UNIVERSIDADE FEDERAL DO PAMPA

CRISTIANO FERREIRA SCHUH

ANÁLISE E IMPLANTAÇÃO DE UMA FERRAMENTA DE GESTÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Alegrete
2015

CRISTIANO FERREIRA SCHUH

ANÁLISE E IMPLANTAÇÃO DE UMA FERRAMENTA DE GESTÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

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

Orientador: Cristiano Tolfo

Coorientador: Mauricio Fiorenza

Alegrete
2015

Ficha catalográfica elaborada automaticamente com os dados fornecidos
pelo(a) autor(a) através do Módulo de Biblioteca do
Sistema GURI (Gestão Unificada de Recursos Institucionais).

A000o Schuh, Cristiano Ferreira

Análise e Implantação de uma Ferramenta de Gestão de Tratamento de Incidentes de Segurança da Informação.

74 p.

Trabalho de Conclusão de Curso (Graduação) -- Universidade Federal do Pampa, BACHARELADO EM CIENCIAS DA COMPUTAÇAO, 2015.

"Orientação: Cristiano Tolfo".

1. 2. 3. I. Título.

CRISTIANO FERREIRA SCHUH

ANÁLISE E IMPLANTAÇÃO DE UMA FERRAMENTA DE GESTÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

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

Trabalho de Conclusão de Curso defendido e aprovado em: 30 de Novembro de 2015.
Banca examinadora:

Cristiano Tolfo

Prof. Dr. Cristiano Tolfo
Orientador
UNIPAMPA

Andréa P. Bordin

Prof. Dr. Andréa Sabedra Bordin
UNIPAMPA

Fernando Della Flora

Fernando Della Flora
UNIPAMPA

Dedico este trabalho inteiramente a minha família. Que sempre estiveram ao meu lado em todos os momentos, bons e ruins da minha vida.

AGRADECIMENTO

Começo agradecendo a minha querida e amada família: Pai, mãe e irmãos, pois sem vocês não estaria aqui, hoje! E em particular:

À minha mãe agradeço o incentivo de estar sempre à frente, a confiança que me depositou frente a todas as decisões e responsabilidades que escolhi assumir durante o curso, o exemplo de caráter e bravura, e perseverança na luta por aquilo que acredita ser o mais justo, valioso e digno. Sem nunca desistir, diante de qualquer dificuldade que a vida nos impôs, agradeço de coração por todos esses ensinamentos e pelas oportunidades. Saibas que te amo muito!

Aos meus irmãos, Diane e Mathias pelo carinho, atenção e pela união de todos, onde apesar das longas distâncias geográficas sempre se fizeram presentes em pensamento e afeto. Saibam que vocês além de irmãos, vocês são meus melhor amigos e que carrego cada um de vocês no meu coração. Amo vocês!

Ao meu amigo, Dr. Rônei, o qual considero como um pai, agradeço os conselhos, os ensinamentos, o carinho de suas muitas conversas em que tivemos. Agradeço também ao modo livre de me deixar escolher, e por mais que eu errasse, sempre estava presente quando precisava me reerguer. A sua disposição de estar sempre me ouvindo independente da hora ou do dia. Só tenho agradecer e dizer que essa conquista também é sua!

Ao meu orientador e meu professor Dr. Cristiano Tolfo, por ter me aceitado como seu orientado. Pela oportunidade de aprender, pelas disciplinas que as tive com o professor, pela enorme paciência em corrigir os meus textos, pela persistência de não aceitar tudo aquilo sempre dizendo que poderia ficar melhor, por me mostrar onde errei e me ensinar como corrigir e por todo tempo dedicado a mim.

Ao meu coorientador Mauricio Fiorenza, pela ajuda em transformar este trabalho de conclusão em realidade, ao tempo que disponibilizou dentro e fora do no local de trabalho para sanar as dúvidas e pelas críticas e sugestões dadas.

Aos meus amigos e colegas que estiveram comigo durante todo esse percurso, que de uma forma ou de outra estiveram presentes e me ajudaram diretamente e indiretamente a chegar até aqui.

A todos os professores da Universidade Federal do Pampa que transmitiram seus conhecimentos com dedicação, seriedade e maestria!

Minha enorme gratidão a todos que se fizeram presente nessa longa jornada, que embora tenha tido momentos tristes foi superada por muitos momentos de alegrias e desafios vencidos.

Muito obrigado a todos!

“Não desista nas primeiras tentativas a persistência é amiga da conquista. Se quer chegar aonde à maioria não chega, faça o que a maioria não faz”.

Bill Gates

RESUMO

A segurança da informação trata da proteção das informações que uma organização possui, eliminando os riscos que afetam a confidencialidade, integridade, disponibilidade e autenticidade dessas informações. Políticas de segurança da informação requerem um conjunto formal de regras que devem ser seguidas e irão constituir a gestão da segurança da informação da organização. Este trabalho de conclusão de curso tem como objetivo a análise e implantação de uma ferramenta de gestão de tratamento de incidentes de segurança da informação. Utilizando o estudo de caso o Núcleo de Tecnologia da Informação e Comunicação da Universidade Federal do Pampa, adotados de forma a compreender os principais conceitos da segurança da informação e incidentes de segurança ocorridos. Na análise do atual modelo de gestão de tratamento de incidentes de segurança da informação identificam-se pontos favoráveis para a implantação do novo modelo de gestão automatizado. Foi realizada a implantação de uma ferramenta que auxilie na gestão do tratamento de incidentes de segurança considerando os processos de segurança da informação executados no núcleo. A consolidação da implantação é dada por meio de um passo a passo da instalação que foi apresentado à equipe do Núcleo de Tecnologia da Informação e Comunicação. Verificou-se que a implantação da ferramenta pode acelerar os processos de resposta aos incidentes de segurança aumentando a segurança, automatizando processos, centralizando as informações e reduzindo custos com recursos humanos da organização.

Palavras-Chave: Segurança da informação, Politica de segurança da informação e Gestão da segurança da informação.

ABSTRACT

Information security is the protection of information that an organization has, eliminating the risks that affect the confidentiality, integrity, availability and authenticity of this information. Information security policies require a formal set of rules that must be followed and will be the organization's information security management. This course conclusion work aims at the analysis and implementation of a treatment tool management of information security incidents. Using the case study Information Technology and Communication Center of the Federal University of Pampa, adopted in order to understand the main concepts of information security and security incidents. In the analysis of the current information security incident handling management model they are identified favorable points for the implementation of the new automated management model. The implementation of a tool that assists in managing the treatment of security incidents taking into account the information security processes run in the core was carried out. The consolidation of deployment is given through a step by step installation that was presented to the Information and Communication Technology Center team. It was found that the deployment tool can speed up the response processes to security incidents increasing security by automating processes, centralizing information and reducing costs for human resources of the organization.

Keywords: Information security, security policy information and management of information security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CAIS – Centro de Atendimento de Incidentes de Segurança

CERT.br – Centro de Atendimento de Incidentes de Segurança

CERTS – Coordenadoria de Redes Infraestrutura e Suporte

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

CSIRT – *Computer Security Incident Response Team*

DDoS – *Distribued Denial of Service*

ITIL – *Information Technology Infrastructure Library*

ITSM – *Information Technology Service Management*

NIC.br – Núcleo de Informação e Coordenação do Ponto BR

NTIC – Núcleo de Tecnologia da Informação e Comunicação

OTRS – *Open Technology Real Services*

RPN – Rede Nacional de Ensino e Pesquisa

RT – *Request Tracker*

RTIR – *Request Tracker for Incident Responst*

SI – Segurança da Informação

TCC – Trabalho de Conclusão de Curso

TI – Tecnologia da Informação

TISI – Tratamento de Incidentes de Segurança da Informação

UNIPAMPA – Universidade Federal do Pampa

Sumário

1 INTRODUÇÃO

A segurança da informação é constituída por conceitos, que devem ser considerados em qualquer organização, porém a forma de implantação é particular para cada organização (FONTES, 2012).

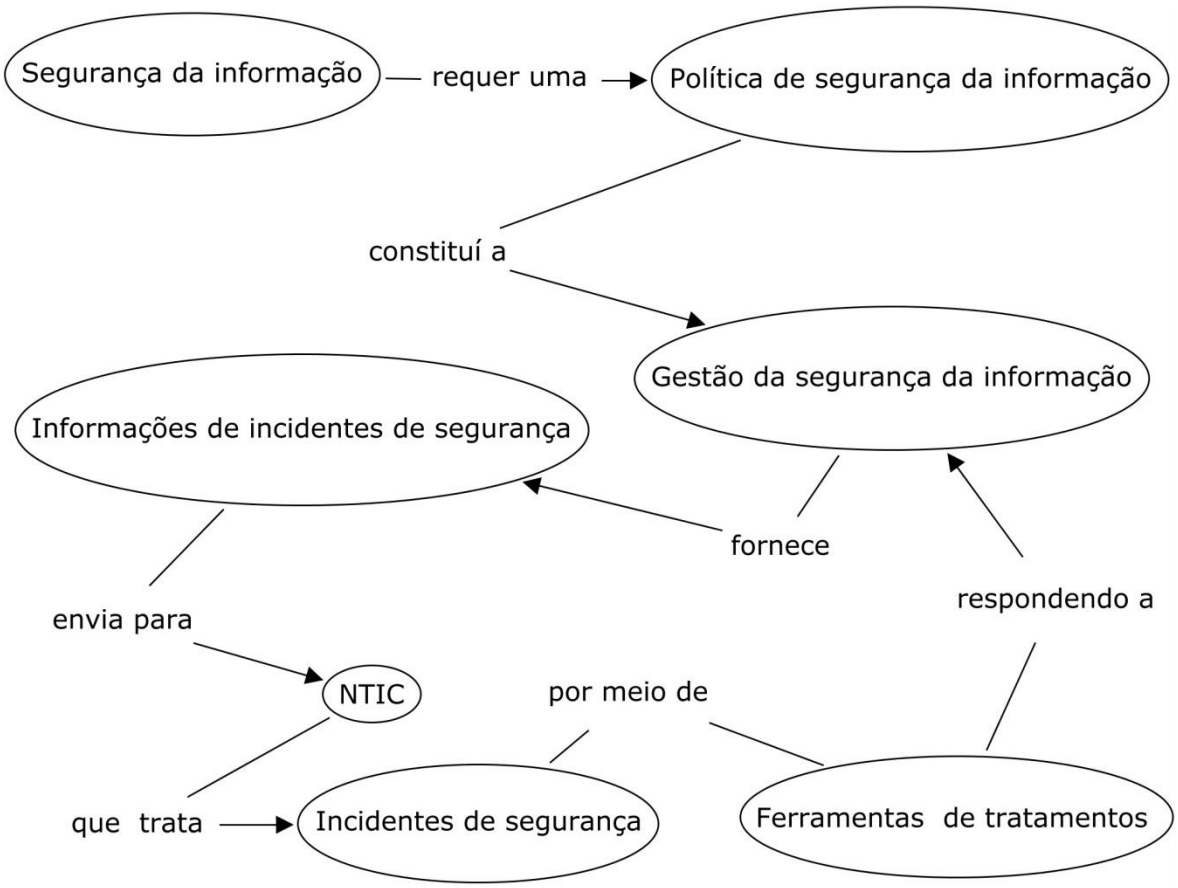
O gerenciamento dos riscos que uma informação está sujeita, pode ser controlada, por meio de uma gestão de segurança da informação com o auxilio de uma ferramenta de tratamento de incidentes de segurança da informação (TISI).

A grande quantidade de informações sendo armazenada em modo digital aumenta ano após ano, segundo SÊMOLA (2003), o que ressalta a importância da correta implantação da ferramenta do TISI. O uso adequado da ferramenta ajuda no funcionamento do sistema corporativo segundo o Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil que centraliza todas as informações sobre ocorrência de incidentes de segurança (CERT.br, 2012).

Ferramentas do TISI têm como objetivo melhorar a gestão da organização fornecendo relatórios gerados a partir das atividades que ameaçam a segurança da informação (SI). A automatização das respostas aos incidentes de segurança pode ser obtida por meio do *Open Technology Real Services* (OTRS), resultando na otimização dos processos dos TISI pelas equipes da SI.

A Universidade Federal do Pampa (UNIPAMPA) dispõe de políticas de SI que em conjunto com o Núcleo de Tecnologia da Informação e Comunicação (NTIC) é responsável pelo processo de detecção, tratamento e resposta dos incidentes de SI que ocorrem nos campus universitário e na reitoria. A Figura 1 exemplifica o processo de formação da gestão da SI no NTIC.

Figura 1- Gestão de tratamento de incidentes de segurança da informação do NTIC/UNIPAMPA.



.

No TISI do NTIC atualmente são utilizados recursos provisórios, sem o uso de um software apropriado para automatização dos processos. Com a análise realizada verificou-se quais as ferramentas de gestão TISI, podem atender os requisitos do NTIC, respeitando as normas e as políticas de segurança da UNIPAMPA. Assim esse trabalho de conclusão de curso tem como objetivo validar a análise e a implantação da ferramenta definida.

1.1 Objetivo geral

Implantar uma ferramenta de gestão de TISI de acordo com os requisitos do NTIC, respeitando as normas e politicas de SI da UNIPAMPA.

1.2 Objetivo específico

Para atender o objetivo geral deste trabalho apresentam-se os seguintes objetivos específicos:

- Automatizar o processo de TISI por meio de uma ferramenta de gestão de TISI.

- Conceber uma solução para a gestão do TISI que também possa ser utilizada por outras organizações atuam na SI.

- Gerar relatórios de incidentes de SI por meio da ferramenta de modo automático.

- Criar notificações internas, gráficos e respostas automáticas dos TISI por meio da ferramenta.

1.3 Justificativa

Segundo o Centro de Estudos, Resposta e tratamento de Incidentes de Segurança no Brasil (CERT.br, 2013) em todo o período do ano de 2013 notificou 352.925 incidentes, isso alerta as organizações que utilizam a internet. Os riscos que as informações e os dados correm ao estar disponível são: ataques virtuais, acesso não autorizado, spam, tentativa de fraudes, código malicioso, entre outros. Os conceitos da segurança da informação abordam os cuidados que a gestão do TISI deve adotar nas organizações. Em relação à segurança da informação:

> O primeiro e mais importante aspecto da segurança da informação é a politica de segurança. Se a segurança da informação fosse uma pessoa a politica da segurança seria o sistema nervoso. Politica é a base da segurança da informação, providencia a estrutura e define os objetivos dos demais aspectos da segurança da informação (PELTIER, 2005,p.17).

O mesmo autor defende a implantação de uma gestão de SI para melhorar o gerenciamento dos riscos e também propõem o uso de uma ferramenta de TISI.

> Um importante fator para o sucesso na implantação de um processo de segurança da informação é implantar uma completa arquitetura de gerenciamento de risco. Esta arquitetura deve estar

> conectada às politicas e aos padrões de segurança da informação e deve direcionar o risco para o negócio em um ambiente automático e contínuo (PELTIER, 2001,p.17).

A gestão da SI analisa o impacto provocado pelos incidentes SI, o que permite que a organização aprenda com seus erros, corrija suas falhas e impeça que os mesmos problemas se repitam no futuro (FERREIRA; ARAÚJO, 2008).

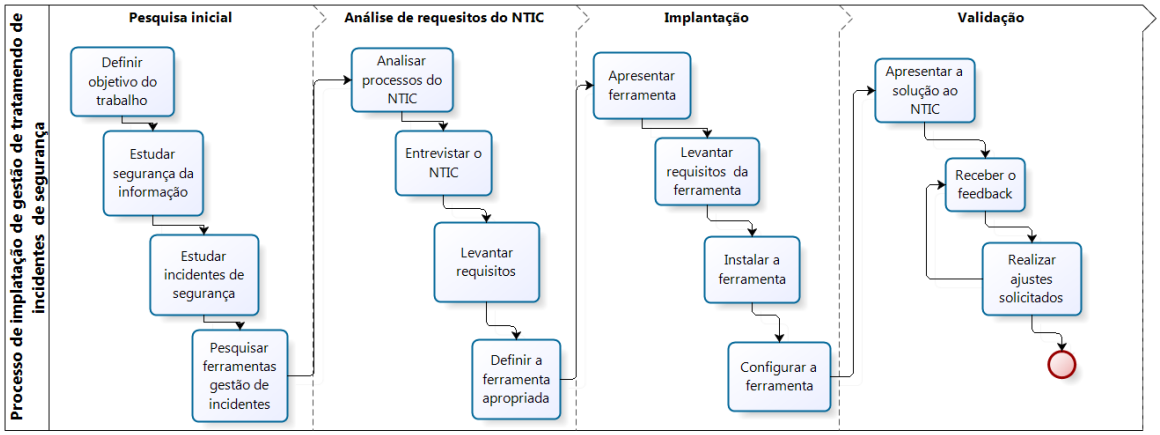
As informações sobre os incidentes de SI das organizações devem ser comunicadas ao *Computer Security Incident Response Team* (CSIRT), que provê serviços de suporte para prevenção, tratamento e respostas aos incidentes de segurança em computadores (CERT.br, 2012).

A eficiência do CSIRT na detecção dos incidentes de SI está relacionada a constantes atualizações por meio de outros CSIRT's, que auxiliam no desenvolvimento do processo de prevenção e TISI. No entanto, a forma de como a gestão dará inicio ao processo TISI dependera de cada organização. No NTIC suas características são peculiares, pois o ambiente de trabalho é heterogêneo, porém as questões da SI são transparente o que melhora a compreensão do seu funcionamento e das suas necessidades.

1.4 Metodologia e Etapas

A metodologia foi dividida em quatro etapas, onde será abordado os procedimentos utilizado no desenvolvimento deste trabalho. O estudo da fundamentação teórica da SI, análise da organização, possibilidade de implantação de uma ferramenta para TISI e a validação da solução pela equipe de SI do NITC. Como mostra a Figura 2.

