ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

Cap QCO MARCUS VINÍCIUS LACERDA FAGUNDES

CUSTOMIZAÇÃO DO *SOFTWARE REQUEST TRACKER* (RT) PARA TRATAMENTO DE INCIDENTES DE SEGURANÇA CIBERNÉTICOS EM *CSIRTS* DE COORDENAÇÃO

Rio de Janeiro
2019

Cap QCO MARCUS VINÍCIUS LACERDA FAGUNDES

CUSTOMIZAÇÃO DO SOFTWARE *REQUEST TRACKER* (RT) PARA TRATAMENTO DE INCIDENTES DE SEGURANÇA CIBERNÉTICOS EM *CSIRTS* DE COORDENAÇÃO

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau de Especialização em Ciências Militares

Orientador: Maj QCO ANDERSON BARROS TORRES

Rio de Janeiro
2019

Cap QCO MARCUS VINÍCIUS LACERDA FAGUNDES

CUSTOMIZAÇÃO DO SOFTWARE *REQUEST TRACKER* (RT) PARA TRATAMENTO DE INCIDENTES DE SEGURANÇA CIBERNÉTICOS EM *CSIRTS* DE COORDENAÇÃO

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau de Especialização em Ciências Militares

Aprovado em

COMISSÃO DE AVALIAÇÃO

_____

ANDERSON BARROS TORRES – Maj QCO – Avaliador 1

Escola de Formação Complementar do Exército

_____

RODRIGO LESTINHO ÁVILA – TC Com – Avaliador 2

Escola de Formação Complementar do Exército

CUSTOMIZAÇÃO DO SOFTWARE *REQUEST TRACKER* (RT) PARA TRATAMENTO DE INCIDENTES DE SEGURANÇA CIBERNÉTICOS EM *CSIRTS* DE COORDENAÇÃO

Marcus Vinícius Lacerda Fagundes[1]

RESUMO

Os meios cibernéticos na administração pública brasileira são utilizados, direta ou indiretamente, para prestar serviços de forma econômica e acessível à população. Entretanto, ataques cibernéticos são cada vez mais frequentes aos órgãos e entidades públicas afetando a plena execução dos serviços à sociedade. Neste contexto, as atividades de resposta a incidentes cibernéticos se tornou amplamente utilizado. Todavia, é necessário também que elas sejam realizadas de forma eficiente. O Centro de Tratamento e Resposta à Incidentes Cibernéticos de Governo (CTIR Gov), órgão integrante do Gabinete de Segurança Institucional (GSI), tem se sobressaído na realização do tratamento de incidentes, se valendo como ferramenta central para suas atividades o *software Request Tracker* (RT). Deste modo, este estudo teve como objetivo analisar a efetividade desta ferramenta na operacionalização das atribuições do CTIR Gov na resposta à incidentes no nível de coordenação, verificando ainda a aplicabilidade da ferramenta em outras equipes de resposta a incidentes, identificando oportunidades de melhoria e recomendações. Este estudo realizou uma análise a partir de dados gerados pelo CTIR Gov, os relatórios estatísticos anuais que estão disponíveis no portal daquele Centro e o dados consolidados dos histórico das ocorrências de incidentes que individualmente são considerados informações de acesso restrito. Inicialmente, foi observada a literatura considerada estado da arte na gestão de incidentes, extraindo-se as principais tarefas do processo de tratamento de incidentes. Em uma segunda etapa, foram comparadas as tarefas identificadas na primeira etapa com as que são atualmente executadas com o apoio do RT no CTIR Gov. Por fim, foi mensurada a efetividade de cada uma destas tarefas utilizando os dados obtidos em conjunto com uma abordagem qualitativa. Os resultados indicam que efetividade do uso do RT para atividades de resposta a incidentes é elevada, pois em todas as métricas avaliadas a taxa média de performance obtida foi superior a 80%, o que demonstra um elevado grau de maturidade do CTIR Gov, quanto o uso das boas práticas e operação e customização do RT. O estudo finaliza com sugestões de melhoria, pois há espaço para aperfeiçoar o uso da ferramenta.

Palavras-chave: Tratamento de Incidentes, Segurança Cibernética, Sistemas de Rastreamento de Ocorrências.

ABSTRACT

Cybernetics in the brazilian public administration are used, directly or indirectly, to provide services economically and accessible to the population. However, cyber attacks are increasingly common to public agencies and entities affecting the full performance of services to society. In this context, cyber incident response activities has become widely used. However, they must also be carried out efficiently. The Brazilian Government CSIRT, Government Cyber Incident Handling and Response Center (CTIR Gov), which is part of the Institutional Security Office (GSI), has excelled in handling incidents, using the Request Tracker (RT) software as its central tool. Thus, this study aimed to analyze the effectiveness of this tool in the operationalization of CTIR Gov attributions in response to incidents at the coordination level, also verifying the applicability of the tool in other incident response teams, identifying opportunities for improvement and recommendations. This study analysed data generated by the CTIR Gov, the annual statistical reports that are available on the CTIR Gov portal and the consolidated historical data on incidents that are individually considered restricted access information. Initially, the literature considered state of the art in incident management was observed, extracting the main tasks of the incident handling process. In a second stage, the tasks identified in the first stage were compared with

1 Capitão QCO de Informática da turma de 2011. Bacharel em Ciência da Computação pela Universidade Federal da Bahia (UFBA) em 2010. Especialista em Aplicações Complementares às Ciências Militares pela Escola de Formação Complementar do Exército em 2011.

those currently performed with the support of the RT in the CTIR Gov. Finally, the effectiveness of each of these tasks was measured using the data obtained together with a qualitative approach. The results indicate that the effectiveness of the use of RT for incident response activities is high, since in all evaluated metrics the average performance rate obtained was above 80%, which demonstrates a high degree of maturity of CTIR Gov, regarding the use of good practices and operation and customization of RT. The study concludes with suggestions, as there is room to improve the use of the tool.

Keywords: Incident Handling, Cyber Security, Issue Tracking Systems.

CUSTOMIZAÇÃO DO SOFTWARE *REQUEST TRACKER* (RT) PARA TRATAMENTO DE INCIDENTES DE SEGURANÇA CIBERNÉTICOS EM *CSIRTS* DE COORDENAÇÃO

1. INTRODUÇÃO

O espaço cibernético tem ganhado cada vez mais relevância nos últimos quarenta anos, proveniente do progresso dos meios computacionais / informatizados, que facilitou o acesso as informações e possibilitaram a criação de uma gama de serviços disruptivos. Como resultado as pessoas, os órgãos públicos e as instituições privadas mudaram seu comportamento, forma de produção e consumo, tornando-se gradualmente mais conectadas e mais dependentes dos meios digitais (SANTOS, 2017).

Atividades maliciosas em ativos computacionais de organizações ou Estados podem impactar seriamente a sociedade, como o ataque ocorrido em maio de 2017 por meio do *ransomware WannaCry. Esse tipo de malware* sequestra ativos computacionais, encriptando seus dados, e pede resgate em criptomoedas. Este ataque afetou organizações de diversos países, incluindo unidades hospitalares do Reino Unido (BBC, 2017). Por conta de ameaças como esta, tornou-se comum a criação, dentro das organizações, de equipes para solucionar incidentes cibernéticos, são chamadas de *Computer Security Incident Response Teams* (CSIRTs), tendo como principal objetivo prevenir e proteger uma determinada comunidade, seja sua própria organização, um setor ou mesmo um Estado (KILLCRECE et al, 2003).

