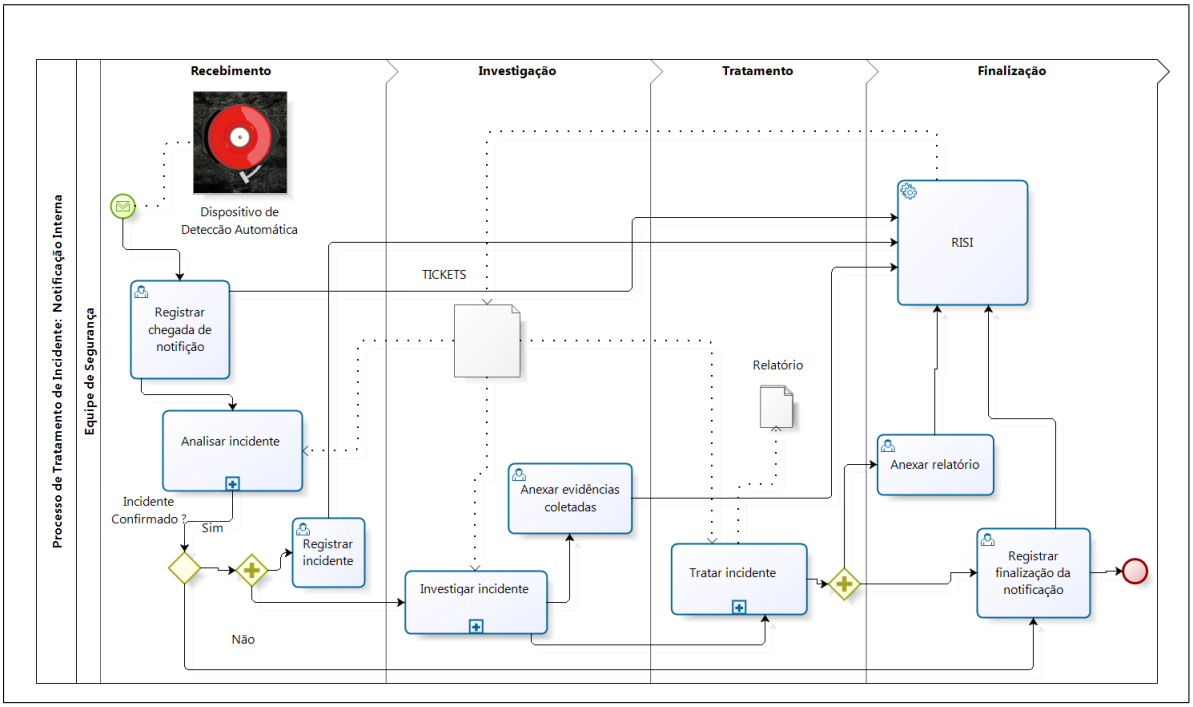
Nesta seção foi demonstrada as modelagens TO-BE para notificações externas e internas, na próxima seção haverá um resumo dos conceitos de repositório, no contexto deste trabalho, e de DDA.

Figura 34 – Modelagem TO-BE Externa.



Fonte: autoria própria.

Figura 35 – Modelagem TO-BE Dispositivo de Detecção Automática.



Fonte: autoria própria.

6 Resultados

Após a realização das modelagens fez-se necessário a validação junto ao grupo de segurança. A validação foi realizada com base em apresentação e entrevistas. Para assim descobrir quais pontos deveriam ser alterados e/ou melhorados e/ou acrescentados para se obter uma otimização das modelagens. Sendo necessário para isto saber da equipe de segurança as modificações e ações que os mesmos acham necessário que seja implementado.

Algumas das respostas mais relevantes ao trabalho estão apresentadas a seguir, com estas respostas foi possível modelar e validar os atuais modelos AS-IS e os modelos TO-BE já apresentados neste TCC.