Figura 2 - Cronograma de atividade.



Na Figura 2, podem-se visualizar as 4 etapas divididas em: Na primeira etapa, a pesquisa inicial sobre o assunto TISI e suas ferramentas. Abordando junto a ela as políticas de classificação e TISI, relatando sobre as principais entidades de apoio a segurança da informação.

Na segunda etapa, a análise está baseada no questionário Apêndice A – Questionário Realizado à Equipe do NTIC, realizada com o responsável do NTIC para auxiliar na escolha da ferramenta para o TISI.

Na terceira etapa, apresentar ao NTIC, a escolha da ferramenta e listar os requisitos para instalação, configuração execução da mesma.

A quarta e última etapa está relacionada à validação dos resultados obtidos após a implantação da ferramenta, avaliando a melhora na gestão do TISI do NTIC.

1.5 Estrutura do Trabalho

O TCC está dividido em capítulos para aborda melhor o tema, o capítulo 1 apresenta o estudo utilizado para alcançar os objetivos deste trabalho, assim como os objetivos gerais, objetivos específicos, justificativa e metodologia.

O capítulo 2 define os conceitos da SI e sua importância, classifica e descreve exemplos de incidentes de SI, abordando as entidades de apoio aos CIRTS.

O capítulo 3 apresenta as ferramentas encontradas para o TISI e descreve suas características, tendo como resultado uma tabela comparativa que será utilizada para definir a ferramenta a ser implantada.

O capítulo 4 aborda o estudo de caso, dos processos de TISI do NTIC, demostrados por meio da modelagem BPMN proposta por Pereira (2013). Essa modelagem descreve o modelo atual AS-IS e o modelo futuro TO-BE que será utilizado para implantação da ferramenta.

O capítulo 5 apresenta os resultados obtidos, a metodologia para os processos de instalação, configuração e validação da ferramenta OTRS para o TISI do NTIC divididos em 4 seções.

O capítulo 6 apresenta a possibilidade de trabalhos futuros em cima da ferramenta abordada e o capítulo 7, a conclusão do TCC- trabalho de conclusão de curso. Após seguem as referências e apêndice utilizados.

2 SEGURANÇA DA INFORMAÇÃO

Com o crescimento das informações armazenadas, disponibilizadas e transmitidas por meio digital, alerta as organizações sobre importância de possuir uma política SI eficiente. A segurança da informação requer uma politica que é baseada nos conceitos de: disponibilidade, integridade, confidencialidade, legalidade, autenticidade e não repúdio de autoria (FONTES, 2006).

Segurança da informação é "[...] uma área do conhecimento dedicada à proteção contra acessos não autorizados, alterações indevidas ou sua indisponibilidade" (SÊMOLA, 2003). De forma mais ampla para melhor compreensão, descrevemos os principais conceitos da SI, são eles:

- Confidencialidade, quando "[...] Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas" (SÊMOLA, 2003).
- Integridade, quando "[...] Toda a informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protege-las contra alterações indevidas, intencionais ou acidentais" (SÊMOLA, 2003).
- Disponibilidade, quando "[...] Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que for requerida independente da finalidade" (SÊMOLA, 2003).
- Autenticidade, propriedade que garante que a informação é proveniente da fonte anunciada e que não sofre alterações ao longo de um processo (FONTES, 2006).
- Não repúdio, propriedade que garante a impossibilidade de negar a autoria em relação a uma transação realizada anteriormente (FONTES, 2006).

2.1 Incidentes de segurança

O estado de alerta é dado a SI a quando um incidente é detectado, pois

> [...] um incidente de segurança é qualquer evento adverso, confirmado ou suspeito relacionado à segurança dos sistemas computáveis ou rede de computadores, ou seja, a ação de violar uma politica de segurança, explícita ou implícita (CERT.br, 2012).

O Centro de Atendimento a Incidente de Segurança – CAIS, em conjunto a Rede Nacional de Ensino e Pesquisa - RNP no ano de 2013, detectaram um grande número de incidentes que afetam a SI. As informações sobre esses incidentes, também são repassadas ao NTIC para que fiquem em alertam (CAIS, 2013). Os principais incidentes de SI detectados pelo CAIS e RNP são:

- Bot, conhecido por código malicioso tem como objetivo permitir que o atacante tenha acesso remotamente dos recursos do computador ou dispositivo atacado, assim tornando-o um hospedeiro para a disseminação de *malwares* e envio de *spams*. Esses incidentes são mais difíceis de serem descobertos, pois não seguem um padrão de desenvolvimento, e podem se comportar de varias formas diferentes de acordo com o dispositivo infectado (CERT.br, 2015).
- Botnet, é uma rede de *bots*, formado por um conjunto de dispositivos infectados com *bots* que são controlados pelos atacantes com fins específicos, quando maior a rede de *bots* mais poderosa é considerada o botnet (CERT.br, 2015).
- Tentativa de Intrusão, conhecido também por tentativa de exploração de vulnerabilidade são associados à *scan* que é um processo de varredura em redes de computadores com objetivo de localizar serviços e portas lógicas que estão ativas e podem ser exploradas para determinados ataques (CERT.br, 2015).
- Phishing, conhecida por fraude, técnica onde o atacante tenta se passar por outra pessoa ou instituição afim de ganhar a sua confiança e, assim, obter informação pessoais das vitimas como senhas, através de e-mails falsos de instituições bancárias por exemplo (CERT.br, 2015).
- Spam, classificado também como conteúdo abusivo, é amplamente usado para enviar e-mail não solicitado em grande quantidade. Aproveita da curiosidade e ingenuidade de suas vitimas para deixa-las mais vulneráveis a outros ataques, usa assuntos recentes da mídia para atrair a curiosidades de suas vitimas (CAIS, 2013)
- DDoS, também conhecido por não disponibilizar o serviço ou informação, são ataques de serviço com objetivo de degradar os sistemas, redes ou serviços. A atividade ocorre com o acionamento remotamente de máquinas infectadas que fazem parte de um botnet ou máquinas vulneráveis conectadas a internet,

atacando o alvo estabelecido, consumindo serviço gerando uma demanda insustentável, causando a indisponibilidade do serviço (CTIR.gov, 2015).

2.2 Tratamento de incidentes

Inicia-se o TISI com a notificação formal encaminhando-a, por meio de formulários, e-mail ou algum sistema informatizado específico, para a equipe responsável da tecnologia da informação (TI) o proprietário da informação (FERREIRA; ARAÚJO, 2008).

A notificação de incidente SI deve incluir dados suficientes, para o responsável da gestão do TISI, possa detectar a origem da ameaça maliciosa, permitindo providenciar medidas cabíveis (CERT.br, 2012). Os dados essenciais que devem estar incluídos em uma notificação são:

- Notificação: Mensagens de notificação que evidenciam a ocorrência do incidente;
- Horários: Data, hora e fuso horário dos logs ou da ocorrência notificada;
- Endereço: Origem do ataque, incluindo IP e porta da conexão.

Após o recebimento da notificação de incidente se faz necessário à análise para a resposta ao CSIRT. O CSIRT solicita que toda organização informe as atividades realizadas nos incidentes, para serem correlacionadas com outros incidentes ocorridos em outras organizações de forma a agilizar o TISI. As informações enviadas ao CSIRT podem ser utilizadas para determinar tendências e padrões incidentes de SI, e servirá para recomendar estratégias de prevenção adequadas (CERT.br, 2013).

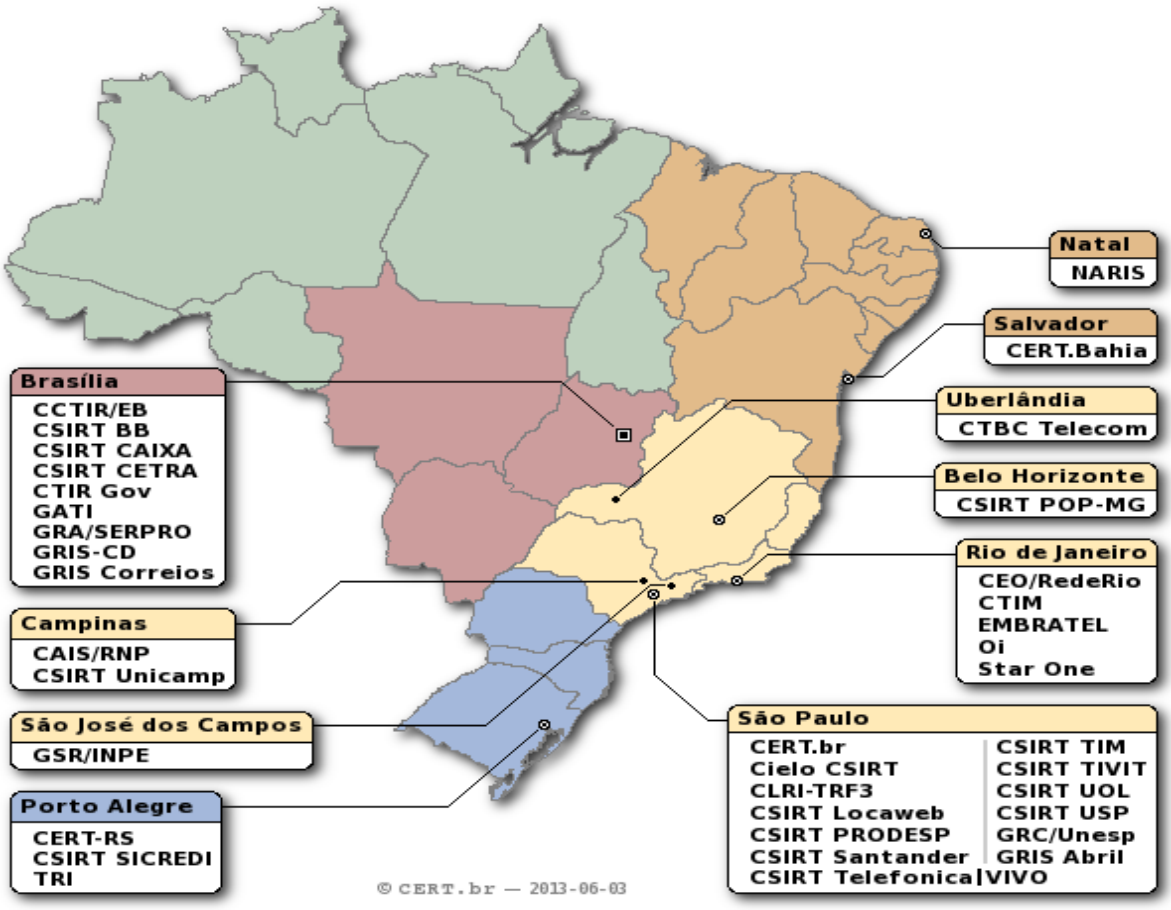
Para iniciar o TISI é necessária uma análise mais aprofundada das informações de acordo com a prioridade de ameaça do incidente. A resposta a um incidente pode assumir formas variadas. Um CSIRT pode

> [...] elaborar e divulgar recomendações para recuperação, contenção e prevenção, que são enviadas para os membros da comunidade por ele atendida e para os administradores de redes e sistemas que serão responsáveis por implementar os passos referentes à resposta ao incidente (CAIS, 2013).

2.3 Entidades de apoio à segurança da informação

As entidades de apoio a de SI tem a finalidade de tratar e prevenir os incidentes, estando ligadas umas com as outras elas compartilham seus conhecimentos para melhor a segurança na internet no Brasil. Na Figura 3 mostra alguns CSIRT's e onde eles estão localizados, entre eles o CTIR.gov um dos mais importantes CSIRT's que desenvolvem esse trabalho.

Figura 3- Localização das entidades de apoio. Adaptado de CERT.br (2013).



2.3.1 CSIRT

Um *Computer Security Incident Response Team* (CSIRT) é uma organização responsável por receber, analisar e responder notificações de atividades relacionadas aos

incidentes de segurança em computadores. Um CSIRT normalmente presta serviços para uma organização bem definida, que pode ser a entidade, como uma empresa, um órgão governamental ou uma organização acadêmica. Um CSIRT também pode prestar serviços para uma empresa, país, rede de pesquisa ou clientes que pagam por seus serviços (CERT.br, 2015).

2.3.2 CERT.br

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é uma organização que representa o CSIRT no Brasil responsável por centralizar todos os incidentes de segurança detectados por outros CSIRT's, mantido pelo Núcleo de Informação e Coordenação do Ponto BR - NIC.br, do Comitê Gestor da Internet no Brasil. O CERT.br é responsável pelo o TISI em computadores que envolvam redes conectadas à Internet brasileira (CERT.br, 2013).

Segundo o CERT.br (2014) seus objetivo são o TISI fornecendo suporte ao processos de recuperação e análise de sistemas comprometidos. Estabelece um trabalho colaborativo com outras entidades, como outros CSIRTs, empresas, universidades, provedores de acesso e serviços de Internet e backbones. Além disso, informa estatísticas públicas dos incidentes tratados e das reclamações de spam recebidas.

O CSIRT's como representante do país tem a responsabilidade de oferecer treinamentos na área de TISI, especialmente para os membros do CSIRTs e instituições que desejam criar seu próprio grupo. Também são funções do CSIRTs a produção de documentação de apoio para administradores de redes e usuários, com a preocupação de aumentar a capacidade de detectar incidente, correlacionando os eventos e determinando as tendências de ataques na internet brasileira.

2.3.3 CAIS

O Centro de Atendimento a incidentes de Segurança - CAIS, criado em 1997 tem como finalidade atuar na detecção, resolução, prevenção e promover uma melhoria contínua na questão da segurança de incidentes na rede acadêmica brasileira (CAIS, 2013). A Rede Nacional de Pesquisa - RNP também atua na segurança da informação, em conjunto ao CAIS para disseminar práticas de segurança nas redes RNP e nas demais instituições vinculadas. O CAIS tem como responsabilidade o atendimento aos incidentes

de segurança, coordenar grupos de segurança, incentivar à criação de novos grupos, distribuir informações, recomendar técnicas de tratamento e auxiliar no uso de ferramentas de TISI (CAIS, 2013).

3 FERRAMENTAS DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

As ferramentas disponíveis no mercado atendem a maioria das necessidades do TISI para a gestão da organização, mas poucas ferramentas possuem recurso de automatização dos procedimentos. O ganho de tempo na resposta ao incidente de SI proporciona uma redução nos custos em relação recursos humanos. Para atender as necessidades da gestão de TISI, a fim de aprimorar seus procedimentos, são listadas as seguintes ferramentas encontradas:

Clearing House for Incident Handling Tools - CHIHT não é uma ferramenta instalável, mas uma ferramenta web, que reunir as diretrizes para utilização de ferramentas no TISI. As informações encontradas referem-se às experiências de uma série de CSIRT´s Europeias, que trabalham em conjunto, como um projeto no âmbito do Grupo de Trabalho da TERENA TF-CSIRT que armazena as informações sobre as ferramentas que são utilizadas e apoiadas por outros CSIRT´s ativos (CHIHT, 2005).

System for Incident Response in Operational Security – SIRIOS é uma ferramenta com plataforma independente, GPL, tem suporte a vários idiomas via *templates* pré-configurados. Apresenta algumas funcionalidades como gerenciamento de contatos de segurança com instituições e possibilita a troca de informações com outros CSIRTs (KLINGMULLER, 2005).

Open Technology Real Services - OTRS, criada em 2001 é uma ferramenta de TISI que possui algumas funcionalidades como: gerenciamento dos incidentes notificados, código aberto, multiplataforma, 32 idiomas, escrito em linguagem ‘Perl’ e ‘JavaScript’, com licença pela *AFFero General Public License*. A ferramenta oferece não só suporte a *help desk*, mas também uma plataforma completa para a gestão de serviços de TI, como o módulo *Process Management* para automatizar os processos de TISI. A possibilidade de instalar pacotes de extensão, para diversas funcionalidades como o ITSM, que atua especificamente nos incidentes de SI (OTRS, 2014) .

Request Tracker – RT, criada pela BestPractical em 2001, é uma ferramenta de TISI com as seguintes características: possui rastreamento de bugs, código aberto, multiplataforma, licença de uso gratuita, atendimento ao cliente, processos de fluxo de trabalho , gerenciamento de mudanças e operações de rede. O RT é totalmente

customizável por meio de uma aplicação via *web* traduzido para 15 idiomas com interface móvel para iPhone, Andoird e dispositivos WebOS (BEST, 2002).

Visto as ferramentas citadas anteriormente para auxiliar na gestão, o RT e OTRS, possuem extensões especificas para o TISI que serão abordadas a seguir.

O Tratamento Automatizado de Incidentes de Rede - TRAIRA, ferramenta de extensão desenvolvida para o RT, ou seja, não pode ser usada sem ter o RT instalado. Desenvolvida pelo, CERT.Bahia (CSIRT do POP-BA/RNP) automatiza o procedimento de detecção, identificação e isolamento dos dispositivos geradores de incidentes de segurança em redes locais. O TRAIRA atua em todas as fases de TISI como preparação, detecção, análise, mitigação, recuperação e ações pós-incidente. Objetivo dessa extensão é a automatização nos processos de identificação e isolamento dos equipamentos causadores de incidentes de segurança com o suporte da a equipe do CERT.Bahia e da Universidade Federal da Bahia (TRAIRA, 2010).

Request Tracker for Incident Respost - RTIR, ferramenta de extensão do RT desenvolvida pela própria BEST PRACTICAL para o TISI, pode ser customizável, possui todas as características do RT e se comunica com outros CERTS´s e CSIRT´s. A extensão RTIR acrescenta algumas funcionalidades como: possibilidade de gerar relatórios em HTLM, auxilio na investigação do incidente, usa IP nativo do RT para IPV4 e IPV6 e gerenciamento de incidentes (BEST, 2002).