Os CSIRTs atuam em um contexto cada vez mais complexo: mais disponibilidade e maior complexidade dos hardwares e dos softwares, mais serviços sendo oferecidos pelas organizações, a sociedade mais dependente do entretenimento e de serviços por meio de ativos computacionais. Neste contexto, aumenta o interesse na exploração de vulnerabilidades nos ativos computacionais por onde trafegam essa massa de dados com finalidades diversas, por exemplo a obtenção de vantagem financeira como no caso do WannaCry. Atualmente é possível encontrar bases de dados de vulnerabilidades e seus *exploits*[1] publicamente em sítios

1 São *softwares* desenvolvidos para comprometer sistemas ou redes por meio da exploração de uma vulnerabilidade (CAMBRIDGE DICTIONARY, 2019).

como: exploit-db.com, metaesploit.com e vulndb.com. Assim, é possível criar *softwares* maliciosos modulares, configuráveis e com pouco conhecimento técnico. Tanto organizações criminosas, quanto Estados soberanos têm buscado identificar fragilidades em ativos computacionais, utilizando-as como armas.

Se por um lado, os ataques utilizam ferramentas cada vez mais sofisticadas, por outro a segurança cibernética por meio dos CSIRTs também necessitam ampliar suas capacidades por meio de ferramentas (MINICK, 2017). Neste contexto, algumas equipes, tais como os CSIRTs das Forças Armadas Brasileiras, passaram a utilizar o software *Request Tracker* (RT) como forma de tomar ciência e trocar informações sobre ameaças e incidentes cibernéticos.

Ante o exposto, elaborou-se um estudo científico com o objetivo de analisar a efetividade do uso da ferramenta RT no suporte a operacionalização das atribuições de CSIRTs que atuam no nível de coordenação. Para tanto, realizou-se uma pesquisa de natureza aplicada, empregando uma análise qualitativa com base em evidências coletadas do estudo de caso realizado no Centro de Tratamento e Resposta à Incidentes Cibernéticos de Governo (CTIR Gov).

Por fim, o trabalho realizou discussões sobre os resultados obtidos com intuito de aperfeiçoar a execução das atividades da Gestão de Incidentes Cibernéticos por meio da ferramenta RT, com base nas melhores práticas identificadas na literatura de referência.

2. REFERENCIAL TEÓRICO

A seguir, será descrito o referencial teórico. No item 2.1, abordou-se o conceito de incidente cibernético e a relevância da gestão de incidentes nas organizações. No item 2.2, detalhou-se o papel dos CSIRTs, destacando a importância da colaboração entre os CSIRTs, de diversos níveis de atuação, na resolução de incidentes. Em seguida, no item 2.3, descreveu-se as características dos *Issues Tracking Systems* e sua aplicação na resolução de ocorrências, sendo o *Request Tracker* uma destas ferramentas. Por fim, no item 2.4, abordou-se a estrutura organizacional do CTIR Gov e suas principais atividades do tratamento de incidentes no nível de coordenação, que é o foco deste trabalho.

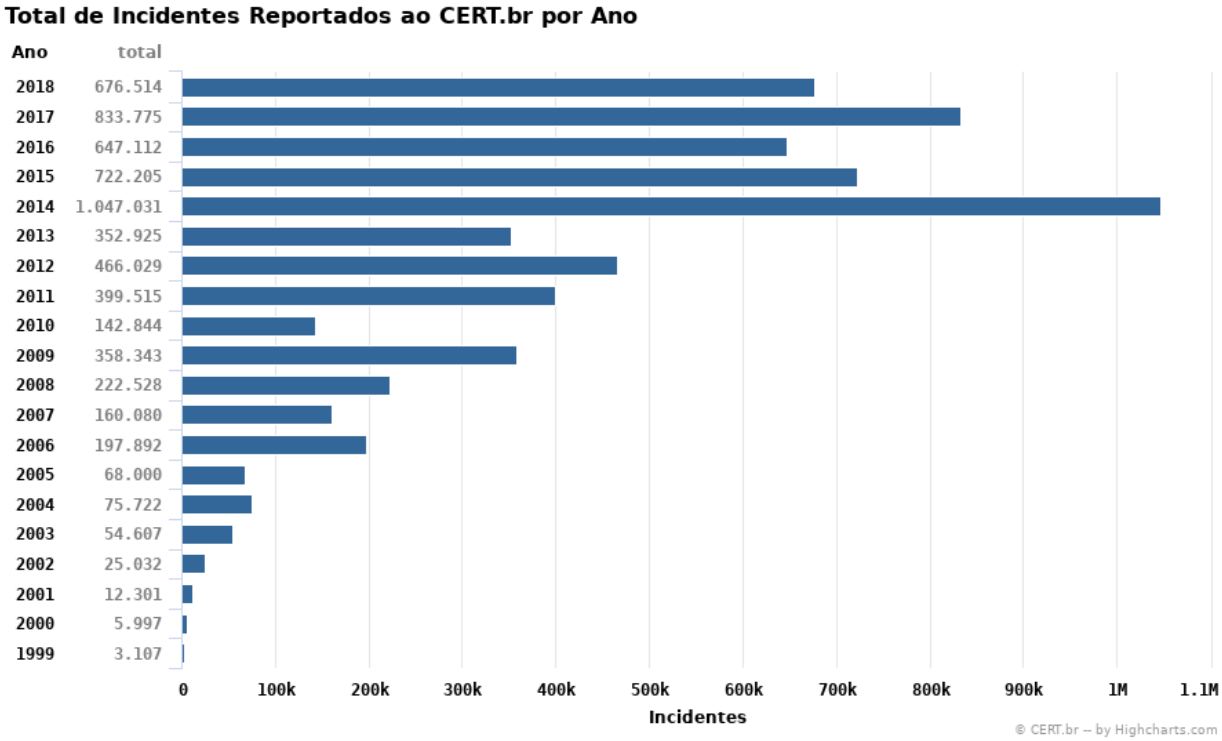
2.1. INCIDENTE CIBERNÉTICO

No contexto da segurança cibernética, evento é qualquer ocorrência observável em um sistema ou rede de computadores. Evento adverso é uma espécie de evento que produz consequências negativas, tais como falha de um sistema, acesso não autorizado a dados sensíveis, destruição intencional ou não de dados. Ao realizar o registro e análise dos eventos torna-se possível identificar quando eventos adversos afetam as políticas de segurança da informação numa organização, que caracterizam a ocorrência de um incidente cibernético (NIST, 2012).

Segundo o Departamento de Segurança da Informação (DSI) do GSI, órgão com competente para supervisionar a atividade nacional de segurança da informação, um incidente cibernético é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou redes de computadores (BRASIL, 2009). Neste trabalho os termos “incidente de segurança”, “incidente de segurança em computadores”, “incidente cibernético” serão tratados apenas como “incidente”.

A Figura 1 exibe a quantidade de incidentes reportados, enviados de forma voluntária, ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Trata-se da base com a série histórica de incidentes a nível nacional mais antiga e mais completa no Brasil. Demostrado, entre picos e vales, a clara tendência de alta da quantidade de incidentes ocorridos nas redes de computadores do país nos últimos vinte anos.