Um dos requisitos da equipe de segurança é a implementação de um dispositivo de detecção automática. A instituição já trabalha com um Sistema de Detecção de Intrusos, do inglês IDS, este sistema verifica as anormalidades na rede entretanto o sistema já em uso não tem meios automáticos de notificação à equipe de alguma anomalia na rede. O requisito da equipe de segurança é haver um dispositivo que permita que os IDS faça a varredura necessária e ao encontrar uma anomalia avise, de preferência por alerta via email, à equipe de segurança.

Outro requisito da equipe de segurança é a implementação de um RISI. Na implementação de um RISI, a atual planilha eletrônica seria eliminada. Para a equipe de segurança esta troca seria aceitável e produtiva, já que a planilha eletrônica é apenas um controle e o RISI é um sistema de banco de dados, que possibilita consultas, geração de relatório, configuração de acordo com o processo entre outros.

No sub processo de Tratamento de incidente quando concluído é gerado um relatório, que recebe o nome "Relatório"acrescentado do número do incidente, este relatório é armazenado em um repositório *online*. Em um relatório geralmente consta: Detalhamento do Trabalho, com dados do incidente, resumo do trabalho realizado na coleta das evidências, entre outros; as Ações Tomadas para o tratamento do incidente; e os Anexos, arquivos anexos, cópia da notificação do incidente, arquivo de *logs*, evidências e demais anexos que seja necessário.

Estes requisitos foram implementado nas modelagem TO-BE, e são alguns dos meios identificados para aprimorar o gerenciamento dos PTISI, assim como possibilitar a diminuição do retrabalho para a equipe de segurança. Um exemplo de como seria aprimorado o gerenciamento dos PTISI é como os IDS, onde a equipe não esperaria apenas por notificações de agentes internos e externos como também contaria com os alertas destes dispositivos para informar sobre possíveis anomalias na rede. Um exemplo aplicável a diminuição do retrabalho da equipe, é com a utilização dos RISI que possibilitam a

geração de relatórios.

Com base no questionário para validação, apresentado à equipe de segurança, que pode ser visto no Anexo B deste trabalho, as respostas obtidas na questão referente se os processos apresentados eram os processos utilizados por eles em um tratamento de segurança, obteve 100% de confirmação. Referente a pergunta sobre as expectativas em relação as modelagens TO-BE, com as inclusões de um RISI e DDA, obteve resposta de 75% em grande parte, sendo 25% como parcialmente.

Referente a pergunta sobre modificações nas modelagens TO-BE para sua otimização. As respostas obtidas sugeriam que fosse acrescentado uma notificação ao comunicante, após a analise do incidente, sobre a confirmação do mesmo. Com o intuito de evitar o reenvio da mesma notificação, evitando assim um retrabalho da equipe de segurança, assim como dar uma satisfação do estado do tratamento do incidente pela instituição.

Referente a pergunta sobre o que poderia ser alterado nas modelagens para que o processo de tratamento de incidente possa ser melhorado. Obteve-se a resposta de acrescentar ao DDA um Testes de Stress, aplicado por um especialista de segurança. A esta mesma pergunta também se obteve resposta de acréscimo de scripts de testes com diferentes exemplos de incidentes, para verificar as condições dos processos de tratamento de incidentes. Assim como formas de verificar se o incidente persistiu após o seu tratamento; uma definição concreta das ferramentas e do repositório a ser implementado. E ainda uma forma de gerar um estudo estatístico dos incidentes tratados, que possa filtrar a origem dos problemas.

Algumas destas sugestões foram implementadas na modelagem TO-BE para sua melhoria. Como a resposta ao pedido de comunicação de andamento do processo ao comunicante. Obteve como resultado o acréscimo de uma atividade de "Resposta sobre o andamento"tanto nas modelagens AS-IS como nas modelagens TO-BE. Com as modelagens dos 3PTISI realizadas e validadas pela equipe de segurança, e pelo CSI/NTIC da instituição, obtem-se o 2PTISI desta instituição. Com as possíveis implementações das ferramentas a possibilidade da diminuição do retrabalho da equipe de segurança, economizando recursos da instituição (incluindo o tempo da equipe como recurso).