Information Technology Service Management - ITSM, ferramenta de extensão para o OTRS homologado pela Pink Elephant que tem suporte para seis processos descrito pelo framework ITIL. O ITSM atribui ao OTRS funcionalidades para o TISI como: recurso de criação de papéis para grupo de incidentes, catálogos de serviços, SLAs, gráfico de ocorrência de incidentes, atendimento a requisição de serviços, mudança de configuração e de ativos de serviços para outro nível de prioridade (OTRS, 2014).

Baseado nas informações de cada ferramenta de TISI citada anteriormente foi gerado uma tabela comparativa entre elas, como mostra a Tabela 1.

Tabela 1- Comparação das ferramentas para o TISI.

Ferramentas para TISI.	SIRIOS	OTRS	RT
Ferramenta instalável.	Sim	Sim	Sim

Multiplataforma.	Sim	Sim	Sim
Suporte de idioma.	Sim	Sim	Sim
Gerenciamento de contatos.	Sim	Não	Não
Comunicação com outros CSIRT´s.	Sim	Sim	Sim
Pacotes de extensão para o TISI.	Não	Sim	Sim
Licença gratuita de uso.	Não	Sim	Sim
Suporte técnico no Brasil..	Não	Sim	Não
Software com informações configuráveis.	Não	Sim	Sim
Suporte a dispositivos móveis.	Não	Sim	Sim
Compatibilidade com banco de dados MySQL, ORACLE, PostgreSQL.	Não	Sim	Sim
Compatível com IPV4 e IPV6.	Sim	Sim	Sim
Comunicação com o ITIL.	Sim	Sim	Não
Software de código aberto.	Não	Sim	Sim
Programado em linguagem perl.	Não	Sim	Não
Instalação simples com suporte.	Sim	Sim	Não
Geração de relatórios e gráficos.	Sim	Sim	Sim
Interface gráfica ajustável.	Sim	Sim	Sim
Gerenciamento de incidentes por equipes.	Não	Sim	Não
Compatível com servidores IMAP, POP3, SMTP.	Não	Sim	Não

Com o estudo realizado sobre as características de cada ferramenta foi definida que o OTRS com a extensão ITSM será implantado para a gestão TISI, pois, é a que contempla a maior parte dos requisitos e funcionalidades requeridas pelo NTIC. Os requisitos do NTIC foram extraídos a partir de um questionário Apêndice A tendo como requisitos básicos: gerenciamento de incidente, geração de relatório de atividade, geração de gráficos, possuir todas as informações dos incidentes entre outras funcionalidades. O OTRS também

atendeu os requisitos do modelo TO-BE que foi apresentado pela equipe do NTIC nas entrevistas realizadas e será exemplificado no capítulo 4.3.

4 ESTUDO DE CASO

O estudo de caso desta monografia é sobre o NTIC da UNIPAMPA que segundo eles

> [...] é um órgão complementar da reitoria da Universidade Federal do Pampa, que tem como objetivo criar e manter condições para o correto funcionamento sistêmico das atividades relacionadas à tecnologia da informação e comunicação, a fim de fornecer suporte ao desenvolvimento do ensino, pesquisa, extensão, gestão e serviços à comunidade, de acordo com as normas da UNIPAMPA (NTIC, 2010).

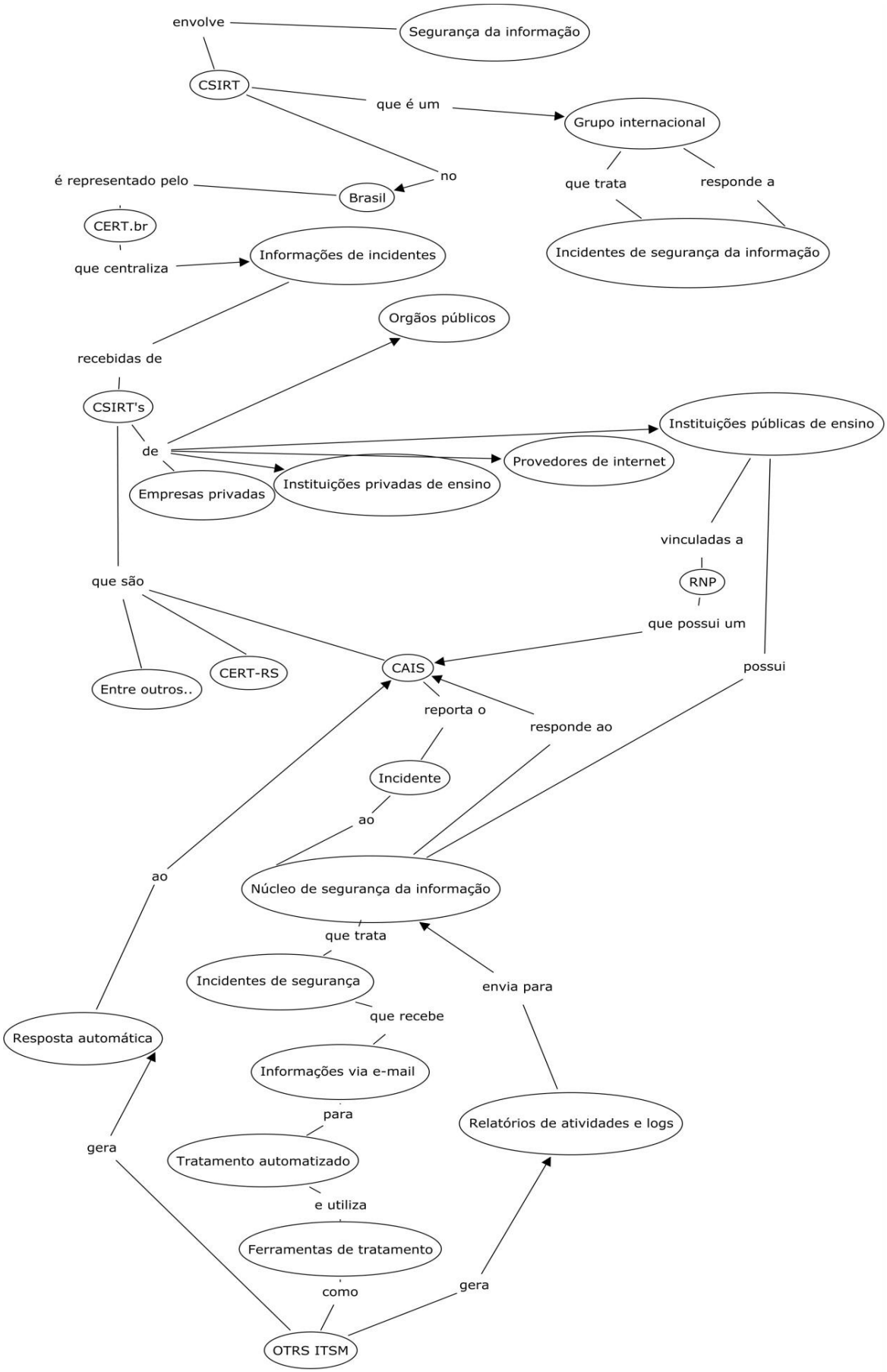
O NTIC tem como umas das suas responsabilidades manter apto o funcionamento e um contínuo processo evolutivo do seu sistema de SI. Com isso, este trabalho estuda implantar uma ferramenta que ajude na automatização para o TISI. Relacionando as necessidades com as funcionalidades que o OTRS possui para atender os requisitos extraídos das respostas dadas no questionário no apêndice A, junto às normas e politicas do NTIC (NTIC, 2010).

Nos seguintes itens seguintes desta seção será apresentada, a estrutura organizacional da arquitetura de SI, os processos executados pela equipe do NTIC, apresentando o modelo atual AS-IS e o modelo TO-BE modelo futuro. A gestão de TISI, com a coleta dos requisitos do NTIC por meio da planilha de registro de notificação de incidentes de segurança da informação.

4.1 Sistema de segurança do NTIC

A arquitetura de segurança do NTIC esta demostrada na Figura 4.

Figura 4 - Arquitetura do NTIC.

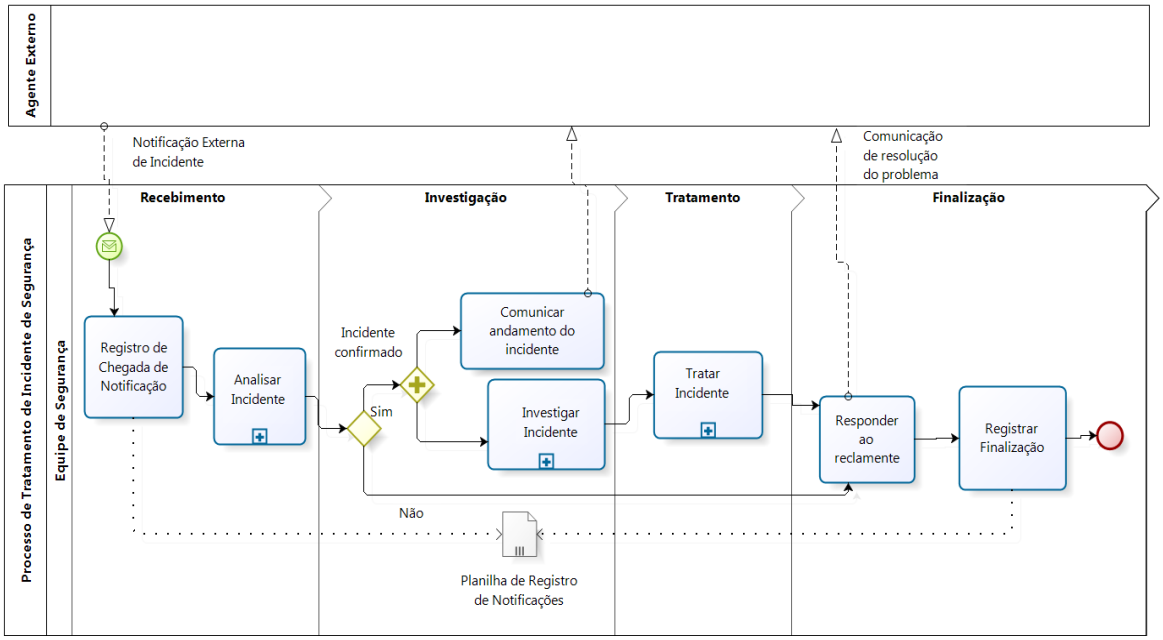


Os processos que evolve essa arquitetura foram mapeados por Pereira (2013) em duas partes. A primeira parte é o modelo AS-IS que assegura a forma de como o sistema esta em andamento pelo NTIC a segunda parte é o modelo TO-BE que sugere melhorias nos processos. Com o modelo AS-IS são demostrado o processo de TISI, onde foi possível notar a necessidade de uma ferramenta de apoio a gestão de TISI. No modelo TO-BE tem-se a visão de como este processo deverá ficar depois da implantação da ferramenta de gestão do TISI.

4.2 Modelo AS-IS

O modelo AS-IS do TISI do NTIC segundo Pereira, (2013) refere-se como ocorrem às notificações e os tratamentos que a equipe do NTIC desenvolve para incidentes de segurança externos, como mostra a Figura 5.

Figura 5 - Modelagem AS-IS notificação de incidente.



FONTE: Adaptado de PEREIERA, 2010.

Como pode ser observado na Figura 5 a modelagem é dividida em 4 etapas são elas; o recebimento, investigação, tratamento e finalização, envolvendo duas entidades o CAIS chamado de agente externo e o NTIC chamado de equipe de segurança.

A modelagem refere-se aos incidentes de segurança externos, a primeira etapa, chamada de recebimento, trata uma suspeita de um incidente de segurança onde o agente externo notifica a equipe com o envio de um e-mail contendo as informações para tomar às ações necessárias, então, a equipe de segurança realiza o registro desta notificação em uma planilha de registro de notificações.

A segunda etapa ocorre à investigação para saber se houve ou não um incidente de segurança, no caso de não se confirmar o incidente uma resposta é enviada para o reclamante, o CAIS. No caso de confirmação do incidente, comunica-se o agente externo, e prossegue a etapa de investigação, que tem como objetivo classificar e descobrir a origem do mesmo.

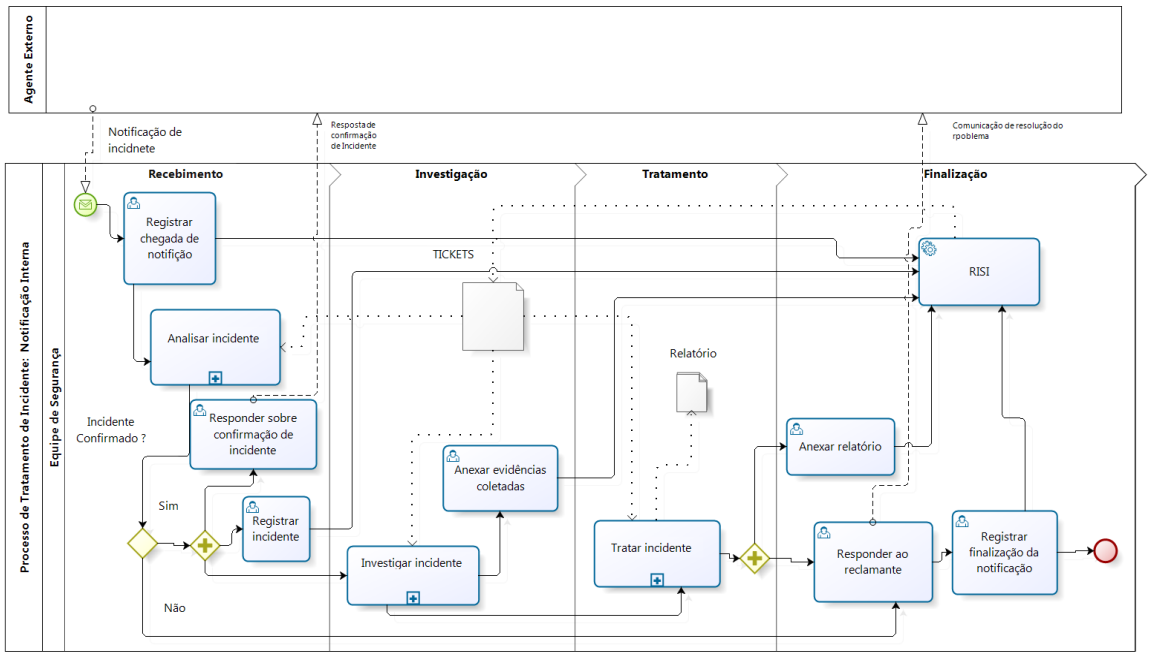
Na terceira etapa refere-se ao TISI realizando pelo NTIC. Na quarta etapa ocorre a finalização que consistem em enviar uma resposta ao agente externo sobre o tratamento realizado no incidente, o registro dessas atividades e o relatório de conclusão das etapas realizadas (PEREIRA, 2013).

4.3 Modelo TO-BE

O modelo TO-BE do TISI foi proposto por Pereira (2013) para melhorar os processos de tratamento e resposta dos incidentes de segurança. A maior parte dos incidentes identificados de origem interna pode ser visualizada como indisponibilidade do serviço ou verificações de rotina por algum membro da equipe. Ressaltando o uso de equipamentos que detectam essas ocorrências automaticamente evitando danos maiores a instituição por esses incidentes de segurança.

Uma nova modelagem foi realizada segundo Pereira (2013), sugere o uso de ferramentas como uma solução para a gestão do NTIC, com a implantação de um repositório de incidentes de segurança para o TISI, como pode ser visualizado na Figura 6.

Figura 6 - Modelagem TO-BE de notificação de incidente. Adaptado de Pereira (2010).



FONTE: Adaptado de PEREIERA, 2010.

Na Figura 6, segundo Pereira (2013), a implementação da questão de tempo para o registro da notificação pelo agente externo referindo-se ao CSIRT que no caso do NTIC é o CAIS. A resposta de confirmação para o agente externo e a modelagem do modelo TO-BE propõe a implantação do repositório de incidentes de segurança da informação para a substituição da planilha de registo de notificações. A geração automática de *tickets* contendo o número original e criando o novo número para controle interno do NTIC irá substituir o registro dessa ocorrência na planilha de registros manual. Na versão TO-BE o processo de cada ocorrência será armazenada no repositório de incidentes de segurança que no caso será o OTRS.

4.4 Planilha de registro de notificações

A planilha de registro de notificações do modelo AS-IS no processo de TISI é utilizada para registrar os procedimentos realizados nos incidentes de segurança como mostra a Figura 7. Nesta Figura é possível observar alguns exemplos do registro de incidentes de SI ocorridos na UNIPAMPA.

Figura 7 - Planilha de registro de notificações de incidentes de seguranças de informação do NTIC/UNIPAMPA.