Figura 1: Incidentes por Ano nas redes brasileiras

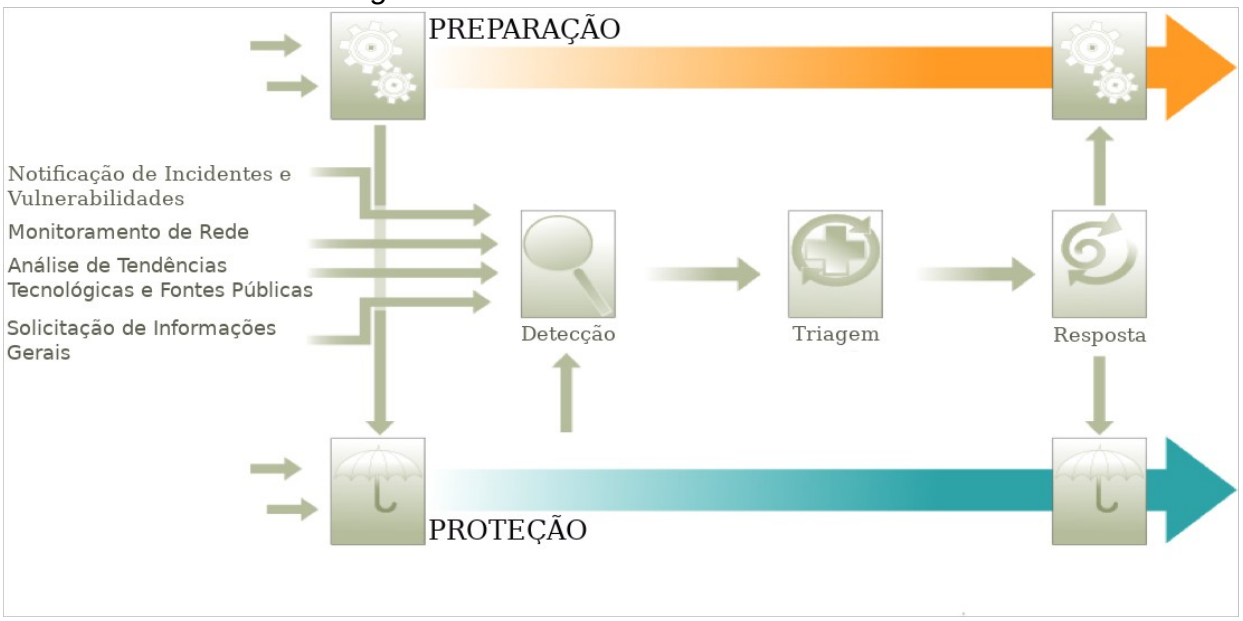


Fonte: CERT.br (2019)

Considerando as definições sobre incidente e observando os dados contidos na Figura 1, identifica-se que a quantidade de incidentes apresentam uma tendência de alta ao longo dos anos. Por isso, faz-se necessário possuir capacidades para gerenciar as ocorrências de incidentes. A Gestão de Incidentes é o conjunto de capacidades que provê a habilidade de gerenciamento dos eventos e incidentes cibernéticos. A plena execução da gestão de incidentes contribui para resiliência operacional das organizações (KILLCRECE, 2005).

A Figura 2 retrata o modelo de melhores práticas propostas por KILLCRECE (2005). Descrevendo a gestão de incidentes em cinco macro processos: Preparação, Proteção, Detecção, Triagem e Resposta. É o modelo atualmente utilizado como referência para as atividades desenvolvidas pelo CTIR Gov na gestão de incidentes.

Figura 2: Modelo de Gestão de Incidentes



Fonte: Killcrece (2005), adaptado pelo autor

Destaca-se que a gestão de incidentes não é apenas a aplicação de tecnologia, por meio de ferramentas e equipamentos, para resolver eventos cibernéticos. Trata-se principalmente de uma atividade de gerencial que demanda o desenvolvimento de um plano de ação, com um conjunto de processos coesos, replicáveis e de qualidade, que possam ser mensurados, por meio de indicadores que possam ser compreendidos dentro da organização (KILLCRECE, 2015). O processo de Preparação, item a seguir, descreve como a gestão pode atuar para criar, controlar e aperfeiçoar as atividades centrais de um CSIRT.

2.1.1. Processo de Preparação

No processo de Preparação são realizadas atividades de sustentação do CSIRT. Ou seja, este processo visa organizar e prover todos os recursos utilizados pelo CSIRT, sejam eles humanos, tecnológicos, de infraestruturas e normativos para que a execução das atividades de gestão de incidentes ocorram de forma coordenada, oportuna e efetiva.

Na Preparação são definidas as funções centrais da gestão de incidentes. Incluindo a determinação dos papeis e responsabilidades, estabelecimento dos meios de comunicação com outras equipes de tratamento ou setores da

organização envolvidas em incidentes, definição de ferramentas essenciais e constituídos procedimentos padrões a serem aplicados no tratamento de incidentes (DOROFEE et al, 2018). Conforme destacado na Figura 2 , a Preparação é uma atividade contínua, ela em conjunto com a Proteção fornece suporte aos outros processos (KILLCRECE, 2005).

2.1.2. Processo de Proteção

No processo de Proteção são executadas atividades para prevenir a ocorrência de incidentes e mitigar impactos quando eles acontecerem. Ou seja, são um conjunto de ações preventivas que visam tornar os sistemas e redes mais resilientes, com o intuito de reduzir ataques bem sucedidos ou reduzir seus danos potenciais (DOROFEE et al, 2018). Este processo é contínuo e envolve toda a gestão de incidentes. Além disso, também recebe as melhorias, sobre a infraestrutura e os processos, oriundas da etapa de Preparação. Observa-se na Figura 2, uma seta partindo da Proteção para Detecção, isto denota o encaminhamento de notificações de incidentes e vulnerabilidades que podem surgir da avaliação contínua da infraestrutura realizada neste processo, as informações levantadas precisam ser repassadas ao processo de Detecção para que sejam agregadas as outras fontes de dados daquele processo (KILLCRECE, 2005).

2.1.3. Processo de Detecção

No processo de Detecção são executadas atividades de coleta de eventos cibernéticos, o conjunto de eventos podem ser observados para identificação de incidentes que já ocorrem ou mesmo para construção de indicadores que possam identificar incidentes futuros (KILLCRECE, 2005). Esse processo tem como insumos não apenas eventos coletados pelos ativos computacionais da organização, mas também recebe informações de vulnerabilidades e incidentes divulgados por fornecedores de softwares e pela mídia especializada, troca de informações sobre ameaças compartilhadas por outras equipes (DOROFEE et al, 2018).

O conjunto de dados apurados no processo de Detecção podem ser tanto reativos, quando se tratam de notificações de incidentes já ocorridos ou em

andamento, quanto proativos, quando se tratam de fatos que possam prevenir a ocorrência de incidentes (DOROFEE et al, 2018). Portanto, a Detecção tem como objetivo coordenar e executar um conjunto de atividades que aumentem a visão do CSIRT sobre sua *constituency*[2], isto é, atividades que forneçam o máximo de informações relacionadas a incidentes ou vulnerabilidades do seu público-alvo. Por fim, esse processo tem como principal artefato de saída incidentes que servirão de insumos para o processo de Triagem, no qual será realizada a primeira análise, ainda superficial, de cada incidente (KILLCRECE, 2005).

2.1.4. Processo de Triagem

No processo de Triagem são executadas tarefas para realizar as primeiras filtragens das ocorrências. Nessa fase são realizadas a classificação e a priorização do incidente, o estabelecimento de relação com outros incidentes/eventos e por fim a atribuição do incidente a um responsável para sua análise aprofundada e possível resolução no processo de Resposta. Portanto, a Triagem serve como um filtro ao processo de Resposta, sendo este o processo no qual efetivamente serão realizadas as investigações mais aprofundadas e efetuado atividades de comunicação (KILLCRECE, 2005).

2.1.5. Processo de Resposta

No processo de Resposta são executadas atividades para se analisar e solucionar os incidentes. É nesta etapa que um incidente é investigado, com intuito de elucidar o seu impacto, o seu escopo e sua tendência na organização. Após o entendimento da ocorrência, o responsável pela análise do incidente, precisa planejar e coordenar ações que devem ser implementadas para conter o impacto, limitar o escopo e mitigar a consecução do incidente, com a finalidade de restabelecer a normalidade das operações da organização.

Diversas outras atividades podem ser incluídas neste processo, tais como:

2 Termo utilizado na comunidade de tratamento de incidentes que denota o público-alvo ou conjunto de clientes de um CSIRT

- coleta de evidências forenses, para possíveis investigações criminais e atribuição de responsabilidade das autoridades legais competentes;
- análise aprofundada dos códigos maliciosos;
- notificações de setores e órgãos envolvidos com o incidente, que possuem responsabilidade na sua resolução ou são impactos pelos danos causados pelo incidente;
- compartilhamento de informações que possam elevar o grau de proteção de outras organizações e CSIRTs.