As modelagens foram validadas, assim obtendo uma forma padronizada de tratar os ISI da instituição. Suprindo a necessidade que existia e obtendo uma forma de socializar o conhecimento da forma como este tratamento é realizado.

Com a validação das modelagens, conclui-se a quarta etapa do cronograma deste TCC mostrada na Figura 1. Concluindo também esta parte do TCC. Nesta seção foram apresentados os resultados obtidos neste TCC para os PTISI desta instituição.

7 Conclusão

Neste trabalho foram apresentados os conceitos de segurança da informação, incidente de segurança da informação, BPM e BPMN. Baseado nestes conceitos e na perspectiva de criar um 2PTISI para uso nesta instituição.

Este trabalho demonstra o projeto e a viabilidade de 2PTISI, os quais para esta instituição faz-se necessário para o modelo atual duas modelagens, uma para notificações internas e outra para notificações externas, como demonstrado nas Figuras 15 e 16.

Assim como para a modelagem dos modelos futuros haver além das notificações externas e internas, também a notificação por DDA. Com a implementação de DDA faz-se necessário o estudo de ferramentas adequadas para a implementação no setor de segurança da instituição.

Os 2PTISI propostos para o ser implementado no setor de segurança é viável e pode ser replicável para outros processos de segurança da informação. Pois dependendo do processo a ser modelado, serão realizadas as modificações apenas nos sub processos do 2PTISI.

A modelagem dos PTISI é viável, útil e necessária para atender a demanda de transmitir os conhecimentos e o PTISI que esta instituição utiliza como demonstrado na Tabela 1.

Verificou-se também que a visão por processo com o auxílio da modelagem pode ser vista como uma forma de representação e socialização do conhecimento entre a equipe de segurança da informação.

Foram descritos algumas das ferramentas que podem ser implementadas para a otimização dos PTISI desta instituição.

A conclusão deste TCC é que a modelagem de um 2PTISI é importante ao NTIC para possibilitar uma forma visual de transmitir seus métodos de tratamento deste tipo de incidente, visualizar o andamento do processo e diminuir o retrabalho.

Em um trabalho futuro seria importante o estudo de como o tratamento de incidentes desta natureza é realizado em outros NTIC, com o intuito de se obter um processo padrão para tratamentos de incidente desta natureza. Assim como a implementação das ferramentas para a otimização destes processos nesta instituição.

Referências

ABPMP. *Guia para o Gerenciamento de Processos de Negócios. Corpo Comum de Conhecimento*. [S.l.], 2009. Citado na página 44.

AIRT. *Aplicattion for Incident Response Teams (AIRT)*. 2005. Disponível em: <http://airt.leune.com/>. Acesso em: 15 de setembro de 2013. Citado na página 39.

BALDAM, R. Análise e modelagem de processos de negócios: Foco na notação bpmn. In: _____. Sao Paulo: Atlas, 2009. cap. Ciclo de Gerenciamento de BPM, p. 109–115. Citado 2 vezes nas páginas 43 e 44.

BARROS, M. V. D.; FERREIRA, M. G. G.; TOLFO, C. Aplicação da modelagem de processos de negócios em sistemas produto-serviço. *XVII SIMPEP - Simpósio de Engenharia de Produção*, nov 2010. Citado na página 47.

BEST. *RT for Incident Response (RTIR)*. 2002. Disponível em: <http://bestpractical-.com/rtir/>. Acesso em: 15 de setembro de 2013. Citado 2 vezes nas páginas 37 e 38.

BONE, A. *RT for Incident Response (RTIR)*. 2006. Disponível em: <https://www-.ja.net/>. Acesso em: 15 de setembro de 2013. Citado 2 vezes nas páginas 36 e 38.

BRUMFIELD, J. *News Center - Verizon Enterprise Solutions*. 2013. Disponível em: <http://www.verizonenterprise.com/news/2013/03/security-veris-dbir-data-cybersecurity>. Acesso em: 15 de setembro de 2013. Citado na página 26.

CAMPOS, A. L. N. *Modelagem de Processos com BPMN*. [S.l.]: Brasport, 2013. Citado na página 45.