	A	B	C	D	E	F	G	H	I	J	K
1	Ticket	Data Incidente	Notificação / Identificação	Data de Abertura	Data de Encerramento	Nº Externo	Classificação	Subclassificação	Unidade	Responsáveis pela Investigação	Relatório
2							2014				
3	IS2014006	19/5/14	20/5/14	21/5/14	22/5/14	57cxxxxxxxxxx	DDoS	DDoS	Campus A	Analista A	http://link retatorio
4	IS2014007	22/5/14	23/5/14	23/5/14	3/6/14	f7exxxxxxxxxx	Configuração	Configuração	Campus B	Analista A	http://link retatorio
5	IS2014008	29/5/14	30/5/14	2/6/14	3/6/14	adaxxxxxxxxxx	Host Infectado	Código malicioso	Campus A	Analista C	http://link retatorio
6	IS2014009	2/6/14	3/6/14	3/6/14	3/6/14	2c7xxxxxxxxxx	Host Infectado	Downadup	Campus C	Analista A	http://link retatorio
7	IS2014010	3/6/14	4/6/14	4/6/14	4/6/14	63cxxxxxxxxxx	Host Infectado	Downadup	Campus C	Analista B	http://link retatorio
8	IS2014011	5/6/14	6/6/14	6/6/14	6/6/14	8b7xxxxxxxxxx	Host Infectado	Downadup	Campus A	Analista C	http://link retatorio
9	IS2014012	7/6/14	8/6/14	9/6/14	10/6/14	7ddxxxxxxxxxx	Host Infectado	Downadup	Campus D	Analista B	http://link retatorio
10	IS2014013	10/6/14	11/6/14	11/6/14	11/6/14	8f3xxxxxxxxxx	Host Infectado	Downadup	Campus B	Analista C	http://link retatorio
11	IS2014014	15/6/14	16/6/14	16/6/14	17/6/14	902xxxxxxxxxx	Host Infectado	Downadup	Campus A	Analista A	http://link retatorio
12	IS2014015	25/6/14	26/6/14	26/6/14	26/6/14	319xxxxxxxxxx	Host Infectado	Bot	Campus C	Analista A	http://link retatorio
13	IS2014016	1/7/14	2/7/14	2/7/14	2/7/14	10fxxxxxxxxxx	Host Infectado	Bot	Campus A	Analista A	http://link retatorio

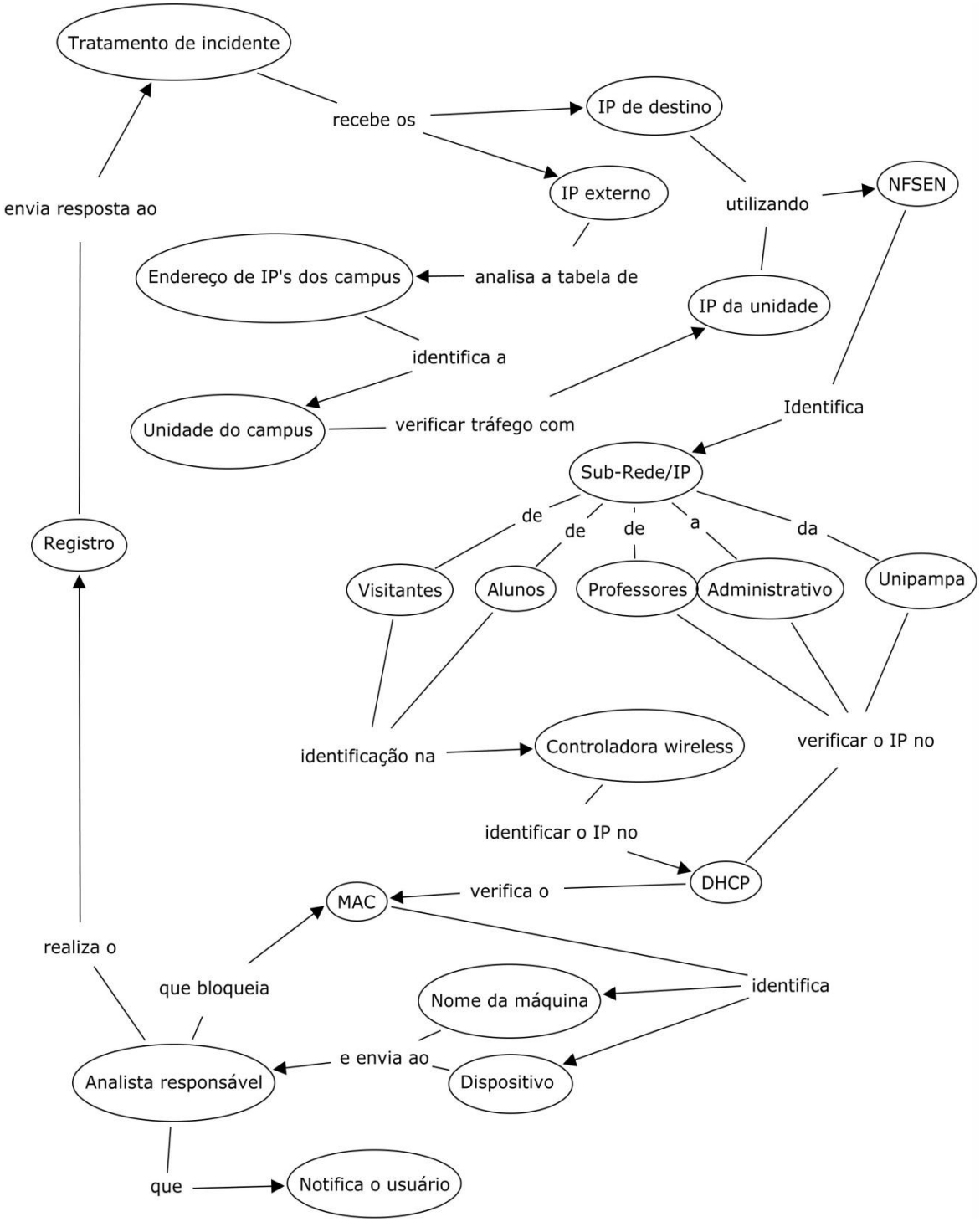
Como pode ser visto na Figura 7 a planilha de registro de notificações de incidentes é composta por 11 colunas composta por: *ticket*, data do incidente, data de notificação, data de abertura, data de encerramento, número de externo, classificação, subclassificação, unidade, responsáveis pela investigação e o link para o relatório. Cada uma destas colunas é preenchida da seguinte forma:

- O *ticket* é gerado pelo analista responsável pelo incidente que segue uma ordem no formato: exemplo IS20140013 onde IS significa incidente de segurança, os quatro primeiros dígitos da esquerda para direita o ano 2014 e os quatros últimos dígitos o a contagem de incidentes no caso o décimo terceiro caso do ano.
- A data inicial do incidente é informada pelo agente o externo o CAIS/RNP que faz o monitoramento da rede externa da UNIPAMPA.
- Data de notificação informada pelo NTIC confirmando o recebimento desta notificação.
- A data de abertura refere-se quando o incidente foi aberto para o processo de análise e investigação pelo NTIC.
- Data de encerramento é dada pelo final do processo de análise e tratamento, junto com a resposta de fechamento ao CAIS/RNP.

- Número de externo é o ID emitido pelo CAIS identificando o incidente, cada incidente recebe um ID diferente.
- Classificação é dada ao tipo de incidente, esta classificação esta composta por: host infectado, violação de Copyrigts, envio de span, arquivo malicioso, varredura de portas, phishing, tráfego suspeito, DDoS entre outros.
- A subclassificação de incidentes é: *bot, downadup, torrent, span*, invasão, trafego suspeito e DDoS usada para identificar um incidente que possui mais de um tipo de técnicas que causa um incidente exemplo um Host infectado pode ser causado por um *bot* ou um *downadup*.
- Unidade representa todas as unidas da UNIPAMPA que são: NTIC, Reitoria, Alegrete, São Gabriel, Bagé, Santana do Livramento, Caçapava, Jaguarão, São Borja, Itaqui e Uruguaiana.
- Os responsáveis pela investigação são os membros da equipe do NTIC, os mesmos investigam e respondem sobre aquele incidente denominado a ele. A equipe e os responsáveis podem variar de acordo com os componentes existente na época do tratamento do incidente de segurança.
- Relatório é visualizado por meio de um *link* que foi gerando pelos membros da equipe onde constam todos os passos realizados durante a análise e investigação de um incidente de segurança, anexando o recebimento do incidente, os logs e evidências.

As informações listadas acima são necessárias para o preenchimento da planilha de registo que são frutos da investigação. Dependendo do incidente o mesmo incidente pode assumir a mesma classificação, mas sua suas informações como, subclassificação, unidade, responsável e outros, podem ser diferentes. A Figura 8 mostra o exemplo das atividades realizadas para um incidente do tipo vírus, que são registradas na planilha de registros de notificações.

Figura 8 - Exemplo de tratamento de incidente de vírus.



Como pode ser visualizada na Figura 8, a forma que é realizada o TISI também está proposta no modelo TO-BE. Após a etapa de investigação se inicia a etapa tratamento realizando os procedimentos desenvolvidos pelo analista responsável do NTIC. Esses

procedimentos de tratamento podem variar de acordo com o tipo de incidente, origem do incidente e analista responsável do NTIC.

5 RESULTADOS OBTIDOS

A realização do estudo sobre SI com foco em incidentes de segurança e a análise das ferramentas disponíveis para o TISI obteve como resultados obtidos:

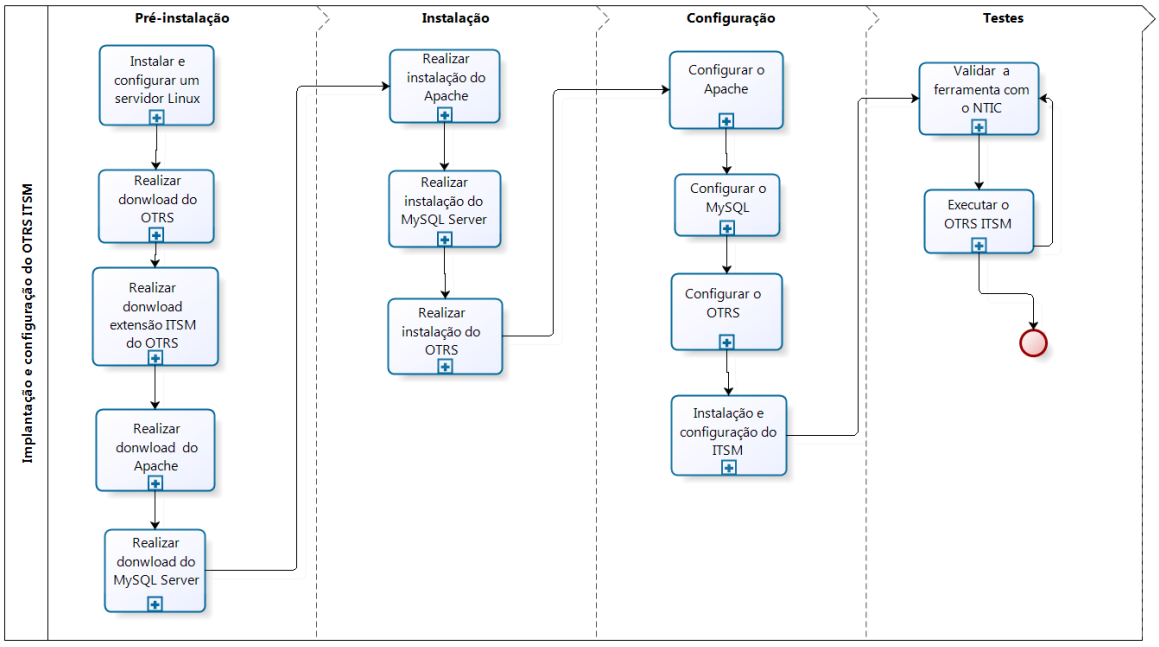
A implantação e configuração do OTRS ITSM para aprimorar os processos da gestão do TISI do NTIC.

O atendimento as solicitações sugeridas pelo NTIC no modelo AS-IS para o modelo TO-BE citadas no capítulo 4 seção 3.

A execução da ferramenta OTRS ITSM foi submetida à validação dos requisitos requisitados pelo NTIC como: histórico de atividades realizadas no incidente, substituir a planilha de registro de atividades, notificar ocorrência de incidentes internos, anexar tratamento realizado pelo responsável junto à resposta do incidente, entre outras melhorias que estão listadas na Tabela 1 de comparação entre os modelos AS-IS e TO-BE.

Para alcançar os resultados objetivos se fez necessário à realização de um cronograma de implantação da ferramenta de TISI como mostra a Figura 9.

Figura 9 - Cronograma de implantação do OTRS.



A Figura 9 esta dividida em quatro passos que contemplam o cronograma de implantação do OTRS e serão detalhadas nos próximos capítulos.

5.1 PRÉ-INSTALAÇÃO E INSTALAÇÃO

O primeiro passo da pré-instalação é disponibilizar o ambiente de trabalho que consiste em uma máquina com o sistema operacional Linux Ubuntu Server 14.04.1 configurado. Após a máquina estando apta para trabalhar, deve-se realizar o downloads das seguintes ferramentas básicas que serão utilizadas e instaladas no servidor Linux, são elas:

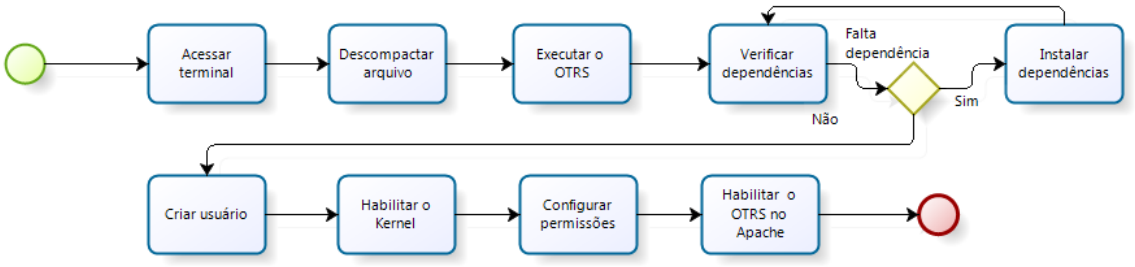
1. Realizar o download do OTRS 3.3.8 através do terminal para a pasta do sistema operacional "/opt/" do através do comando abaixo:
   - sudo wget http://ftp.otrs.org/pub/otrs/otrs-3.3.8.tar.bz2
2. Realizar os downloads dos pacotes ITSM 3.3.8 pela interface gráfica através do endereço http://ftp.otrs.org/pub/otrs/itsm/packages33/, são eles:
   - General Catalog 3.3.8
   - ITSM Core 3.3.8
   - ITSM Incident Problem Management 3.3.8
   - ITSM Configuration Management 3.3.8
   - ITSM Change Management 3.3.8
   - ITSM Service Level Management 3.3.8

Segundo passo, realizar os downloads e a instalação das ferramentas Apache2, MySQL e o Perl, utilizando o gerenciador de pacotes do próprio sistema operacional o Linux Ubuntu, o apt-get a partir dos seguintes comando:

1. Instalar o servidor web o Apache2.
   - sudo apt-get install apache2
2. Instalar o banco de dados o MySQL Server, durante a instalação um usuário e senha devem ser criados como administrador do banco de dados:
   - sudo apt-get install mysql-server
   - sudo apt-get install libapache2-mod-perl2
3. Instalar a linguagem de programação multiplataforma Perl:
   - sudo apt-get install perl

O próximo passo é a instalação do OTRS que é feita manualmente seguindo um passo a passo como é descrito a seguir. A Figura 10 mostra o subprocesso de instalação do OTRS, contendo nove passos necessários.

Figura 10 - Subprocesso de instalação do OTRS.



Iniciar o terminal Linux e acessar a pasta /opt/, todos os procedimentos a seguir deveram ser executados dentro desta pasta.

1. Descompactar o arquivo com o OTRS com o comando:
   - sudo tar jxvpf otrs-3.3.8.tar.bz2
2. Renomear pasta otrs-3.3.8.tar.bz2 para otrs com o comando:
   - sudo mv otrs-3.3.8 otrs
3. Executar o módulo de verificação de dependências do OTRS com o comando:
   - /opt/otrs/bin/otrs.CheckModules.pl

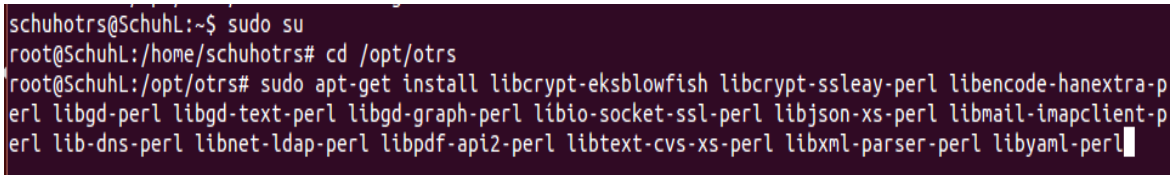
Ao executar o comando citado a cima será realizada uma verificação de dependências das bibliotecas do sistema que precisam ser instaladas para que o OTRS funcione corretamente, como mostra a Figura 11.

Figura 11- Dependências do OTRS

```
schuhotrs@schuhotrs-VirtualBox:/opt/otrs$ bin/otrs.CheckModules.pl
  o Archive::Tar.....................ok (v1.90)
  o Crypt::Eksblowfish::Bcrypt.......Not installed! (optional - For strong passw
ord hashing.)
  o Crypt::SSLeay....................Not installed! (optional - Required for Gen
eric Interface SOAP SSL connections.)
  o Date::Format.....................ok (v2.24)
  o DBI..............................Not installed! (required - Please install t
his module - )
  o DBD::mysql.......................Not installed! (optional - Required to conn
ect to a MySQL database.)
  o DBD::ODBC........................Not installed! (optional - Required to conn
ect to a MS-SQL database.)
  o DBD::Oracle......................Not installed! (optional - Required to conn
ect to a Oracle database.)
  o DBD::Pg..........................Not installed! (optional - Required to conn
ect to a PostgreSQL database.)
  o Encode::HanExtra.................Not installed! (optional - Required to hand
le mails with several Chinese character sets.)
  o GD...............................Not installed! (optional - Required for sta
ts.)
    o GD::Text.......................Not installed! (optional - Required for sta
ts.)
    o GD::Graph......................Not installed! (optional - Required for sta
ts.)
  o IO::Socket::SSL..................ok (v1.965)
  o JSON::XS.........................Not installed! (optional - Recommended for
faster AJAX/JavaScript handling.)
  o List::Util::XS...................ok (v1.27)
  o LWP::UserAgent...................ok (v6.05)
  o Mail::IMAPClient.................Not installed! (optional - Required for IMA
P TLS connections.)
    o IO::Socket::SSL................ok (v1.965)
  o ModPerl::Util....................Not installed! (optional - Improves Perform
ance on Apache webservers dramatically.)
  o Net::DNS.........................ok (v0.68)
  o Net::LDAP........................Not installed! (optional - Required for dir
ectory authentication.)
  o Net::SSL.........................Not installed! (optional - Required for Gen
eric Interface SOAP SSL connections.)
  o PDF::API2........................Not installed! (optional - Required for PDF
 output.)
    o Compress::Zlib.................ok (v2.060)
  o Text::CSV_XS.....................Not installed! (optional - Recommended for
faster CSV handling.)
  o Time::HiRes......................ok (v1.9725)
  o XML::Parser......................Not installed! (optional - Recommended for
faster xml handling.)
  o YAML::XS.........................Not installed! (required - Please install t
his module - )
schuhotrs@schuhotrs-VirtualBox:/opt/otrs$
```

Na Figura 11 podemos verificar todas as dependências listadas em amarelo e vermelho como ‘Not installed!’ que são bibliotecas que necessitam ser instaladas. Para isso deve-se utilizar o gerenciador de pacotes apt-get do Linux Ubuntu, dentro da pasta /opt/otrs, execute os comandos listados na Figura 12.