2.2. CSIRT

Um CSIRT é uma organização, equipe ou grupo responsável por realizar os serviços da gestão de incidentes. Os serviços são frequentemente realizados para um determinado público-alvo, usualmente chamado de *constituency*. A *constituency* de um *CSIRT* pode ser a organização da qual ele faz parte, uma empresa ou uma instituição pública; uma região ou país; ou ainda um cliente *(*KILLCRECE et al*, 2003).*

Existem CSIRTs organizados em diferentes formatos e tamanhos, fornecendo diferentes serviços a sua *constituency*. Recomenda-se a formalização da criação do CSIRT na organização, incluindo a definição da sua missão, do seu modelo ou estrutura organizacional e da sua autonomia, e do seu público-alvo (BRASIL, 2009). Segundo Killcrece et al (2003) os CSIRTs podem ser classificados quanto a sua estrutura organizacional:

- Equipe de Segurança: Neste modelo, não existe setor ou grupo responsável exclusivamente para tratamento de incidentes na organização. A equipe será formada por integrantes da TI que além de suas funções regulares acumulam a resposta à incidentes de forma isolada quando eles ocorrerem, ou seja, geralmente de modo reativo.
- CSIRT Centralizado: No modelo centralizado, a equipe está fisicamente em apenas um local e tem responsabilidade sobre toda a organização ou *constituency.* Em geral, neste modelo, os times estão dedicados as funções do CSIRT.

- CSIRT Distribuído: No modelo distribuído ou descentralizado, a equipe está espalhada dentro da organização ou geograficamente. O pessoal pode atuar operacionalmente de forma independente, no entanto, deve existir uma gerência para coordenar e alinhar as atividades da equipe. Os times podem ser dedicados as funções do CSIRT ou atuar acumulando outras atribuições.
- CSIRT Misto ou Combinado: Este modelo é uma combinação dos CSIRTs Centralizado e do CSIRT distribuído. No qual, existe uma equipe central com atribuições de coordenação e serviços específicos para toda a *constituency*. Enquanto alguns times descentralizados podem se dedicar exclusivamente a alguns setores estratégicos da organização.
- CSIRT de Coordenação: São times, comumente centralizados, que atuam como coordenadores ou facilitadores do tratamento de incidentes em diversas organizações independentes entre si. O CSIRT de Coordenação geralmente possui uma *constituency* maior e um escopo de atuação mais amplo, por outro lado muitas vezes uma autonomia menor dentro das organizações que apoia.

Uma dúvida recorrente quando um CSIRT inicia suas atividades na sua organização é quais serviços serão prestados, como divulgar esses serviços para sua *constituency* e para outros CSIRTs. Esse problema pode ser explicado parte pela falta de padronização dos nomes dos serviços prestados e parte pela complexidade de identificar quais serviços são prioritários para o negócio da *constituency* (SEI, 2002).

Desta forma, o FIRST (2019) estabeleceu um *framework* de serviços para CSIRTs, com o intuito de criar uma linguagem comum entre todos CSIRTs. Objetivo do documento é descrever de maneira ampla a coleção de serviços de segurança cibernética sem a intenção de pormenorizar como estes serviços devem ser realizados, pois entende-se que os serviços podem ser executados de várias formas a depender da realidade de cada CSIRT e sua organização.

Os serviços são agrupados em áreas, essas áreas servem para classificar e agrupar serviços relacionados, facilitando o entendimento e divulgação. A seguir lista-se as áreas e seus respectivos serviços:

- Gerenciamento de Eventos de Segurança (GE): Monitoramento e detecção; Análise;
- Gerenciamento de Incidentes de Segurança (GI): Recebimento de notificações de incidentes; Análise de incidentes; Análise de artefatos e evidências forenses; Coordenação de incidentes; Suporte à gestão de crises.
- Gerenciamento de Vulnerabilidades (GV): Pesquisa / descoberta de vulnerabilidades; Recebimento de notificações de vulnerabilidades; Análise de vulnerabilidades; Coordenação de vulnerabilidades; Divulgação de vulnerabilidades; Resposta à vulnerabilidades;
- Consciência Situacional (CS): Obtenção de dados; Análise e interpretação; Comunicação; e
- Transferência de Conhecimento (TC): Construção de consciência; Educação e treinamento; Exercícios cibernéticos; Assessoria técnica e normativa.

Enquanto, o *framework* de serviços do FIRST (2019) tem como objetivo criar uma nomenclatura para os diversos atividades exercidas por um CSIRT, o modelo de gestão de incidentes descreve como partes destes serviços se integram, ou seja, o modelo de Killcrece (2005) propõe um modo de operacionalizar serviços que são interdependentes, com enfase às boas práticas. Os principais serviços aplicáveis ao modelo de gestão de incidentes são os incluídos nas seguintes áreas de serviço: Gerenciamento de Incidentes de Segurança e Gerenciamento de Vulnerabilidades. Pois possuem serviços que podem ser executados no ciclo Detecção – Triagem – Resposta contemplando ainda os processos ininterruptos de Preparação e Proteção.

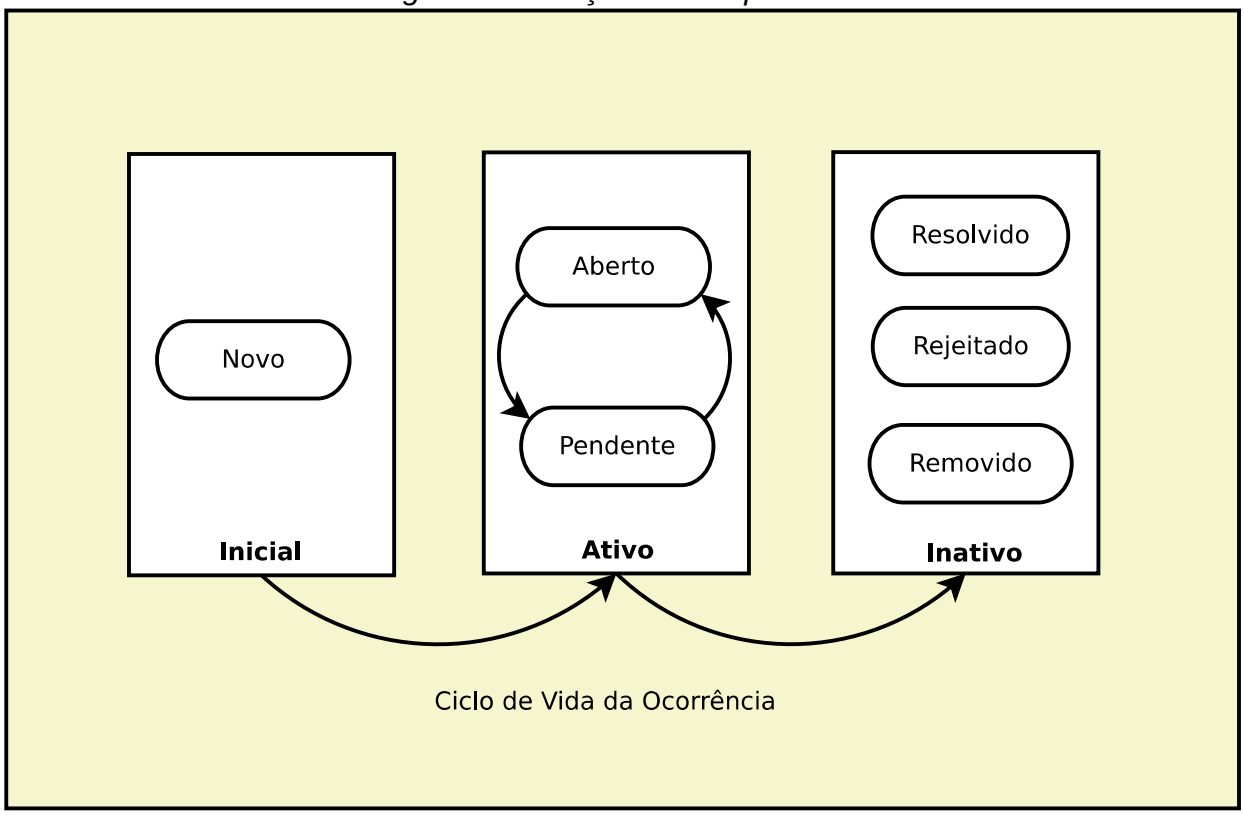
Enfim, os CSIRTs possuem uma gama de serviços que podem exercer, sendo necessário observar o modelo de gestão de incidentes para orientar como esse serviços se relacionam e podem ser executados seguindo as boas práticas. Ao passo que o RT detalhado no item a seguir, tem sido utilizado por muitos CSIRTs como ferramenta que operacionaliza parte desses serviços, em particular, aqueles ligados ao recebimento de notificações, análise das informações recebidas e conclusão dessas ocorrências.