CERT.BR. 1998. Disponível em: <www.cert.br>. Acesso em: 15 de setembro de 2013. Citado 2 vezes nas páginas 26 e 32.

CISCO. *Os cinco principais problemas de seguranca de pequenas e medias empresas*. 2006. Disponível em: <http://www.cisco.com/web/PT/assets/docs-/5_principais_problemas_seguranca_PME.pdf>. Acesso em: 15 de setembro de 2013. Citado na página 32.

CRUZ, T. *BPM e BPMS - Business Process Management e Business Process Management Systems*. 2. ed. [S.l.]: Brasport, 2010. Citado 2 vezes nas páginas 43 e 45.

DOCUMENTATION, U. *Nessus Compliance Checks*. 2013. Disponível em: <http:-//www.tenable.com/>. Acesso em: 15 de setembro de 2013. Citado na página 42.

EVEF, A. *A Marca Verizon*. 2012. Disponível em: <http://www.evef.com.br-/conceito%20e%20mensuracao%20de%20marca.php>. Acesso em: 15 de setembro de 2013. Citado na página 26.

FILHO, A. M. S. Segurança da informação: Sobre a necessidade de proteção de sistemas de informações. *Revista Espaço Acadêmico*, ISSN 1519.6186 Ano IV, n. 42, Novembro 2004. Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm>. Acesso em: 15 de setembro de 2013. Citado na página 21.

FLORA, F. D. *A Influência do NAT na Indentificação e Tratamento de Incidentes de Segurança da Informaçao*. Monografia (monografia) — Universidade Gama Filho, Alegrete, 2010. Citado 6 vezes nas páginas 21, 22, 52, 55, 58 e 63.

FONTES, E. *Seguranca da Informacao: O usuario faz a diferenca*. 2. ed. [S.l.]: Saraiva, 2006. Citado 3 vezes nas páginas 21, 25 e 26.

GARCIA, F.; CUVILLIER, S. Análise e modelagem de processos de negócios: Foco na notação bpmn. In: _____. edição. Sao Paulo: Atlas, 2009. cap. A modelagem na prática: a experiência do CEPEL (Centro de Pesquisa de Energia Elétrica), p. 161–202. Citado na página 45.

LAUFER, R. P. *Introdução a Sistemas de Detecção de Intrusão*. rlaufer@gta.ufrj.br: [s.n.], 2003. Disponível em: <http://www.gta.ufrj.br/grad/03_1/sdi/sdi-1.htm>. Acesso em: 15 de setembro de 2013. Citado 2 vezes nas páginas 40 e 41.

LEOBONS, R. M. *Detecção de Intrusos*. rleobons@gmail.com, 2012. Disponível em: <http://www.gta.ufrj.br/grad/03_1/sdi/sdi-1.htm>. Acesso em: 15 de setembro de 2013. Citado na página 41.

LOPES, R. M. *Gestão do conhecimento: O desafio de um novo paradigma*. Monografia (monografia) — Universidade de Brasília, Brasília, janeiro 2002. Citado na página 21.

MADEIRA, F. *Arpwatch*. 2008. Disponível em: <http://www.madeira.eng.br/wiki-/index.php?page=Arpwatch>. Acesso em: 15 de setembro de 2013. Citado na página 41.

NÓBREGA, J. *A lei em um mundo sem fronteiras*. 2013. Disponível em: <oglobo.globo-.com/a-lei-num-mundo-sem-fronteiras-6773585>. Acesso em: 15 de setembro de 2013. Citado na página 25.

NETO, M. A. A. Análise e modelagem de processos de negócios: Foco na notação bpmn. In: _____. edição. Sao Paulo: Atlas, 2009. cap. Técnicas de Modelagem: Uma abordagem pragmática, p. 52–76. Citado na página 45.

NG syslog. *Gerenciamento de registros confiáveis*. 2013. Disponível em: <http://www-.balabit.com/network-security/syslog-ng/opensource-logging-system>. Acesso em: 15 de setembro de 2013. Citado na página 41.