Figura 12 - Comandos para instalar as dependências de bibliotecas do OTRS.

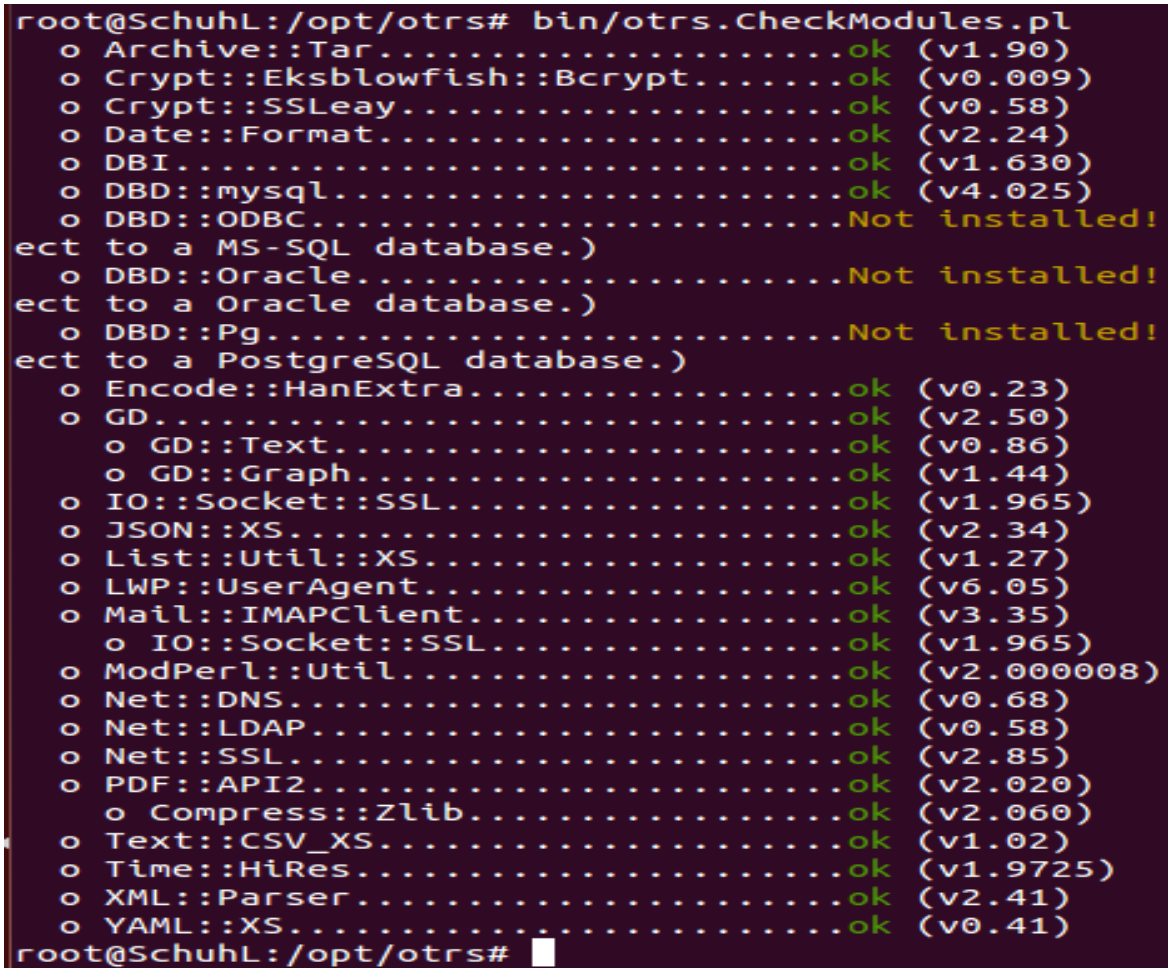


Os comandos que são visualizados na Figura 12 podem ser executados de forma individual para acompanhar a instalação passo a passo de cada biblioteca, seguindo a seguinte ordem de comandos listados abaixo:

- sudo apt-get install libcrypt-eksblowfish
- sudo apt-get install libcrypt-ssleay-perl
- sudo apt-get install libencode-hanextra-perl
- sudo apt-get install libgd-perl
- sudo apt-get install libgd-text-perl
- sudo apt-get install libgd-graph-perl
- sudo apt-get install líbio-socket-ssl-perl
- sudo apt-get install libjson-xs-perl
- sudo apt-get install libmail-imapclient-perl
- sudo apt-get install lib-dns-perl
- sudo apt-get install libnet-ldap-perl
- sudo apt-get install libpdf-api2-perl
- sudo apt-get install libtext-cvs-xs-perl
- sudo apt-get install libxml-parser-perl
- sudo apt-get install libyaml-perl

Após a instalação desses pacotes é necessário conferir se todas as dependências foram satisfeitas com mostra a Figura 13 repetindo o comando “/opt/otrs/bin/otrs.CheckModules.pl” no terminal Linux.

Figura 13 – Dependências instaladas do OTRS.



Na Figura 13 as dependências que constam como “ok” estão instalados e pode ser utilizado pelo o OTRS. No entanto, ainda constam como dependência como “Not installed!” que se refere ao banco de dados ODBC, Oracle e PostgreSQL que neste caso não serão utilizados, pois, o banco de dados escolhido para esta instalação é o MySql Server.

Ao finalizar as dependências do OTRS, próximo passo é a criação do usuário OTRS como os seguintes comandos dentro da pasta /opt/otrs:

Criar um usuário para o OTRS chamado otrs com o comando no terminal:

- sudo user add –d /opt/otrs/ -c ‘OTRS user’ otrs

Adicionar o usuário otrs ao grupo chamado www-data ao servidor Apache2 com o comando:

- sudo usermod –a –G www-data otrs

Próximo passo do subprocesso e instalação do OTRS é habilitar o Kernel para o funcionamento de escalação.

Este comando copia a Config.pm.dist para Config.pm

- sudo cp Kernel/Config.pm.dist Kernel/Config.pm

Este comando habilita envio de escalação e notificação do OTRS copiando a configuração do GenericAgent.pm.dist para GenericAgent.pm.

- sudo cp Kernel/Config/GenericAgent.pm.dist Kernel/Config/GenericAgent.pm

Ao finalizar o processo de habilitar o kernel prossegue o processo de configuras as permissões para o usuário do OTRS para a pasta /opt/otrs:

Usando o comando abaixo concedemos todas as permissões ao usuário otrs e ao grupo otrs do servidor web.

- sudo bin/otrs.SetPermissions.pl --otrs-user=otrs --web-user=www-data --otrs-group=www-data --web-group=www-data /opt/otrs

Após liberar as permissões é preciso habilitar o OTRS dentro do Apache com os seguinte comando :

- sudo su ln –s /opt/otrs/script/apache2-httpd.include.conf /etc/apache2/sites-available/otrs.conf

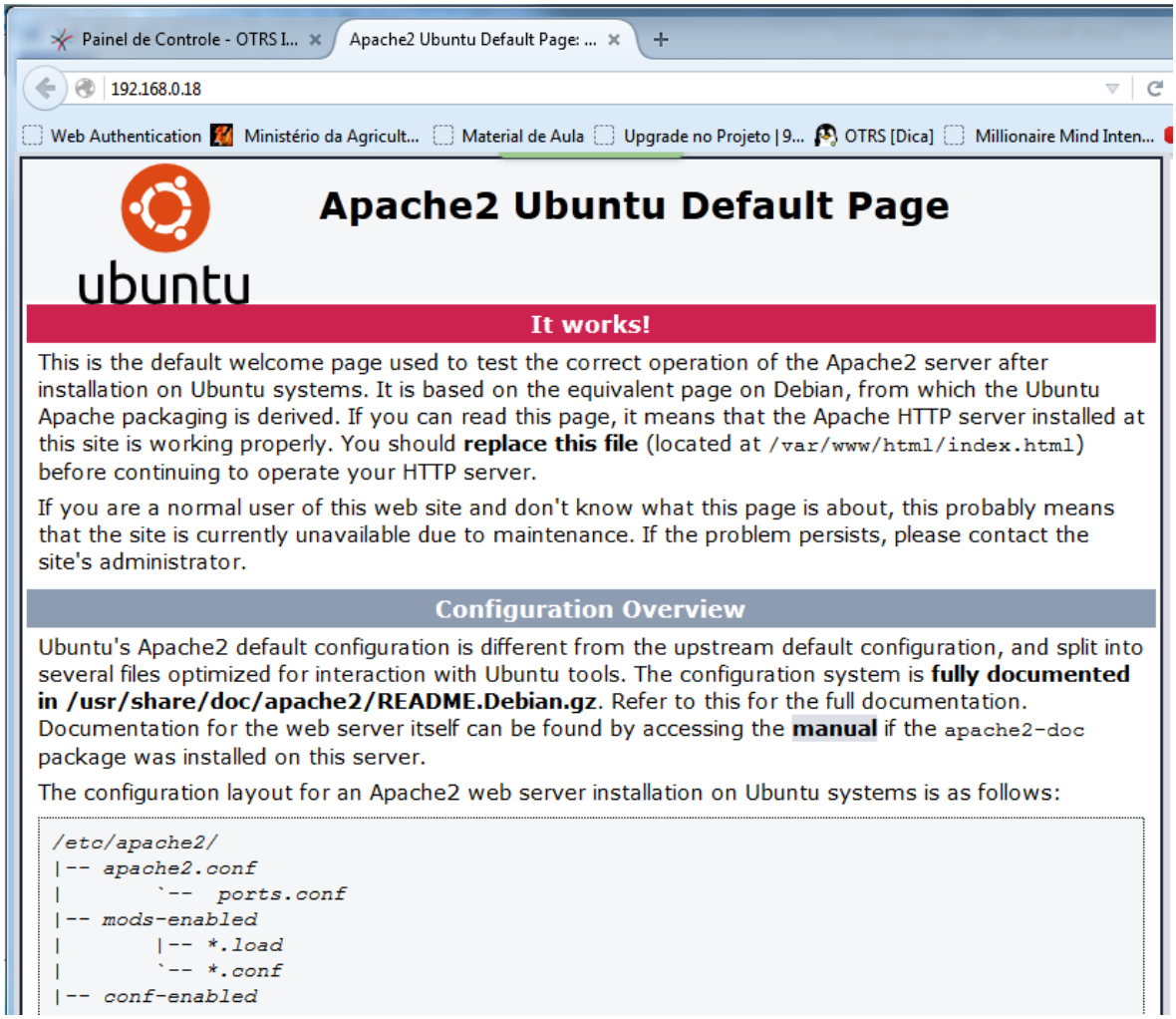
Logo é necessário ativar o apache e recarregar as configurações com os comandos:

- a2ensite otrs
- service apache2 reload

5.2 CONFIGURAÇÃO DO OTRS E EXTENSÃO ITSM

Na etapa de configuração se faz necessário a configuração do Apache, MySQL Server, OTRS na instalação e configuração do ITSM. A configuração do Apache2 não foi alterada deixando no modo padrão como mostra a Figura 14.

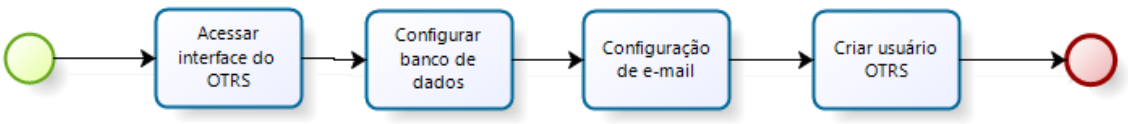
Figura 14 – Configuração do apache.



Na Figura 14 pode se visualizar e verificar a instalação bem sucedida do Apache2 através do IP do servidor Linux a configuração padrão do Apache2.

A configuração do MySQL server esta demonstrada pelo subprocesso configuração do usuário OTRS, como mostra a Figura 15.

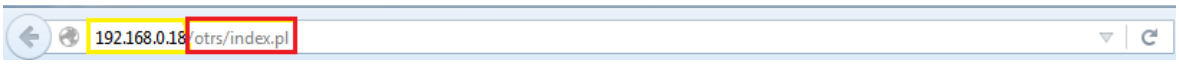
Figura 15 - Configuração do usuário OTRS pela interface.



A Figura 15 mostra a configuração do OTRS usando a interface gráfica através do navegador, durante esses processos um novo banco de dados é criado.

O processo de configuração do OTRS só pode ser realizado através da interface gráfica, com o navegador como mostra a Figura 16.

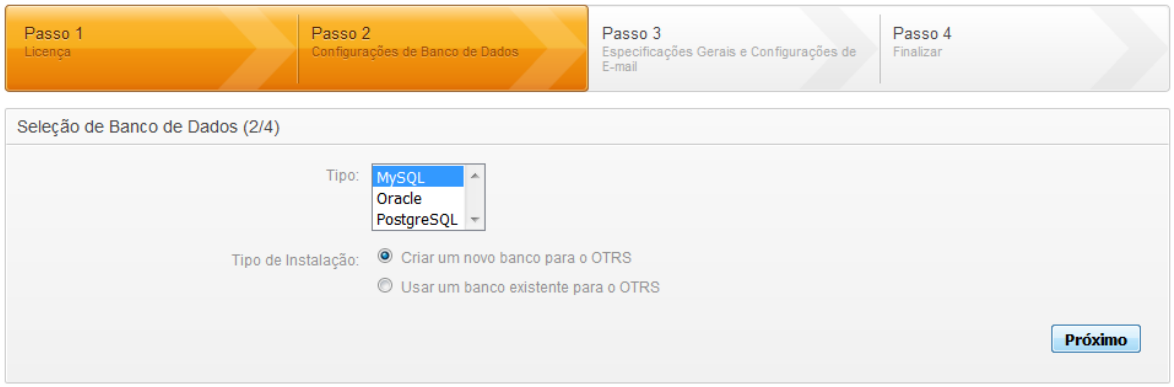
Figura 16 - Endereço para configuração do OTR.



Na Figura 16 a caixa em destaque de cor amarela mostra o IP do servidor web configurando com o Apache2 e a caixa destacada na cor vermelha mostra o comando "/otrs/installer.pl" para acesso as configurações do OTRS.

Após acessar as configurações do OTRS, na Figura 17 mostra os quatros passos básicos para configurar a ferramenta.

Figura 17 - Escolha do bando de dados.

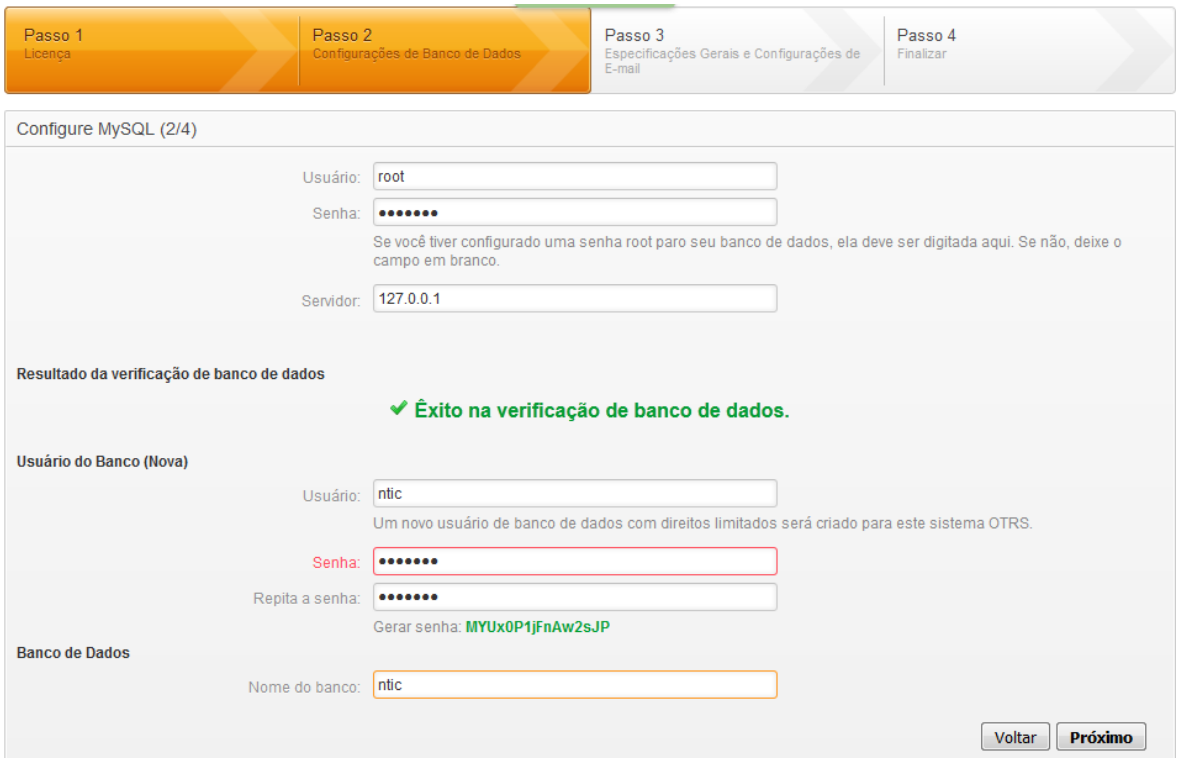


Os 4 passos exibidos na Figura 17 na parte superior referem-se a: licença de uso da ferramenta, configuração do banco de dados, configurações gerais com a configuração do e-mail e a confirmação dos dados.