2.3. REQUEST TRACKER

O RT é um *software* livre da classe de ferramentas conhecida por *Issue Tracking System* (ITS). Os ITS são sistemas baseados em ocorrências (ou tíquetes), cujo principal objetivo é rastrear todo o ciclo de vida das ocorrências. Pelo seu caráter genérico, ITS são utilizados amplamente nos mais diversos casos de uso, tal como gerenciamento do ciclo de vida de desenvolvimento de software, no suporte a usuários de computadores, em *call centers* ou mesmo no gerenciamento de projetos.

As situações padrões das ocorrências no RT, como é possível observar na Figura 3, são divididas em três conjuntos lógicos: Inicial, Ativo e Inativo. A situação ou estado que cada tíquete pode passar faz parte de um conjunto lógico. O conjunto “Inicial” por padrão possui apenas o status “Novo” que denota a situação de ocorrências ainda não analisadas. O conjunto “Ativo” por padrão possui os estados *“Aberto” e “Pendente”,* eles denotam situações de ocorrências que ainda estão sendo trabalhadas ou que ainda não foram finalizadas. Enquanto o conjunto “Inativo” por padrão possui os estados “Resolvido”, “Rejeitado” e “Removido”, eles denotam situações finalísticas das ocorrências (BEST PRACTICAL, 2019).

Figura 3: Situações do Tíquete no RT

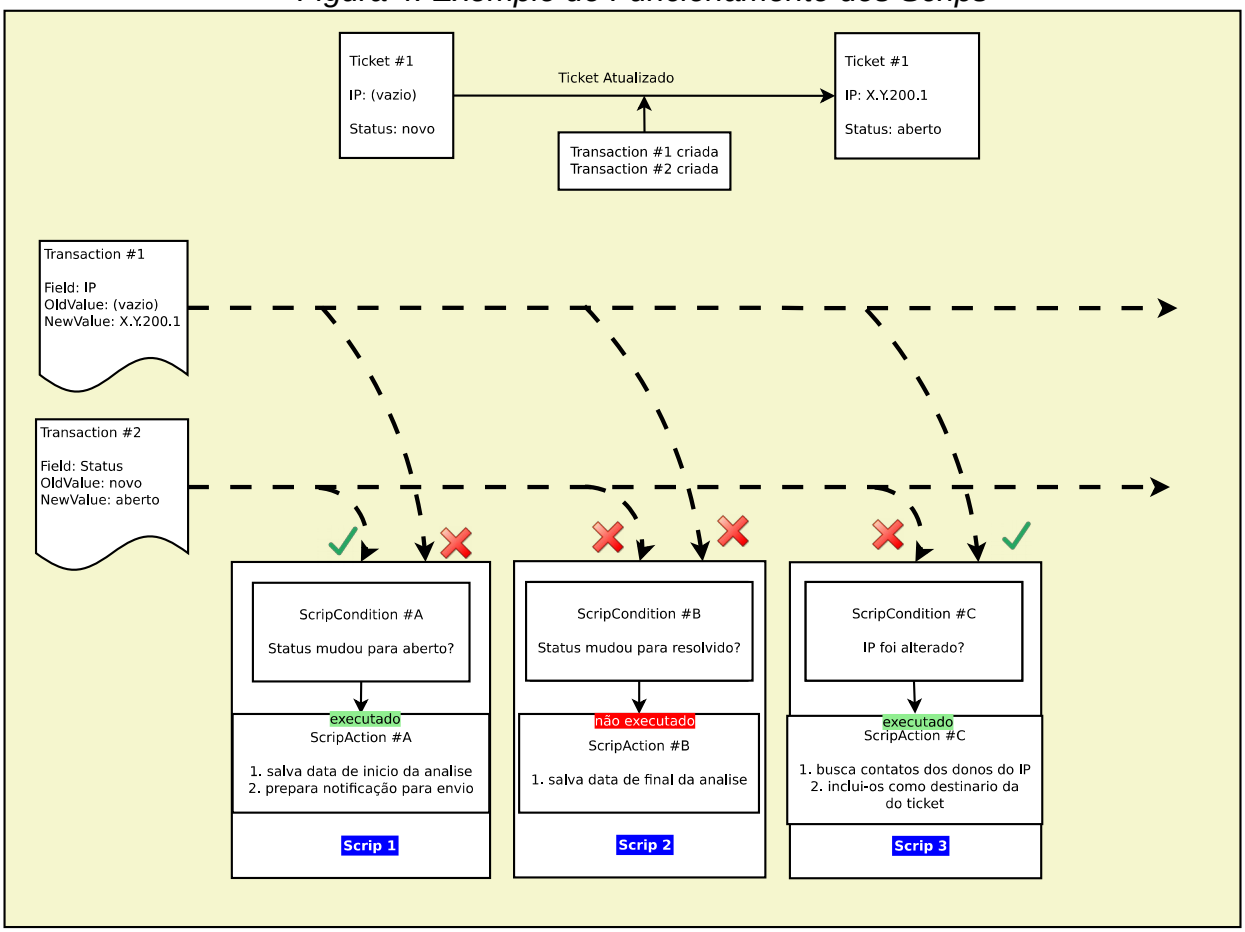


Fonte: O autor

O RT é uma ferramenta flexível que pode adaptar-se a diversos casos de uso, é possível personalizar completamente o ciclo de vida das ocorrências. São configuráveis na ferramenta: os estados*,* respeitando os três conjuntos lógicos apresentados*;* o seu *workflow, ou seja,* quais transições são permitidas entre os estados definidos; e quem terá permissão de realizar cada uma das transições definidas.

Como parte do *workflow* de uma ocorrência, o RT possui uma regra de negócio que potencializa a sua aplicação nos mais diversos casos de uso. Isso é possível pela funcionalidade chamada de Scrips, sua aplicabilidade pode ser observada na Figura 4*.* Os Scrips são compostos de uma condição (*ScripCondition*) e uma ação (*ScripAction*). No exemplo, o "*Ticket #1*" representa uma ocorrência, que teve o campo IP definido e o *status* atualizado para aberto. Cada mudança nas ocorrências são registrados como um nova transação (*Transaction*). Neste caso, a "*Transaction #1*" registra a alteração do IP, de "vazio" para um endereço hipotético "X.Y.200.1". De forma similar a "*Transaction #2*" representa a mudança do *status*, de "novo" para "aberto". Toda vez que uma nova transação é registrada, a ferramenta verifica se as condições de cada *Scrip* foi satisfeita. Ainda na Figura 4, percebe-se que a "*Transaction #1*" satisfaz a condição do "*Scrip 3*", logo neste caso somente o "*ScripAction #C*" é executado. Enquanto a "*Transaction #2*" satisfaz a condição do "*Scrip 1*", portanto neste exemplo somente o "*ScripAction #A*" é executado. Dessa forma, é possível compor um conjunto de condições, que podem ser entendidas como gatilhos, para as ações a serem executadas de forma automatizada (BEST PRACTICAL, 2019).