NTIC. *Histórico*. 2010. Disponível em: <http://ntic.unipampa.edu.br/quem-somos-2-/historico/>. Acesso em: 15 de setembro de 2013. Citado na página 51.

NTIC. *Plano Diretor de Tecnologia da Informação e Comunicação*. [S.l.], 2011. Citado na página 51.

OMG. *Business Process Model and Notation (BPMN)*. [S.l.], 2011. Citado na página 45.

RUTGERS. *Information Protection and Security*. 2010. Disponível em: <https://-/rusecure.rutgers.edu/content/rtir-request-tracker-incident-response>. Acesso em: 15 de setembro de 2013. Citado na página 39.

SêMOLA, M. *Gestao de Seguranca da Informacao. Uma visao executiva.* 1. ed. [S.l.]: Elsevier, 2003. Citado 3 vezes nas páginas 25, 26 e 28.

SNORT. 2013. Disponível em: <http://www.snort.org/>. Acesso em: 15 de setembro de 2013. Citado na página 41.

SOARES, D. A.; INSFRAN, L. S. B. *Estudo exploratorio utilizando BPMN em um processo de Engenhariade Requisitos*. Monografia (monografia) — Universidade de Brasilia - Instituto de Ciencias Exatas - Departamento de Ciencia da Computacao, Brasilia, 2011. Citado 2 vezes nas páginas 48 e 49.

SORIANO, M. Information and network security. *Czech Technical University of Prague*, 201? Citado na página 40.

SWATCH. *Swatch configuration steps*. 2013. Disponível em: <http://archives.neohapsis-.com/archives/snort/2005-03/att-0288/swatch_configuration.pdf>. Acesso em: 15 de setembro de 2013. Citado na página 41.

UBUNTU, D. *Logwatch*. 2013. Disponível em: <https://help.ubuntu.com/community-/Logwatch>. Acesso em: 15 de setembro de 2013. Citado na página 41.

UNIPAMPA. Estatuto. mar 2011. Disponível em: <http://www.unipampa.edu.br-/portal/universidade>. Citado na página 51.

VALLE, R.; OLIVEIRA, S. B. *Analise e Modelagem de Processos de Negocios. Foco na notacao BPMN.* 1. ed. [S.l.]: Editora Atlas S.A., 2009. Citado na página 45.

VERIS. *Framework de Classificação de Incidentes de Segurança da Informação*. 2010. Disponível em: <http://www.mindmeister.com/pt/44961919/veris-incident-classification>. Acesso em: 15 de setembro de 2013. Citado 10 vezes nas páginas 27, 29, 30, 31, 32, 34, 35, 40, 81 e 82.

VERIZON. *Exemplos de Classificação de Incidentes*. 2010. Disponível em: <http:/-/verisframework.wiki.zoho.com/Classification-Examples.html>. Acesso em: 05 de maio de 2012. Citado 3 vezes nas páginas 33, 35 e 36.

VERIZON. 2012. Disponível em: <http://about.verizon.com/index.php/about/our-company and http://newscenter2.verizon.com/kit/vcorp/factsheet.html>. Acesso em: 15 de setembro de 2013. Citado na página 26.

VERIZON. *The History of Verizon Comunications*. 2013. Disponível em: <http:/-/espanol.verizon.com/enes/sdwww/investor/corporatehistory.htm>. Acesso em: 15 de setembro de 2013. Citado na página 26.