O primeiro passo é aceitar a licença de uso da ferramenta, o segundo passo é a escolha do banco de dados que foi instalada anteriormente.

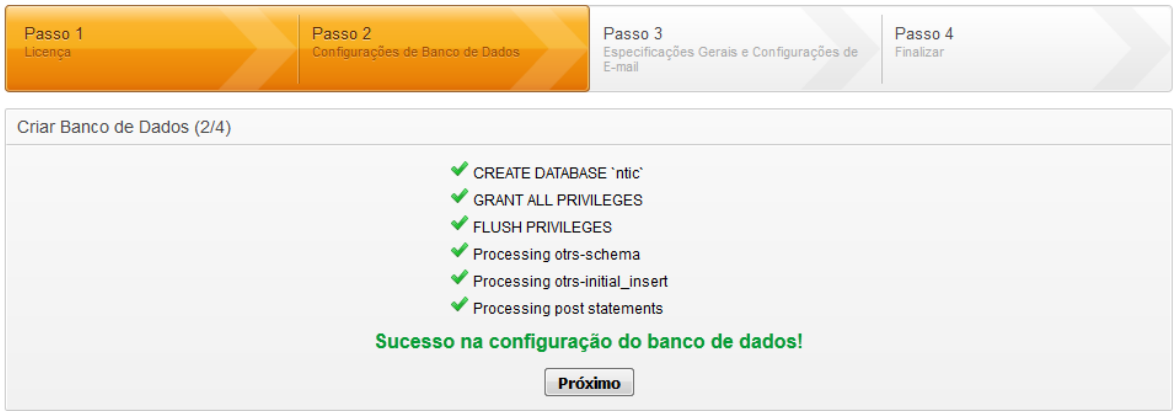
Na configuração do banco de dados deve ser criado um novo banco de dados para o sistema OTRS armazenar seus dados, como mostra a Figura 18.

Figura 18 - Criando banco de dados para o usuário do OTRS.



Para continuar a configuração como mostra a Figura 18 deve-se informar o nome do usuário e senha do banco de dados. Para confirmar os dados uma mensagem de "Êxito na verificação de banco de dados" será exibida. Tendo esta confirmação o passo seguinte é criar um novo usuário e senha, para o banco de dados do OTRS e aguardar a confirmação como mostra a Figura 19.

Figura 19 - Banco de dados criado



A Figura 19 exibe a confirmação da criação e configuração do banco de dados para o OTRS.

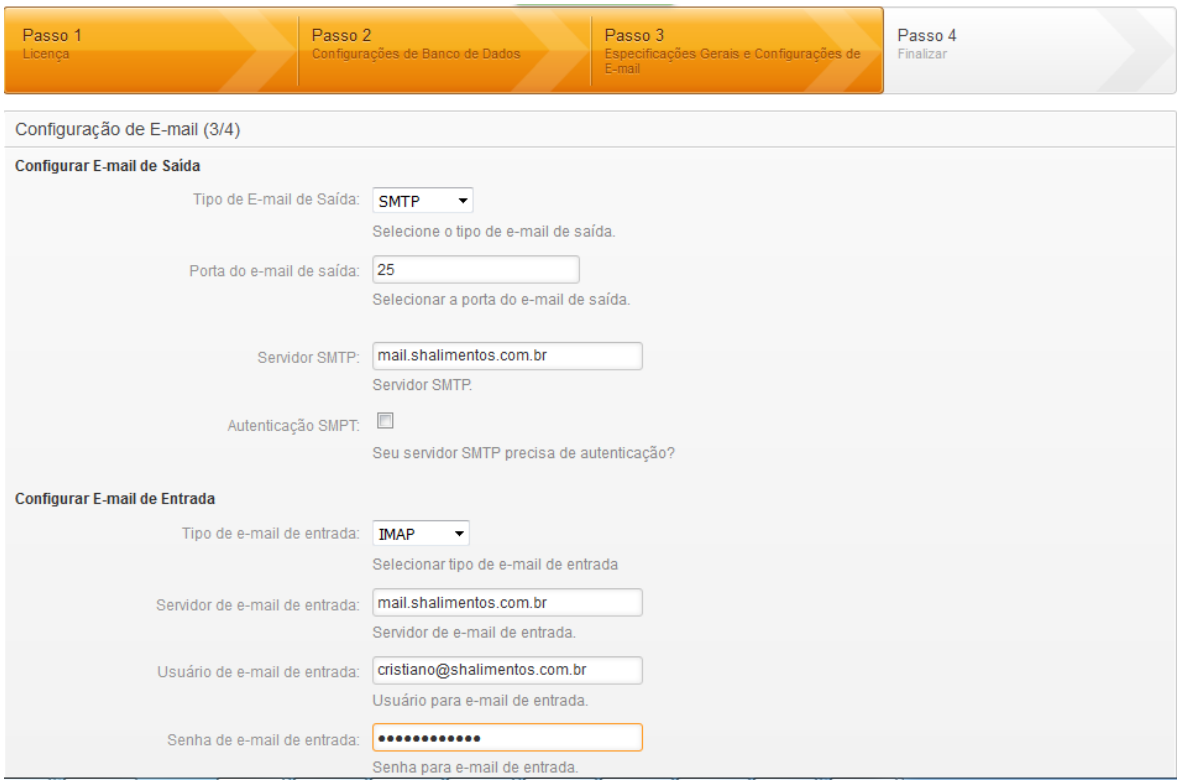
No terceiro passo são realizadas as configurações gerais do sistema, como pode ser visualizado na Figura 20.

Figura 20 - Configuração do administrador do OTRS.

A Figura 20 mostra os campos necessários para configuração básicas do sistema, os principais são: a conta de e-mail do administrador do OTRS, nome da organização que será gerenciada e o idioma.

O próximo passo é a configuração da conta do servidor de e-mail como mostra a Figura 21.

Figura 21 - Configuração do e-mail de entrada e saída do OTRS.

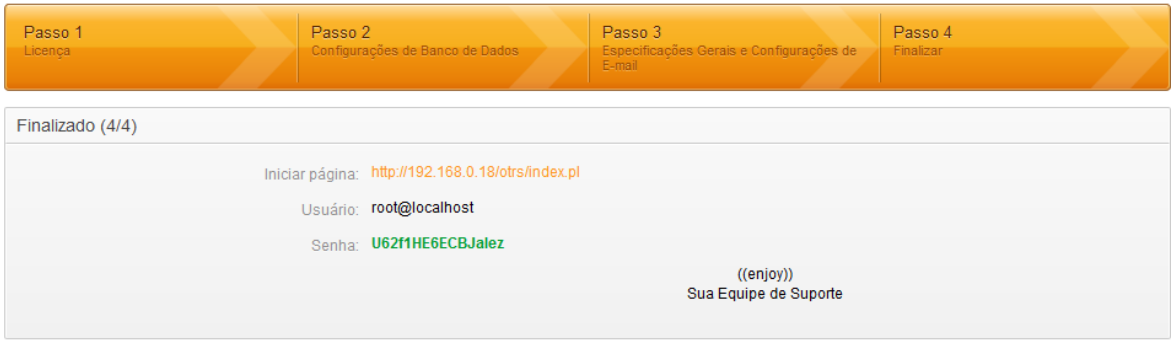


A configuração do servidor de e-mail exibida na Figura 21, composta pelo e-mail de saída e entrada. O e-mail de saída refere-se ao endereço do servidor que o OTRS utilizará para enviar as repostas, das notificações de incidentes de segurança recebidas pelo CAIS. Deve-se configurar também o tipo de e-mail neste caso o SMTP, a porta de saída, o endereço do servidor de e-mail e informar a se o e-mail utiliza autenticação para envio. O servidor de entrada refere-se ao endereço e-mail que receberá as notificações de incidentes de segurança enviado pelo CAIS para o NTIC. Deve-se configurar também o tipo do e-mail de entrada neste caso o IMAP, endereço e-mail de entrada e o usuário e senha do e-mail configurado.

Esta etapa de configuração do e-mail permite ao NTIC receber e enviar e-mail com resposta às notificações recebidas pelo CAIS dentro do OTRS.

O quarto e último passo da configuração básica do usuário do OTRS é a confirmação dos dados informados como mostra a Figura 22.

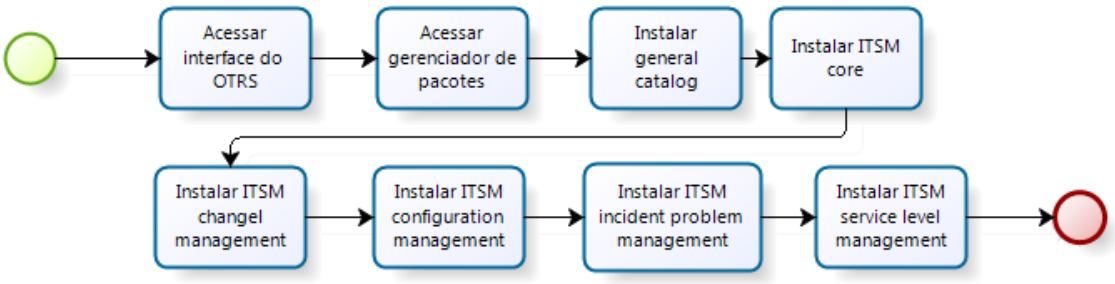
Figura 22 - Informações de acesso ao OTRS.



Ao finalizar a configuração de usuário do OTRS, como pode ser vista na Figura 22, o sistema fornece o endereço de acesso à ferramenta indicado pela informação “Iniciar página” e informa os dados do administrador do OTRS, como nome de usuário e senha.

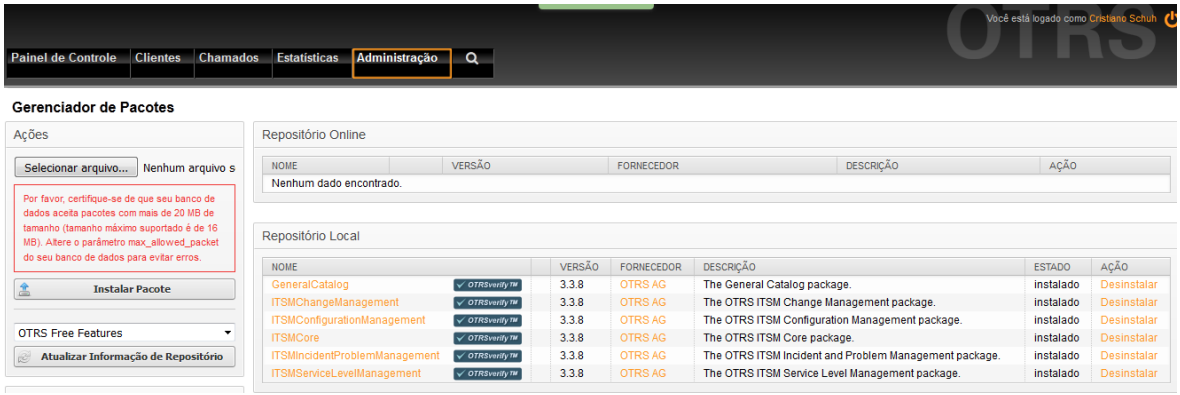
O último processo de configuração é a etapa de instalação e configuração do ITSM, para esta etapa foi criado um subprocesso de instalação e configuração da extensão ITSM como mostra a Figura 23.

Figura 23 - Instalação e configuração da extensão ITSM.



A Figura 23 exibe as etapas de instalação e configuração da extensão ITSM, que utiliza os pacotes descritos na primeira parte da pré-instalação. A instalação dos pacotes ocorre através da interface gráfica do OTRS, na página principal, na aba superior consta a opção administração, como mostra a Figura 24, dentro da área administração de sistema, existe o gerenciador de pacotes como mostra a Figura 24.

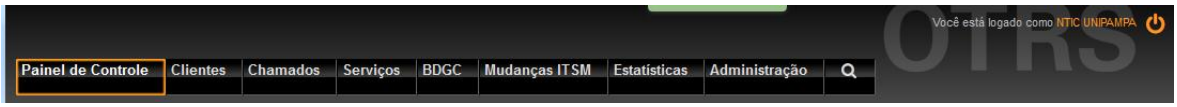
Figura 24 - Gerenciador de pacotes do OTRS.



Na Figura 24 mostra o gerenciador de pacote, onde na lateral esquerda são selecionados os pacotes baixados, que constam na etapa de pré-instalação e na área de repositório local lista-se os pacotes instalados e configurados.

Após a instalação dos pacotes do ITSM são acrescentadas opções na área de controle da página principal do OTRS como mostra a Figura 25.

Figura 25 - Interface de controle OTRS ITSM.

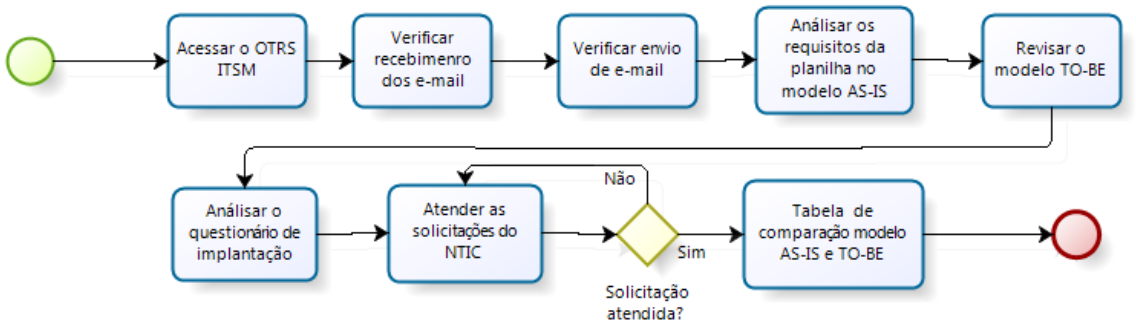


Na Figura 25 pode ser visto as opções de serviço, BDGC e mudanças ITSM, que foram adicionadas a área de controle do OTRS. Após a instalação da extensão ITSM, essas opções oferecem mais recursos de controle para a equipe do NTIC fornecendo outras opções de configuração para o TISI.

5.3 VALIDAÇÃO E EXECUÇÃO DA FERRAMENTA OTRS

A última etapa do cronograma de implantação do OTRS ITSM é a validação da ferramenta, em conjunto com a equipe do NTIC. Realizou-se por meio de testes e simulações o funcionamento do OTRS, seguindo o subprocesso criado de validação da ferramenta como mostra a Figura 26.

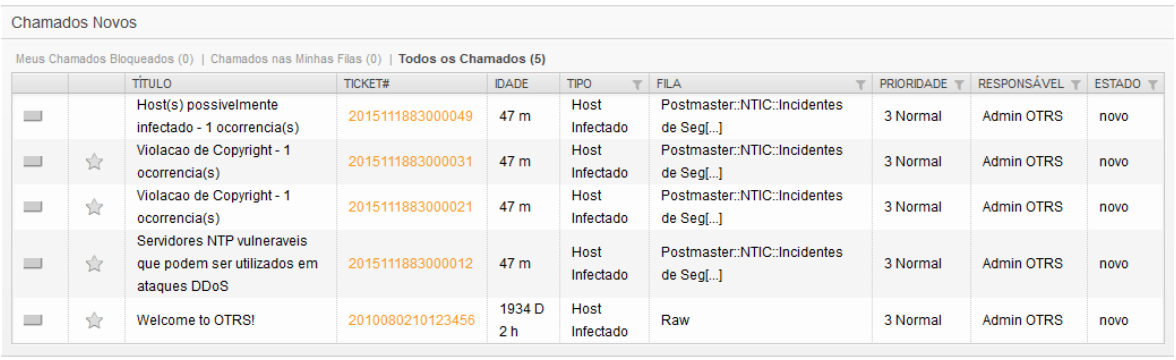
Figura 26 - Subprocesso de validação do OTRS.



O subprocesso de validação exibido na Figura 26 aborda 8 atividades, são elas: acessar o OTRS, verificar recebimento de notificação, enviar e-mails, analisar a planilha de requisitos do modelo AS-IS, revisar o modelo TO-BE, atender requisitos no questionário apêndice A e gerar uma tabela comparativa entre os modelos AS-IS e TO-BE, após a implantação do OTRS ITSM.

O processo de verificar o recebimento de e-mail no sistema OTRS é realizada para testar a configuração do servidor de e-mail de entrada, esse processo é configurado de modo automático, como mostra a Figura 27.

Figura 27 - Confirmação do recebimento dos e-mails de notificação de incidentes.