Figura 4: Exemplo do Funcionamento dos Scrips



Fonte: O autor

A ferramenta pode integrar-se facilmente às organizações, pois ela pode ser configurada para receber todos os e-mails direcionados a um ou mais endereços tais como: suporte@organização, abuse@organização, vendas@organização, etc. Uma equipe da organização pode tanto utilizar a interface web da ferramenta quanto receber mensagens nos seus endereços eletrônicos, cadastrados previamente na sua conta do RT, por meio de automatização via *Scrips (BEST PRACTICAL, 2019)*.

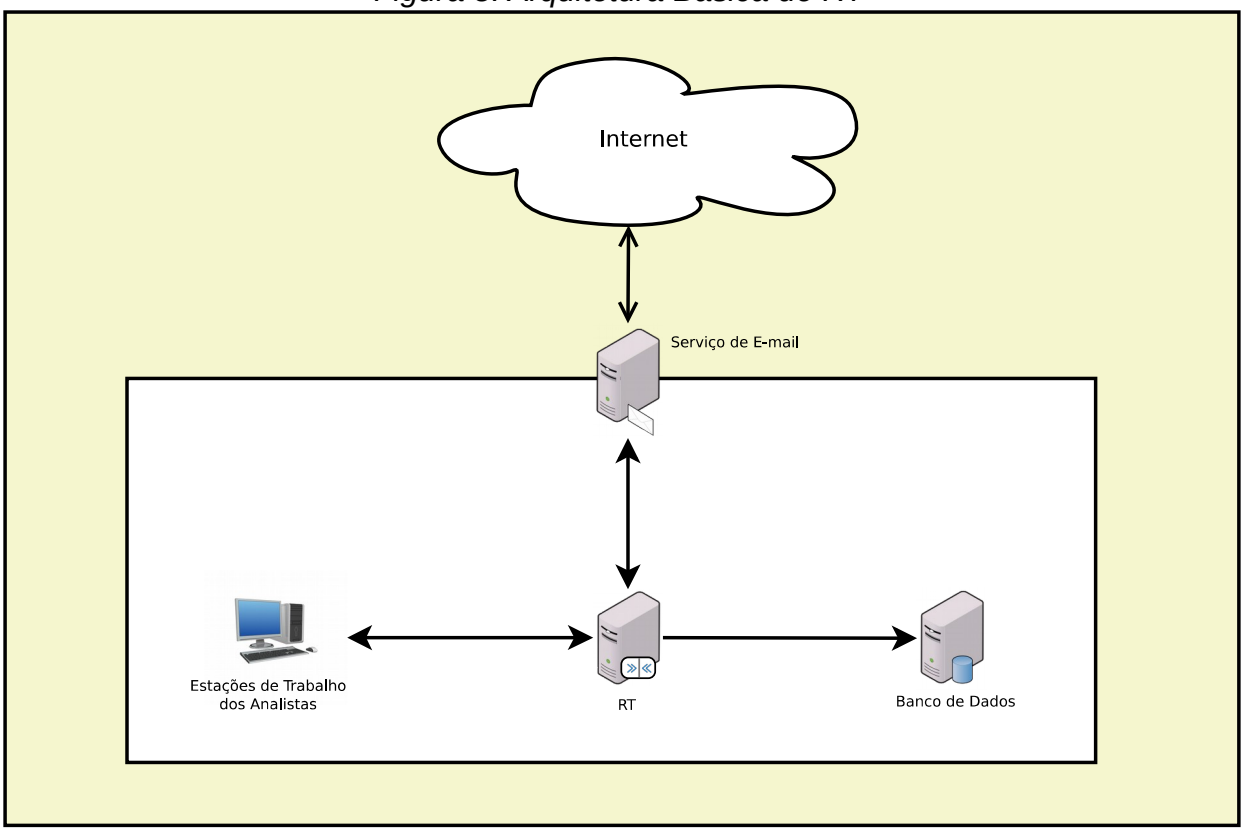
O RT permite ainda a personalização ou ampliação de suas funcionalidades e sua interface via a incorporação de extensões. O RT possui uma gama de extensões públicas e com código aberto (META CPAN, 2019). É possível ainda a implementação de extensões, possibilitando a integração com outros softwares e adaptação mais adequada para a regra de negócio desejada.

Entre diversas funcionalidades da ferramenta, destacam-se ainda: a manutenção do histórico de ocorrências, a qual permite que todos os registros sejam pesquisáveis, incluindo os tíquetes removidos, uma vez que a remoção é lógica;

controle de *Service Level Agreements* (SLA), por meio do qual é possível estabelecer níveis de urgência das ocorrências, em que cada nível possui um tempo máximo de resolução, ao se atribuir um nível de urgência para uma ocorrência, o controle para cumprimento do prazo máximo é feito automaticamente pela ferramenta; e, *dashboards* personalizados, sendo possível criar quadros resumos da situação das ocorrências além de gráficos que podem sintetizar essa informações de maneira visual.

Extrai-se da documentação do RT a sua arquitetura básica, apresentada na Figura 5 (BEST PRACTICAL, 2019). Enquanto apresenta-se um ciclo de tratamento de incidentes básico na Figura 6, para tanto considera-se as situações das ocorrências na Figura 3 e também a modelo de gestão de incidentes na Figura 2.

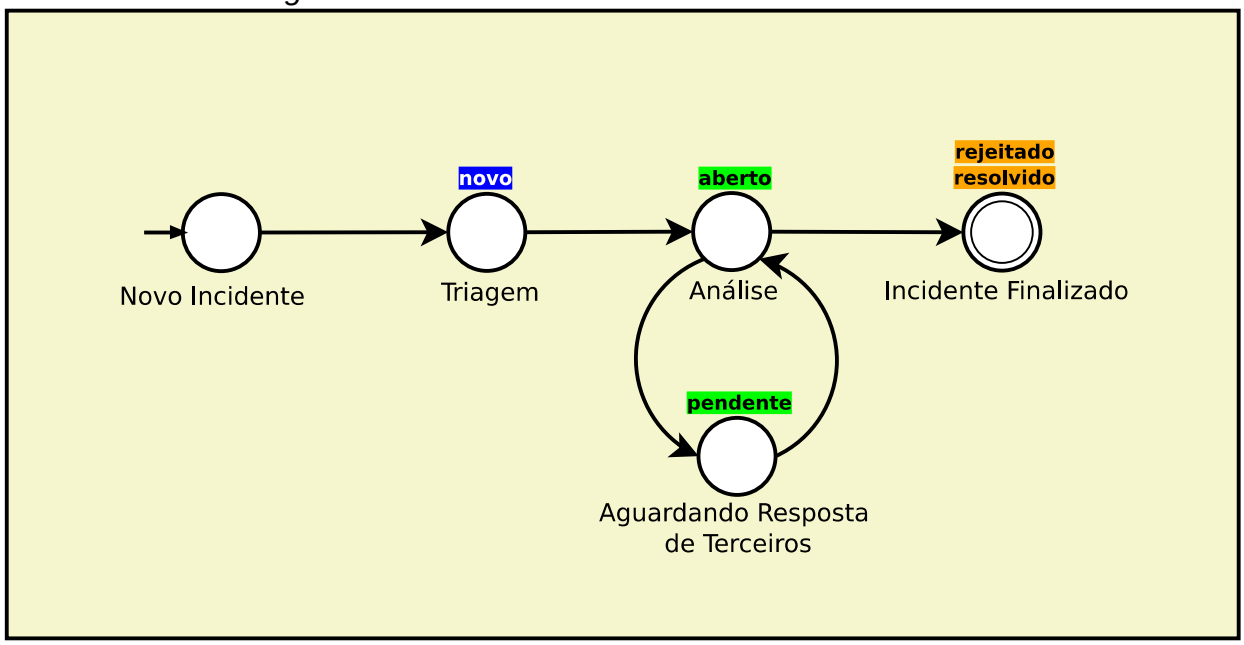
Figura 5: Arquitetura Básica do RT



Fonte: O autor

A Figura 5 exibe a arquitetura básica para o uso do RT, um serviço de e-mail que recebe e envia os e-mails para a ferramenta. O próprio serviço do RT que é utilizado por meio da sua interface *web* por seus usuários. E sua comunicação com o banco de dados transacional que armazena os dados do *software* (BEST PRACTICAL, 2019).