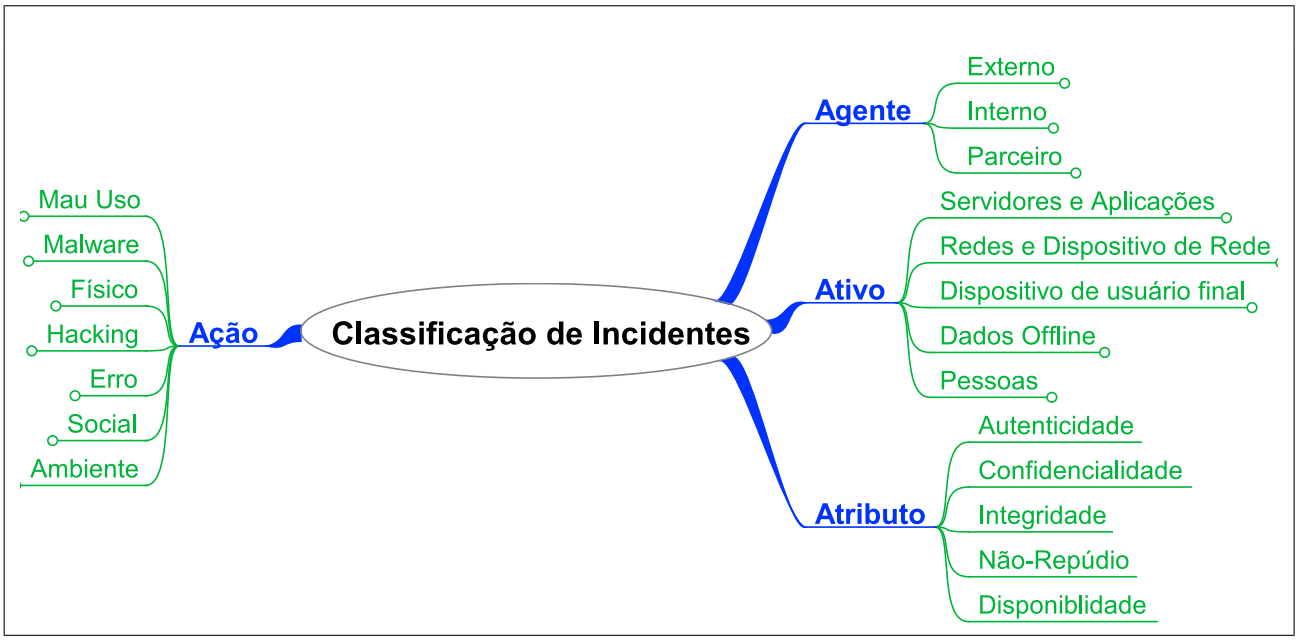
WENDT, E.; JORGE, H. V. N. *Crimes cibernéticos: Ameaças e procedimento de investigação.* [S.l.]: Brasport, 2012. Citado na página 32.

Anexos

ANEXO A – Classificação Incidente de Segurança da Informação

Mapa da classificação de Incidentes de Segurança da Informação, onde os elementos principais estão em destaque (Ação, Ativo, Agente e Atributo).