Chamados Novos

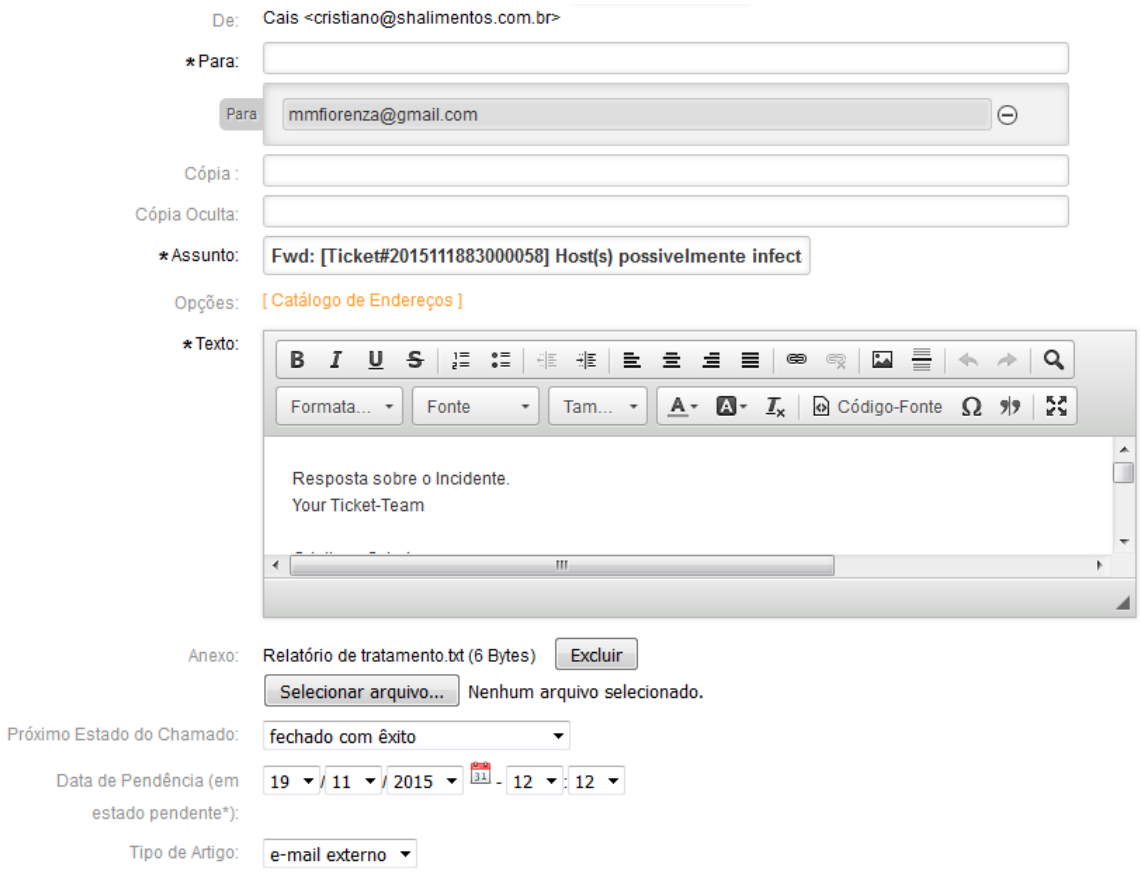
Meus Chamados Bloqueados (0) | Chamados nas Minhas Filas (0) | **Todos os Chamados (5)**

		TÍTULO	TICKET#	IDADE	TIPO	FILA	PRIORIDADE	RESPONSÁVEL	ESTADO
		Host(s) possivelmente infectado - 1 ocorrencia(s)	2015111883000049	47 m	Host Infectado	Postmaster::NTIC::Incidentes de Seg[...]	3 Normal	Admin OTRS	novo
		Violacao de Copyright - 1 ocorrencia(s)	2015111883000031	47 m	Host Infectado	Postmaster::NTIC::Incidentes de Seg[...]	3 Normal	Admin OTRS	novo
		Violacao de Copyright - 1 ocorrencia(s)	2015111883000021	47 m	Host Infectado	Postmaster::NTIC::Incidentes de Seg[...]	3 Normal	Admin OTRS	novo
		Servidores NTP vulneraveis que podem ser utilizados em ataques DDoS	2015111883000012	47 m	Host Infectado	Postmaster::NTIC::Incidentes de Seg[...]	3 Normal	Admin OTRS	novo
		Welcome to OTRS!	2010080210123456	1934 D 2 h	Host Infectado	Raw	3 Normal	Admin OTRS	novo

Na Figura 27 exibe a lista de todos os e-mails recebidos pelo OTRS, essa lista é atualizada automaticamente contendo todos os e-mails enviados pelo CAIS ao NTIC, listados como chamados novos, aguardando atendimento.

O próximo passo é verificar o envio de resposta por e-mail através do OTRS ao CAIS comunicando o tratamento realizado, como mostra a Figura 28.

Figura 28 - Envio de resposta do TISI através do OTRS ITSM.



Como pode ser visto na Figura 28, o teste de funcionamento da ferramenta, simulando uma situação real de TISI. O endereço de e-mail ‘cristiano@shalimento.com.br’ representa o e-mail do CAIS, o e-mail para resposta do TISI utilizado foi o ‘mmfiorenza@gmail.com’ representando o CAIS. Junto a esse e-mail de resposta, este anexado o documento do TISI, que no caso desse teste foi chamado de “relatório de tratamento.txt” atendendo um requisito do NTIC. Para enviar o e-mail de resposta, o estado do chamado deve ser alterado para atualizar o OTRS, nesse caso o estado foi alterado para ‘fechado com êxito’. Ao finalizar o envio do e-mail é preciso verificar o recebimento do mesmo, como mostra a Figura 29.

Figura 29 - E-mail de resposta do TISI através do OTRS ITSM.

Cais

para mim

Resposta sobre o Incidente.
Your Ticket-Team

Cristiano Schuh

--
Super Support - Waterford Business Park
5201 Blue Lagoon Drive - 8th Floor & 9th Floor - Miami, 33126 USA
Email: hot@example.com - Web: http://www.example.com/
--
---- Mensagem encaminhada de Maurício Fiorenza - NTIC <mauriciofiorenza@unipampa.edu.br> ---

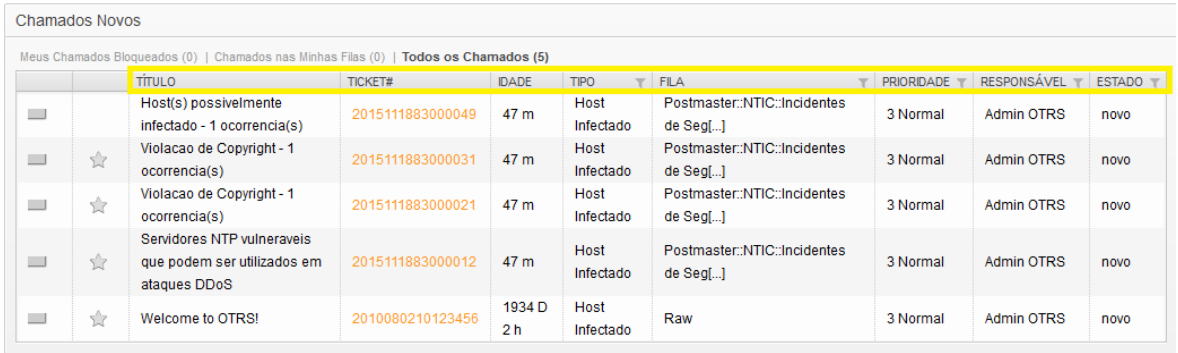
De: Maurício Fiorenza - NTIC <mauriciofiorenza@unipampa.edu.br>
Para: cristiano@shalimentos.com.br
Assunto: Host(s) possivelmente infectado - 1 ocorrencia(s)
Data: 2015-11-18 12:02:26
...

---- Fim da mensagem encaminhada ---

Como pode ser visto na Figura 29, a confirmação do recebimento do e-mail de resposta do TISI enviado ao CAIS por meio do OTRS. Neste caso o e-mail do CAIS é representado pelo endereço de e-mail de ‘mauriciXXXXX@unipampa.edu.br’.

A próxima etapa de validação do OTRS se faz necessário analisar a planilha de registro de notificações de incidentes de SI contida no modelo AS-IS, para verificar se as mesmas informações são encontradas no OTRS requeridas pelo NTIC, como mostra a Figura 30.

Figura 30 - Campos solicitados pelo NTIC.



Chamados Novos

Meus Chamados Bloqueados (0) | Chamados nas Minhas Filas (0) | **Todos os Chamados (5)**

		TÍTULO	TICKET#	IDADE	TIPO	FILA	PRIORIDADE	RESPONSÁVEL	ESTADO
		Host(s) possivelmente infectado - 1 ocorrencia(s)	2015111883000049	47 m	Host Infectado	Postmaster::NTIC::Incidentes de Seg[...]	3 Normal	Admin OTRS	novo
	☆	Violacao de Copyright - 1 ocorrencia(s)	2015111883000031	47 m	Host Infectado	Postmaster::NTIC::Incidentes de Seg[...]	3 Normal	Admin OTRS	novo
	☆	Violacao de Copyright - 1 ocorrencia(s)	2015111883000021	47 m	Host Infectado	Postmaster::NTIC::Incidentes de Seg[...]	3 Normal	Admin OTRS	novo
	☆	Servidores NTP vulneraveis que podem ser utilizados em ataques DDoS	2015111883000012	47 m	Host Infectado	Postmaster::NTIC::Incidentes de Seg[...]	3 Normal	Admin OTRS	novo
	☆	Welcome to OTRS!	2010080210123456	1934 D 2 h	Host Infectado	Raw	3 Normal	Admin OTRS	novo

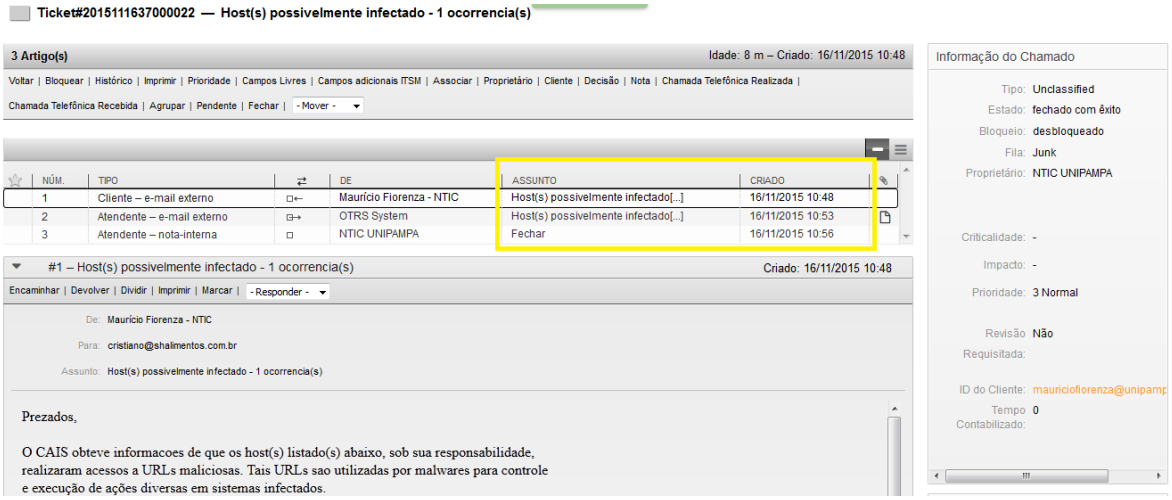
Como podem ser visualizados na Figura 30, os campos em destacados em amarelo representam as informações sobre o incidente de SI solicitadas pelo NTIC, essas informações estão descritas abaixo:

- O título, descrição prévia do assunto da notificação do CAIS sobre o incidente.
- O ticket, número único gerado automaticamente pelo sistema para cada e-mail recebido, substituindo o ticket da planilha de registro de atividades.
- A Idade, tempo em horas de espera da notificação recebida pelo OTRS.
- O tipo, classificação do incidente, substitui a subclassificação da planilha de registro de atividades.
- A fila é usado para todo os incidentes com a mesma classificação, que no caso será adaptada para substituir o campo de classificação da planilha de registro de atividades.
- A prioridade, classificação do grau de urgência para o atendimento do incidente.
- O responsável representa a pessoa que fez o atendimento do incidente, ele substitui o responsável pela investigação do incidente na planilha de registro de atividades.
- Estado, informa se o e-mail recebido é uma nova notificação ou se já foi atendido.

As informações citadas anteriormente estão contidas também no relatório de atividades gerado pelo OTRS, juntamente com outras informações que serão adaptadas, como:

- A unidade, referente os registo de atividades na planilha de registro de incidentes, será substituída pelo campo cliente que representa cada unidade do campus da universidade.
- No campo relatório da planilha de registo de atividades onde consta apenas o link para o relatório será substituído pelo campo de anexo onde é possível anexar o relatório diretamente na resposta do incidente.
- No campo da planilha de registo de atividades referente à data de abertura, data do incidente, data de encerramento, estão encontrados no registro de atividade de cada incidente, como mostra a Figura 31.

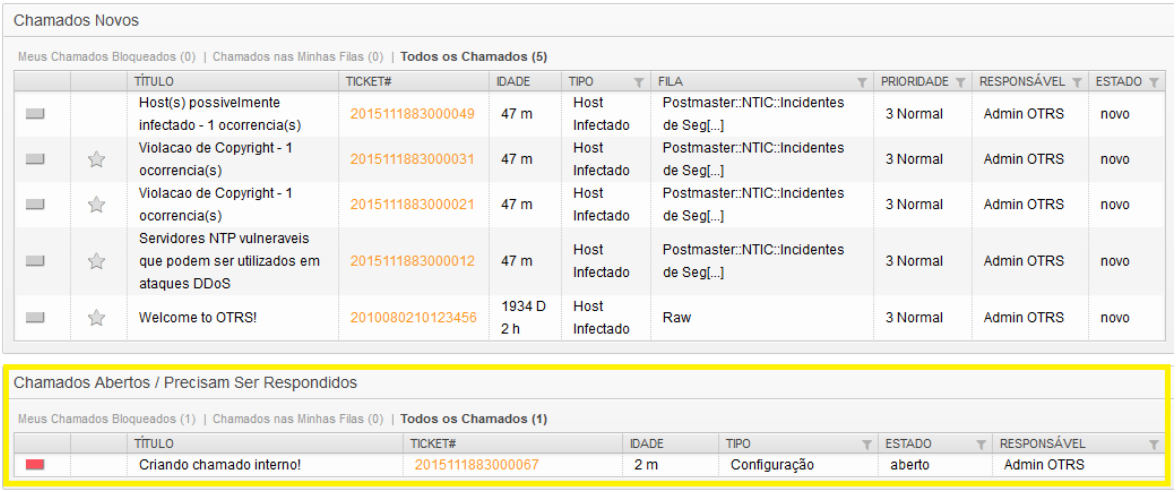
Figura 31 - Registro de atividades realizadas.



Podemos visualizar na Figura 31, destacados em amarelo as informações referentes aos campos, data do incidente, data de abertura e a data do encerramento do incidente.

A próxima atividade se faz necessária à revisão do modelo TO-BE juntamente com questionário do apêndice A para relacionar o que OTRS já atendeu e quais são as outras necessidades do NTIC. Na revisão dos requisitos do NTIC, observou-se a necessidade de registrar incidentes internos independente do CAIS, essa solicitação também pode ser realizada pelo OTRS, como mostra a Figura 32.

Figura 32 - Registro de incidente interno pelo NTIC.



A Figura 32 mostra destacado em amarelo o registro de um incidente interno criado pelo NTIC independente das notificações recebidas pelo CAIS.

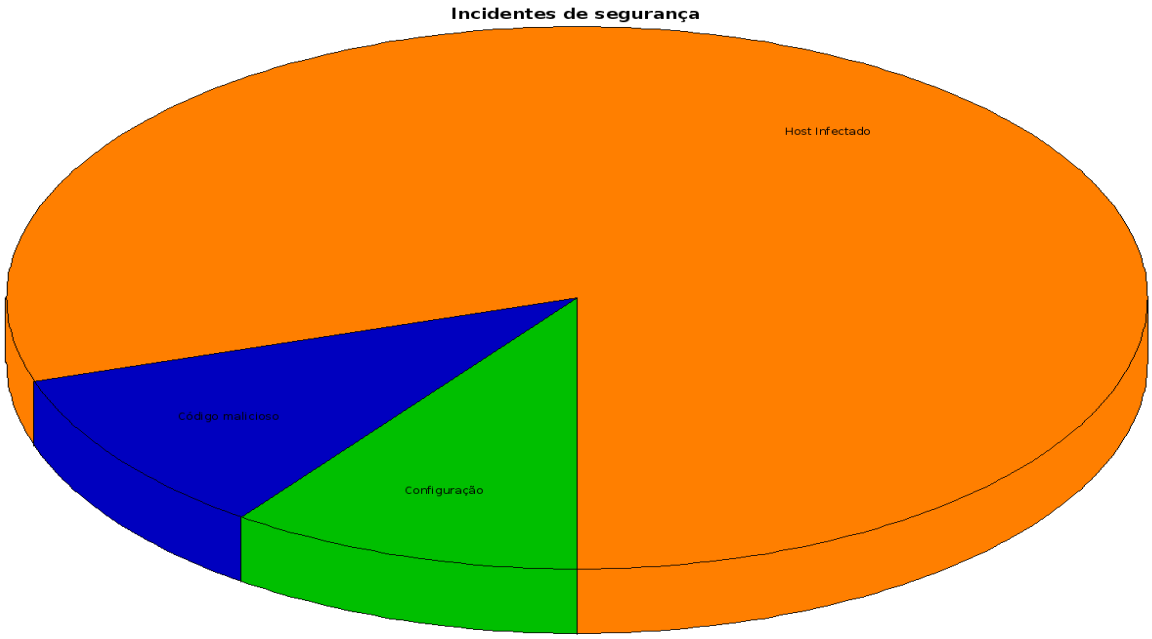
Na atividade descrita como atender as solicitações do NTIC, se fez necessário realizar um questionário encontrado no apêndice A, para saber quais são as outras melhorias que poderiam ser agregadas à gestão do TISI por meio do OTRS. Como resultado foi proposto, que o OTRS gera-se um relatório de atividade automaticamente, que substitui-se a planilha de registro de notificações, como mostra a Tabela da Figura 33.

Figura 33 - Planilha de registro de atividades gerada automaticamente pelo OTRS ITSM.