Figura 6: Ciclo de Tratamento de Incidentes Básico



Fonte: O autor

A Figura 6 denota o ciclo de tratamento de incidentes que pode ser adotado na instalação padrão do RT, ou seja, sem considerar a adição de customizações a ferramenta. Este ciclo é passível de ajuste por meio da alteração da configuração do ciclo de vida da ferramenta *(*BEST PRACTICAL, 2019*)*.

Por conta de todo o arcabouço oferecido pela arquitetura do RT é possível adaptá-lo e integrá-lo as mais diversas áreas *(*BEST PRACTICAL, 2019*)*. No tratamento de incidentes, é uma ferramenta poderosa, pois pode ser continuamente ajustada conforme as demandas surjam, de tal forma que novas vulnerabilidades ou incidentes possam ser cobertos pelo *software.* Neste processo incremental e iterativo os mais diversos incidentes e vulnerabilidades podem ser tratados pela Equipe por meio do RT. Além disso, outros serviços de CSIRTs também podem ser oferecidos com a utilização da ferramenta, tais como: análise de artefatos e evidências forenses, divulgação de vulnerabilidades, exercícios cibernéticos e assessoria técnica e normativa.

Neste sentido, Caldas (2011) esclarece as motivações do CTIR Gov quanto a adoção da ferramenta:

> *A escolha do RT foi baseada em algumas características destacadas abaixo:*
>
> - *O RT é multiplataforma, podendo ser instalado inclusive na plataforma de sistemas operacionais utilizada no CTIR Gov;*
> - *A customização das ações do sistema é codificada em Perl, linguagem com vasta documentação disponível;*

- *A distribuição do RT é livre, podendo ser baixado, instalado e modificado livremente de problemas legais ou encargos financeiros;*
- *A utilização do sistema é bastante flexível, permitindo adaptação à diversos tipos de ambientes;*
- *A comunidade de usuários e desenvolvedores do sistema é extensa e mantém listas de discussões e tutoriais que representam importantes fontes de consulta; e*
- *O RT é relativamente fácil de instalar, configurar, personalizar e operar.*

2.4. CTIR GOV

O CTIR Gov atua como CSIRT de coordenação, com responsabilidade nacional, possuindo como público-alvo todos os órgãos e entidades governamentais. Portanto, a missão desse Centro é “coordenar e realizar ações destinadas à gestão de incidentes computacionais, no que se refere à prevenção, ao monitoramento, ao tratamento e à resposta a incidentes computacionais de responsabilidade nacional” (BRASIL, 2019).

Utiliza o modelo centralizado e atua sem autonomia, isto é, possui um time que exerce suas atividades no mesmo local físico, porém, atua sem autonomia na tomada de decisões nos órgãos que apoia, realizando recomendações sobre os procedimentos a serem executados ou medidas de mitigação ou recuperação durante a resolução de um incidente (BRASIL, 2009). A decisão final das ações a serem tomadas e sua execução são responsabilidade dos órgãos envolvidos diretamente nos incidentes. O Centro coopera ainda com outras equipes fora da sua *constituency* sempre que incidentes partam ou atinjam outros entes (CTIR GOV, 2019a).

Quanto aos serviços prestados, o CTIR Gov atua, baseada em nomenclatura própria, com a seguinte lista de serviços e seus correspondentes segundo o *framework* do FIRST (CTIR GOV, 2019a):

Tabela 1: Serviços do CTIR Gov - Comparativo de Nomenclaturas

Nomenclatura do CTIR Gov	**Nomenclatura do FIRST**
Notificação de incidentes	Recebimento de notificações de incidentes Recebimento de notificações de vulnerabilidades
Análise de incidentes	Análise de incidentes Análise de vulnerabilidades
Suporte à resposta a incidentes	Suporte à gestão de crises
Coordenação na resposta a	Coordenação de incidentes

incidentes	Coordenação de vulnerabilidades
Distribuição de alertas, recomendações e de estatísticas	Análise e interpretação Comunicação
Cooperação com outras equipes de tratamento de incidentes	Exercícios cibernéticos Assessoria técnica e normativa.

Fonte: CTIR Gov (2019a)

Enquanto a lista de serviços desde de 2011 até a presente data permanecem praticamente inalterados, as categorias, e principalmente suas subcategorias, de incidentes tratados pelo Centro aumentaram drasticamente no intervalo (CALDAS, 2011):

Tabela 2: Evolução dos Tipos de Incidentes Tratados pelo CTIR Gov

Incidentes Tratados em 2011		**Incidentes Tratados em 2019**	
Categoria	**Qtde de Subcategorias**	**Categoria**	**Qtde de Subcategorias**
Abuso de Sítio	4	Abuso de Sítio	12
Malware	4	Malware	6
Fraude	1	Fraude	5
Vazamento de Informações	2	Vazamento de Informações	4
Escaneamento	1	Escaneamento	1
-	-	Indisponibilidade	1
-	-	DDoS	13
-	-	SSL/TLS	2
Outros	1	Outros	1

Fonte: CTIR Gov (2019b)

A evolução dos tipos de incidentes tratados do CTIR Gov, observada na Tabela 2, pode ser explicada pela busca do Centro em detectar e tratar incidentes mais frequentes ou mais danosos às redes de governo (CTIR GOV, 2019b). Em outro aspecto, a capacidade de adaptação, ao longo dos anos, dos procedimentos e *software* do Centro foi viável por contar uma metodologia focada em melhoria contínua, conforme descrito no item 2.1 e contar com software principal uma ferramenta flexível como RT, conforme descrito no item 2.3.

3. METODOLOGIA

A fim de serem atingidos os objetivos estabelecidos, foi empreendida uma pesquisa bibliográfica e documental, pautada em dissertações, monografias, trabalhos de conclusão de curso, artigos científicos, manuais, leis, normas e reportagens pertinentes ao tema, ao final referenciados. Para a identificação de trabalhos relevantes e atinentes ao tema buscou-se nas bases de dados da Carnegie Mellon University (2019), Revistas Exército Brasileiro (2019), Google Scholar (2019), na Biblioteca Digital do Exército (2019), entre outros sítios. Os principais termos e expressões buscadas foram: “incidente computacional”, “incidente cibernético”, “tratamento de incidentes”, “gestão de incidentes”, “*incident handling*”, “*incident management*”, “*request tracker*” e “*request tracker for incident handling*”.

Se em uma primeira fase a pesquisa bibliográfica e documental serviu como alicerce para identifica-se as principais atividades e serviços, em uma segunda fase aplicou-se uma pesquisa exploratória, por meio do estudo de caso no CTIR Gov, pretendeu-se identificar a estrutura organizacional do Centro, apontar os serviços de CSIRTs prestados pelo órgão, dentre esses serviços realizados destacou-se aqueles que são executados atualmente por meio do RT.