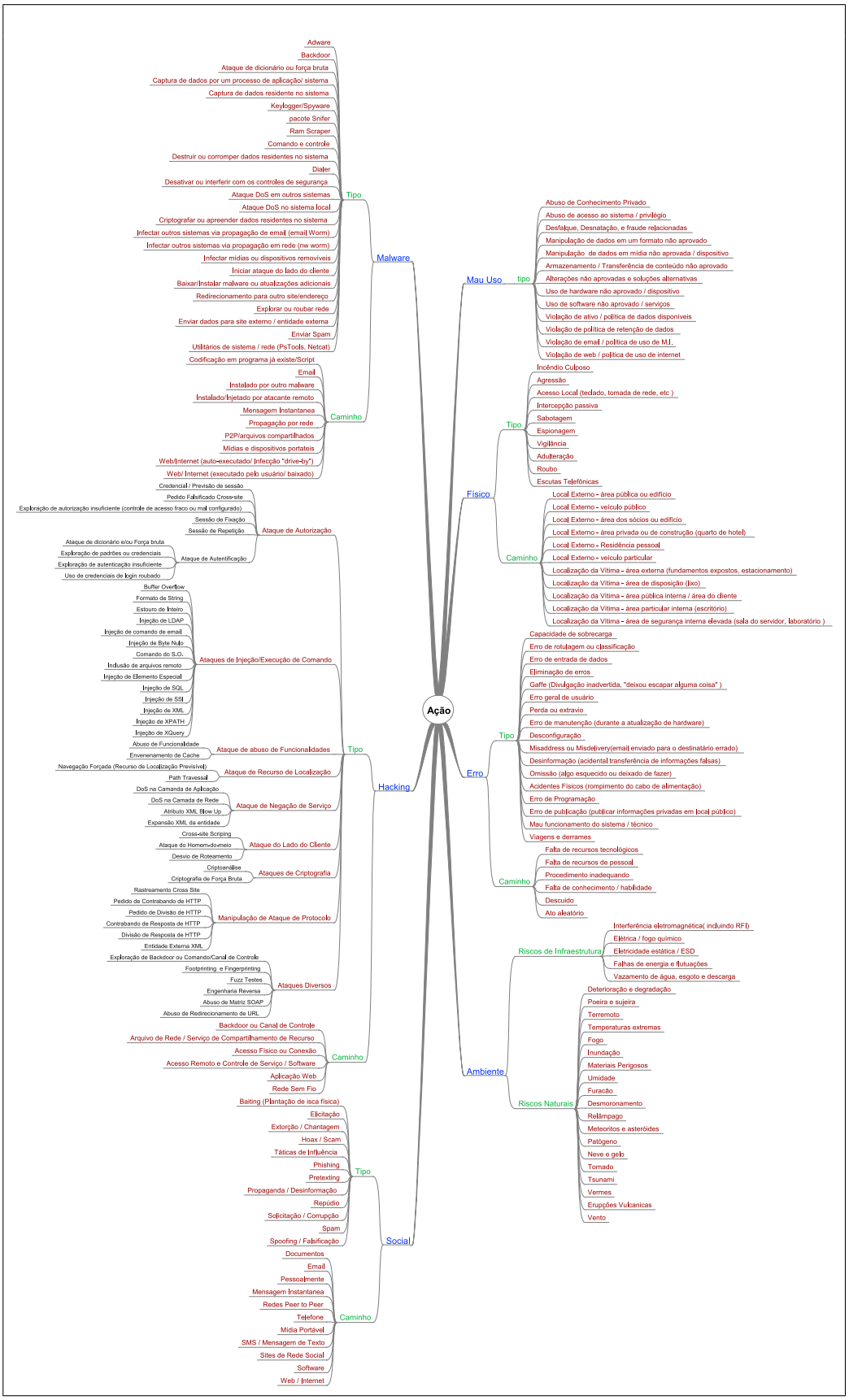
Figura 36 – Quadro Geral da Classificação de Incidente de Segurança da Informação.



Fonte: Adaptado de VERIS (2010).

A Classificação de Incidente de Segurança da Informação com foco no Agente pode ser observada na Figura 4. Assim como a classificação com foco no ativo pode ser observado na Figura 5. O mesmo pode ser observado na Figura 3, referente ao atributo. Mapa da Classificação de Incidente de Segurança da Informação tendo em destaque na Ação.

Figura 37 – Classificação de ISI com foco no Ação.



Fonte: Adaptado de VERIS (2010).

ANEXO B – Questionário Aplicado à Equipe de Segurança

Questionário

Este questionário tem como objetivos ser uma das formas de auxiliar na verificação da implementação de Processos Padrões de Tratamento de Incidente de Segurança da Informação 2PTISI ocorridos nesta instituição. Verificar se a modelagem TO-BE está de acordo com o que pode ser implementável e outras formas de sua otimizada. Será apresentado à equipe de segurança desta instituição responsável pelo tratamento de incidente desta natureza.

Com base nas modelagens de processos AS-IS, modelagem do processo atual, das modelagens de notificação de incidentes realizadas por agentes externos ou internos. Os processos contidos nestas modelagens (Analisar, Investigar, Tratar e Responder) são os processos padrões para o tratamento de incidente utilizado ?

( ) sempre.

( ) geralmente.

( ) raramente.

( ) nunca.

Obs.:

Com base nas modelagens de processos TO-BE, modelagem do processo em estado futuro, para as notificações de incidente realizadas por agentes externos, internos ou por dispositivo de detecção automático de incidente. As alterações realizadas estão de acordo com as suas expectativas ?