	A	B	C	D	E	F	G	H	I	J	K
1	Ticket#	Idade	TÃ-tulo	Criado	Alterado	Hora de Fechamento	Fila	Estado	Prioridade	Cliente	Tipo
2	2015111883000060	281235	Criando chamado interno!	18/11/2015 12:48	18/11/2015 12:52	18/11/2015 12:52	Postmaster::NTIC::Incidentes	closed successful	5 very high	analista	ConfiguraÃ§Ã£o
3	2015111883000050	284009	Host(s) possivelmente infe	18/11/2015 12:02	18/11/2015 12:17	18/11/2015 12:17	Postmaster::NTIC::Incidentes	closed successful	4 high	mauriciofiorenza	Host Infectado
4	2015111883000040	284011	Host(s) possivelmente infe	18/11/2015 12:02	18/11/2015 12:02		Postmaster::NTIC::Incidentes	new	3 normal	mauriciofiorenza	Host Infectado
5	2015111883000030	284013	Violacao de Copyright - 1 oc	18/11/2015 12:02	20/11/2015 23:17	20/11/2015 23:15	Postmaster::NTIC::Incidentes	closed successful	3 normal	mauriciofiorenza	CÃ³digo malicioso
6	2015111883000020	284015	Violacao de Copyright - 1 oc	18/11/2015 12:02	18/11/2015 12:02		Postmaster::NTIC::Incidentes	new	3 normal	mauriciofiorenza	Host Infectado
7	2015111883000010	284017	Servidores NTP vulneraveis	18/11/2015 12:02	18/11/2015 12:02		Postmaster::NTIC::Incidentes	new	3 normal	mauriciofiorenza	Host Infectado

Como pode ser visto na Figura 33, essa nova planilha de registro de notificação de incidentes comtempla todos os requisitos listados na antiga planilha de registro de notificação de incidentes. Essa nova planilha gerada automaticamente pelo OTRS também pode ser configurada de acordo com as necessidades do NTIC. Outra necessidade do NTIC é a possibilidade de gerar gráficos com informações sobre incidentes, que também é realizada por meio do OTRS como mostra a Figura 34.

Figura 34 – Gráfico gerado pelo OTRS ITSM dos incidentes notificados.



Como pode ser visto na Figura 34 o gráfico representa a proporção dos tipos de incidentes notificados pelo NTIC, em laranja representa os host´s infectados, em azul os de código malicioso e em verde os de configuração. No entanto, a ferramenta OTRS fornece a possibilidade de gerar outros gráficos com outras informações de acordo com a necessidade do NTIC.

Na ultima atividade do subprocesso de validação, foi realizada a tabela de comparação do modelo AS-IS com o modelo TO-BE. Essa tabela comparativa exemplifica o que era realizado no modelo AS-IS e o que mudou com o modelo TO-BE com a implantação do OTRS ITSM, como mostra a Tabela 2.

Tabela 2 - Tabela de comparação do modelo AS-IS com o modelo TO-BE.

Modelo AS-IS	**Modelo TO-BE**
Registro de atividades realizadas sobre um incidente de forma provisória e manualmente por meio de uma planilha no google docs;	O sistema OTRS cria automaticamente uma planilha registrando todas as informações sobre o incidente de segurança;

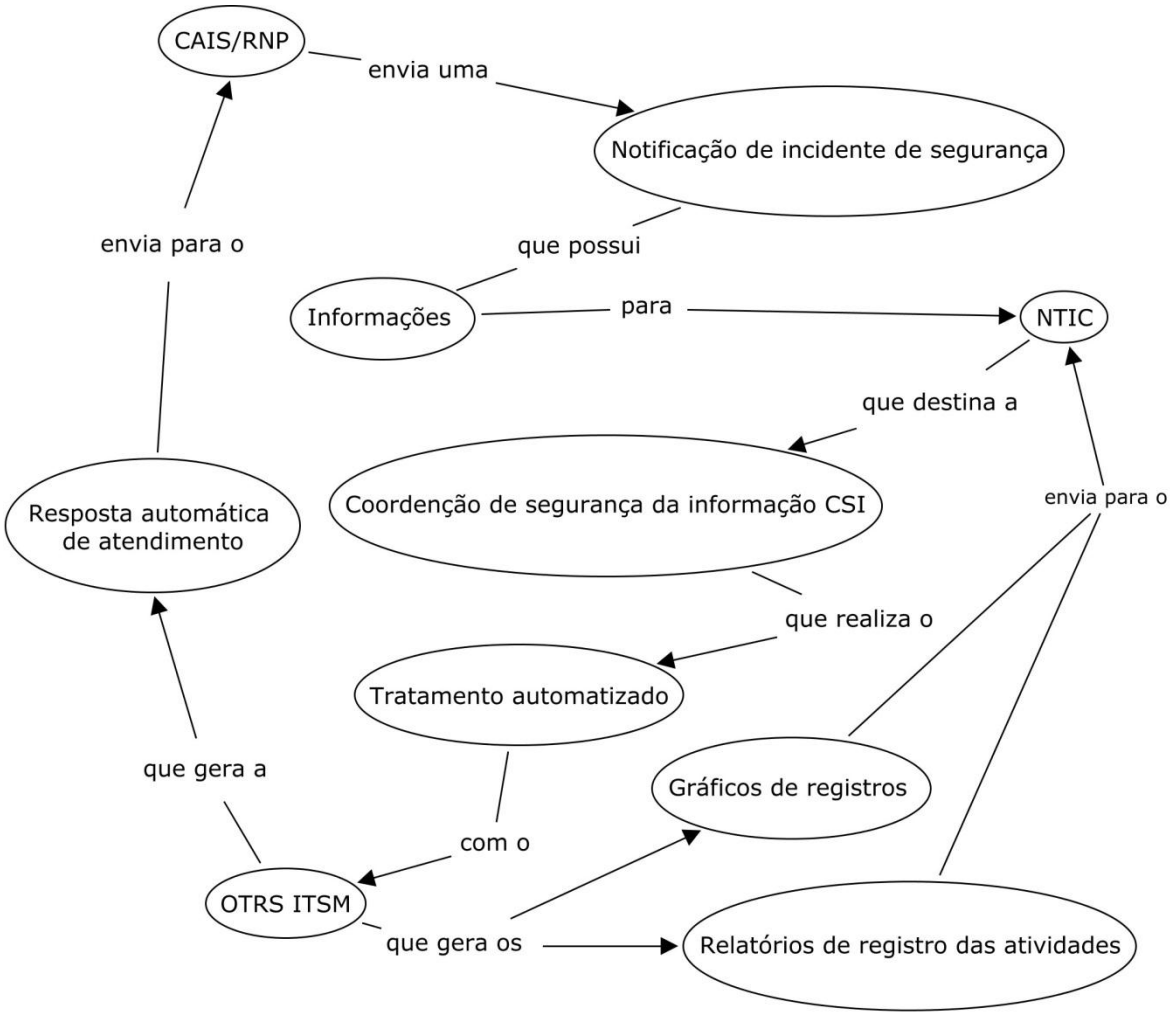
Geração de ticket interno manualmente;	Geração de ticket interno automaticamente pelo sistema OTRS;
Solução provisória de registro de incidentes internos;	Possibilita a criação de registro de incidente interno dentro do OTRS;
Informações sobre um incidente de forma descentralizada;	Todas as informações sobre o incidente estão centralizadas;
Necessidade de adicionar um link para visualizar o relatório do tratamento do incidente de segurança;	Possibilidade de anexar documentos e relatórios junto à resposta do tratamento do incidente de segurança;
Falta de segurança no armazenamento da planilha de registro de atividade;	Sistema com usuário e senha para acessar informações sobre atividades realizadas em um incidente de segurança;
Resposta de atendimento realizada de forma manual pelo responsável;	Resposta de atendimento gerada automaticamente para o solicitante;
Tipos diferentes de incidentes sem agrupamento;	Classificação de tipos diferentes de incidentes através de grupos ou filas;
Solução provisória de compartilhamento de informações sobre os incidentes para todos os membros da equipe através de e-mail pelo da google o gmail;	Informações compartilhadas para todos os membros da equipe através de usuário e senha do sistema OTRS;
Não possui encaminhamento de incidentes para outro nível de tratamento;	Possui encaminhamento, dividido por nível para tratar diferentes incidentes;
Não possui visualização de modo gráfico de todos os incidentes notificados;	Visualização de modo gráfico de todos os incidentes notificados;
Não possui registro de histórico das atividades sobre os incidentes de segurança.	Histórico de atividades sobre os incidentes de forma padronizada;

Não há possibilidades de adicionar recursos.	Possibilidade e adicionar novos recursos de acordo com a necessidade do NTIC.

A Tabela 2 mostra todas as solicitações atendidas do modelo TO-BE com a contribuição da implantação da ferramenta OTRS ITSM, comparados com o antigo modelo AS-IS.

Com o término da implantação do OTRS, obteve-se uma melhora na gestão do TISI do NTIC. A Figura 35 mostra a como fica a gestão do TISI após a implantação do OTRS ITSM.

Figura 35 - Tratamento de incidentes com o OTRS ITSM.



Pode ser visualizada na Figura 35, a implantação do OTRS ITSM no TISI do NTIC, identificando os processos gerados por meio do OTRS. A geração de relatórios de atividade e históricos de atendimento será feito dentro do OTRS ITSM, o que acelera o processo de criação e armazenamento dos registros de atividades, substituindo a atual planilha de registro de notificações.

6 TRABALHOS FUTUROS

Este trabalho fez parte de um estudo de caso realizado na gestão de TISI do NTIC, onde foi implantada a ferramenta OTRS.

O OTRS possui outras versões e extensão além dessa que foi implantada, como a versão OTRS 5 beta com o pacote nível 3, que possui maiores recursos como por exemplo: interface responsiva, serviço de SMS integrado, notificações personalizadas e modelos de processo predefinidos. Para implantar a nova versão, deve-se realizar um novo estudo relacionando os requisitos do NTIC com as funcionalidades e requisitos do sistema. Outra possibilidade existente no OTRS é a configuração de seus recursos para atuar no tratamento específico de alguns incidentes de forma automática, resultando num melhor desempenho do TISI pela equipe do NTIC.

7 CONCLUSÃO

A análise realizada na gestão do TISI no NTIC da UNIPAMPA, constatou-se a importância da implantação de uma ferramenta de gestão, para melhorar os procedimentos adotados e padronizar para o TISI. Para atender os objetivos requisitados pelo NTIC, foi estudado as políticas e normas de segurança da informação da UNIPAMPA, definindo a ferramenta de gestão de TISI o OTRS - *Open Technology Real Services.*

Usando a ferramenta OTRS obteve-se os relatórios dos TISI, automaticamente, a qual substitui a atual planilha de registro de notificações de incidentes de SI. Atendeu-se os requisitos do NTIC de gerar notificações de incidentes internos, anexar relatórios junto ao e-mail de resposta ao CAIS e a geração de gráficos das informações que forem solicitadas.

Com este trabalho é possível implantar a ferramenta OTRS, por meio dos procedimentos detalhados da instalação, configuração e execução, possibilitando o uso na gestão de TISI do NTIC e também em outras organizações que utilizam recursos de TI. Ao término deste trabalho, ao utilizar as ferramentas descritas, e realizar as configurações necessárias, conclui-se que todos os objetivos propostos foram alcançados.

8 REFERÊNCIA

Apache. (1997). *HttpServer Projet*. Acesso em 20 de julho de 2014, disponível em http://httpd.apache.org/download.cgi

BEST. (2002). *RT- Request Tracker*. Acesso em 5 de julho de 2014, disponível em www.bestpractical.com/rt/

BEST. (2002). *RTIR: RT for incidente response*. Acesso em 5 de Julho de 2014, disponível em Best Pratical: https://www.bestpractical.com/rtir/

CAIS. (2013). *Centro de atendimento a incidentes de segurança*. Acesso em 19 de junho de 2014, disponível em Rede nacional de ensino e pesquisa: http://www.rnp.br/cais/sobre.html

CAIS. (2013). *Incidentes de segurança da informação.* RNP.

CERT.br. (2012). *Sobre o CERT.br*. Acesso em 20 de maio de 2014, disponível em Centro de estudos, resposta e tratamento de incidentes de segurança no brasil: http://www.cert.br/sobre

CERT.br. (17 de fevereiro de 2013). *Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança*. Acesso em 20 de maio de 2014, disponível em www.cert.br/stats/incidentes/2013-jan-dec/analise.html

CERT.br. (2015). Acesso em 25 de junho de 2015, disponível em http://cartilha.cert.br/

CHIHT. (2005). Acesso em 16 de maio de 2014, disponível em Clearing house for incident handling tools: http://www.ensia.europa.eu/activities/cert/supor/chiht

CTIR.gov. (2015). Acesso em 15 de outubro de 2015, disponível em www.ctir.gov.br/

FERREIRA, F., & ARAÚJO, M. (2008). *Política de segurança da informação. 2. ed.* Rio de Janeiro: Ciência Moderna Ltda.

Fiorenza, M. (20 de 04 de 2014). NTIC.

FLORA, F. D. (2010). A Influência do NAT na Indentificação e Tratamento de Incidentes de Segurança da Informação. *Monografia (monografia) - Universidade Gama Filho*. Alegrete.

FONTES, E. (2006). *Segurança da informação: Usuário faz a diferença. 2. ed.* São Paulo: Saraiva.

FONTES, E. (2012). *Política e normas para a segurança da informação: Como desenvolver, implanter e manter regulamentos para a proteção da informação nas organizações.* Rio de Janeiro: BRASPORT Livros e multimídia Ltda.

KLINGMULLER, T. (15 de maio de 2005). SIRIOS. A framework for CERTs.

MySQL. (2014). *Download MySQL Community Server*. Acesso em 7 de julho de 2014, disponível em http://dev.mysql.com/downloads/mysql/

NTIC. (2010). Acesso em 2 de maio de 2014, disponível em Núcle de tecnologia da informação e cominucação: http://nitc.unipampa.edu.br/conselho-gestor-de-tic/regimentos/

OTRS. (2014). Acesso em 3 de junho de 2014, disponível em Open technology real services: http://www.otrs.com/software/otrsitsm-features/

Peltier, T. (2001). *Information Scurity Policies, Procedurs, and Stardards: Guidelines for effective information security mangement.* Auerbach.

Peltier, T. (2005). *Information Security Risk Analysis 2nd ed.* CRC Press.

PEREIRA, I. B. (2013). Modelagem de processos de tratamento de incidentes de segurança da informação do NTIC/UNIPAMPA. *Monografia - Universidade Federal Pampa - Curso de Graduação em Ciência da Computação*. Alegrete.

SÊMOLA, M. (2003). *Gestão de segurança da informação. Uma visão executiva.* Rio de Janeiro: Elsevier.

TRAIRA. (2010). Acesso em 2 de maio de 2014, disponível em Tratamento de incidentes de rede automatizado: http://www.pop-ba.rnp.br/Cert/Traira

UNIPAMPA. (março de 2011). Acesso em 12 de maio de 2014, disponível em Universidade Federal do Pampa: http://www.unipampa.edu.br/portal/universidade/403

APÊNDICE A – QUESTIONÁRIO REALIZADO À EQUIPE DO NTIC

Nome: Maurício Martinuzzi Fiorenza
Cargo: Analista de TI

QUESTIONÁRIO SOBRE INCIDENTES DE SEGURANÇA NO NTIC

Este questionário tem como objetivo analisar a importância da implantação de uma ferramenta de gestão de tratamento de incidentes de segurança da informação. Os resultados deste questionário irão auxiliar na escolha da ferramenta e na forma que ela deve ser configurada.

1- **Qual a importância do tratamento de incidentes de segurança?**

O tratamento de incidentes busca diminuir o risco de ataque as informações da instituição e minimizar o dano caso o ataque ocorra.

2- **Quais os requisitos que a ferramenta de tratamento de incidentes deve atender?**

- Registro de incidentes externos e internos.
- Centralização dos dados relacionados a incidentes.
- Automatização das respostas ao órgãos notificantes.

3- **Com a implantação da ferramenta, qual o objetivo principal do uso dessa ferramenta?**

Automatizar algumas das etapas do processo de tratamento de incidentes, agilizando assim o trabalho das equipes.

4- **No que se refere às estatísticas de incidentes de segurança é um requisito que a ferramenta deve disponibilizar?**

Sim, este tipo de informação é primordial para a gestão de TI na UNIPAMPA. De posse destes dados a alta gestão pode decidir como e quando interferir nos serviços de TI.

5- **No que se refere aos registros das atividades, porque é importante guardar e gerar esses registros?**

Com essa base de dados de atividades disponível é possível buscar soluções para problemas já tratados anteriormente.

6- **Automatização de respostas dos incidentes, qual a vantagem dessa implantação?**

Dar agilidade ao tratamento, e registro das respostas em uma base de dados única.

7- **No que se refere aos logs, gerar logs é necessário?**

A UNIPAMPA como instituição pública, está sujeita a auditorias de órgãos fiscalizadores, neste ponto que o registro das atividades se torna importante, como informação para as auditorias.

8- **No que se refere a registro de incidentes, há ferramenta deve contemplar criação de incidentes internos?**

Sim, hoje em dia temos diversos tipos de incidentes notificados por usuários internos, que precisam ser registrados e tratados.

9- **Há necessidade de prover uma segurança para as informações que estão contidas na atual planilha de registro de atividades de incidentes?**

Sim, nesta planilha constam informações importantes sobre vulnerabilidades em nossos sistemas. Garantir que não ocorra acesso indevido é de fundamental importância para a Segurança da Informação na UNIPAMPA.

10- **A ferramenta de tratamento de incidentes de segurança deve conter o recurso de resposta automática a fim de comunicar que o incidente será atendido?**

Sim. O órgão regulador exige uma resposta a cada ação no tratamento dos incidentes.