( ) totalmente.

( ) em grande parte.

( ) parcialmente.

( ) não as retrata.

Obs.:

Com base nas modelagens de processos TO-BE, referente a modelagem de notificação por agente externo e interno o que poderia ser modificado para sua otimização?

R.:

Com base no que foi apresentado na modelagem TO-BE o que poderia ser alterado para a otimização dos processos de tratamento de incidente de segurança da informação da organização?

R.:

ANEXO C – Fluxo de Dados

Tratamento de Incidente de Segurança

Tabela 3 – Incidente: Código Malicioso.

Passo	**Quem Faz ?**	**O Que Faz ?**
1	CAIS	Notificação externa de um código malicioso originário da instituição UNIPAMPA;
2	Equipe de Segurança	Receber a notificação;
3	Analisar Incidente	Identificar IP;
3.1	Analisar Incidente	IP não pertence à instituição;
3.1.1	Analisar Incidente	Encaminhar para a resposta;
3.2	Analisar Incidente	IP pertence a instituição;
3.3	Analisar Incidente	Encaminhar para a Investigação;
4	Investigar Incidente	Comparar IP, data e hora;
4.1	Investigar Incidente	Não corresponde;
4.1.1	Investigar Incidente	Encaminhar para a Resposta;
4.2	Investigar Incidente	Corresponde;
4.2.1	Investigar Incidente	Descobrir a qual campus pertence o IP STIC;
4.2.2	Investigar Incidente	Auditar: coleta de informações;
4.2.1.1	Investigar Incidente	Verificar log central, coletar informações do Firewall; coletar informações do DHCP; e outros afins ...
4.2.1.2	Investigar Incidente	Informações suficientes
4.2.1.3	Investigar Incidente	Informações insuficientes
4.2.1.4	Investigar Incidente	Solicitar dados ao STIC
4.2.2	Investigar Incidente	Recebimento de dados do STIC
4.3	Investigar Incidente	Dados confere com a notificação;
4.3.1	Investigar Incidente	Encaminhar para o tratamento
4.3.2	Investigar Incidente	Dados não confere com a notificação;
4.3.2.1	Investigar Incidente	Encaminhar para a resposta;
5	Tratar Incidente	Enviar solicitação do bloqueio do MAC(CORE);
5.1	Tratar Incidente	Recebimento de informação de bloqueio realizado;
5.2	Tratar Incidente	Informar ao STICou ao usuário (ou ambos) sobre o bloqueio realizado;
6	Responder	Responder ao Comunicante e ao reclamante;
7	Responder	Finalizar.

Fonte: Autoria própria.

Tabela 4 – Incidente: SPAM.

Passo	**Quem Faz ?**	**O Que Faz ?**
1	Usuário	Notificação interna de possível SPAM via e-mail;
2	Equipe de Segurança	Receber a notificação;
3	Analisar Incidente	Email notificando Sem email original
3.1	Analisar Incidente	Solicitar e-mail original;
3.1.1	Analisar Incidente	Encaminhar para a resposta
3.2	Analisar Incidente	Email notificando com email original
3.2.1	Analisar Incidente	Encaminhar para a Investigação
4	Investigar Incidente	Identificar fonte de origem;
4.1	Investigar Incidente	Encaminhar para o tratamento;
5	Tratar Incidente	Origem Interna: Auditar,
5.1	Tratar Incidente	Auditar: coleta de informações;
5.1.1	Tratar Incidente	E-mail legítimo;
5.1.2	Tratar Incidente	Encaminhar para a resposta;
5.1.3	Tratar Incidente	SPAM detectado;
5.1.3.1	Tratar Incidente	Notificar STIC e responsável;
5.2	Tratar Incidente	Origem Externa: Encaminhar para o CAIS;
5.3	Tratar Incidente	Aguardar resposta do responsável
5.4	Tratar Incidente	Encaminhar para resposta ao comunicante
6	Responder	Responder ao comunicante
7	Responder	Finalizar.

Fonte: Autoria própria.