Enquanto, na fase final, buscou-se realizar uma discussão sobre os resultados obtidos na segunda fase, a partir de uma abordagem qualitativa, analisou-se as informações apresentadas, verificou-se a efetividade da utilização do RT no contexto de tratamento de incidentes, objetivo deste trabalho. Apresentou-se ainda, uma conclusão deste trabalho com uma descrição sucinta de todas as etapas realizadas.

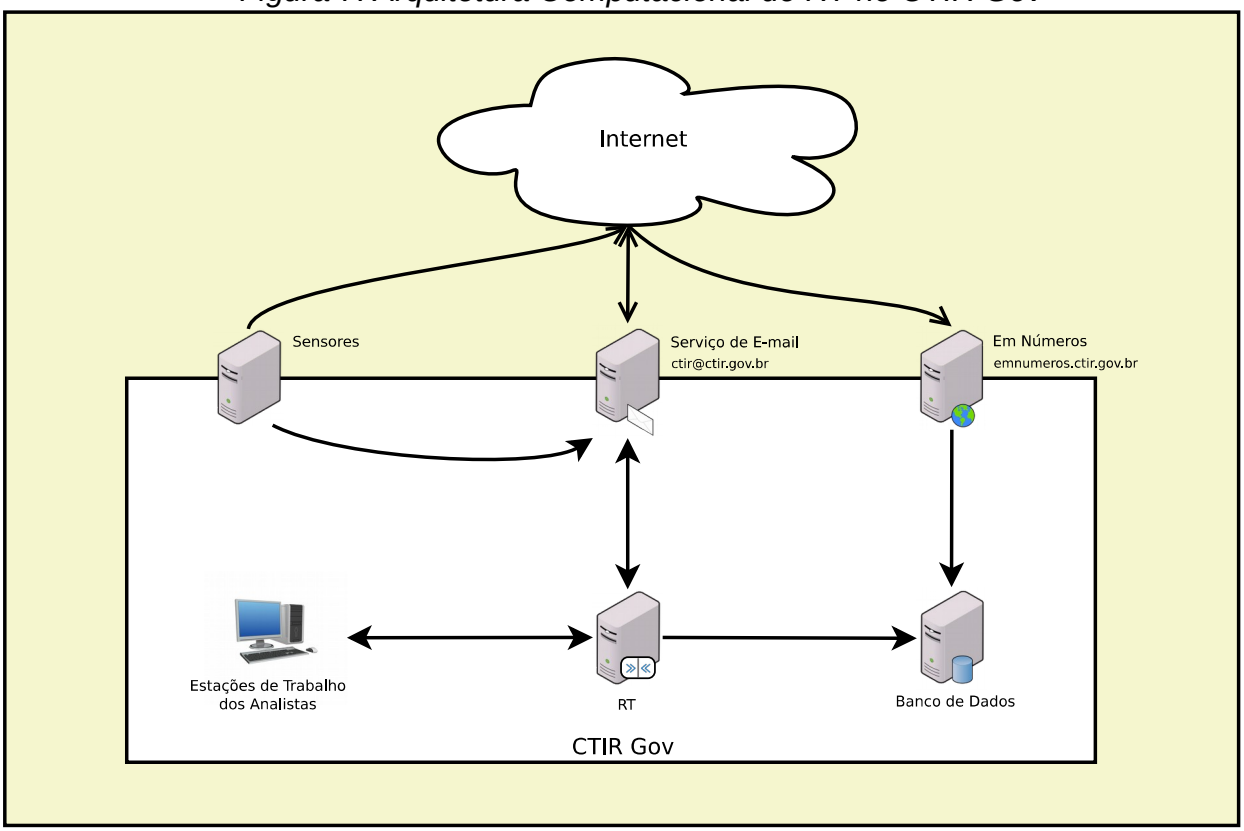
4. RESULTADOS OBTIDOS

A partir da pesquisa bibliográfica e documental e por meio do estudo de caso buscou-se entender a estrutura organizacional, serviços e forma de atuação do CTIR Gov, sobretudo as atividades atinentes ao tratamento de incidentes que são exercidas por meio do *software Request Tracker.* Os resultados são apresentados a seguir.

4.1. APLICAÇÃO DA METODOLOGIA DO CTIR GOV

Por meio da pesquisa bibliográfica, documental e do estudo de caso realizado sobre o trabalho exercido no CTIR Gov, foi possível sintetizar a sua arquitetura computacional para a gestão de incidentes no diagrama da Figura 7.

Figura 7: Arquitetura Computacional do RT no CTIR Gov



Fonte: O autor

A Figura 7 destaca os principais serviços e ativos computacionais na estrutura do CTIR Gov que interagem e/ou dependem do RT. Ressalta-se que esta estrutura exposta é simplificada, desenhada desta maneira para que fosse didática o suficiente para expor os resultados deste trabalho, porém sem o intuito de detalhar as minúcias da infraestrutura do Centro que fugiria o escopo deste estudo. Portanto, por meio deste diagrama é possível observar:

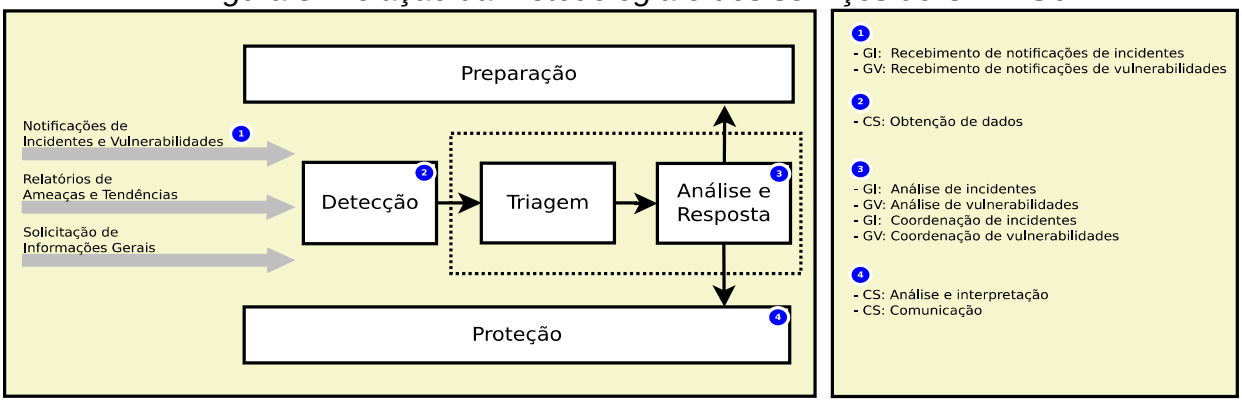
- o Servidor de E-mail: a entrada única de notificações, o e-mail ctir@ctir.gov.br, que entrega cada e-mail para o RT, e este servidor que envia para terceiros as mensagens que saem do RT;

- os Sensores: são um conjunto de serviços desenvolvidos pelo Centro que coletam informações de fontes públicas sobre incidentes ou vulnerabilidades em redes e ativos do governo, são as principais fontes para o processo de detecção do CTIR Gov, ao detectar possíveis incidentes remetem estes por e-mail ao RT;
- as Estações dos Analistas: representam as estações de trabalho dos analistas do CTIR Gov, que acessam o RT para tratar as ocorrências de incidentes;
- o RT: o sistema de ocorrências interage com os e-mails recebidos e com as interações dos analistas, de forma automática, de acordo com as condições e ações preestabelecidas, assim como registra cada mudança realizada;
- o BD: mantém todos os registros do RT, destaca-se que cada e-mail e seus anexos recebidos ou enviados por meio do RT, são registrados este banco de dados;
- o Em Números: site do CTIR Gov (2019b), que expõem informações públicas sobre as estatísticas de incidentes de governo, que sumarizam os dados das ocorrências de incidentes do RT, acessíveis por meio do seu banco de dados.

Dadas as interações dos ativos computacionais do Centro, é possível aprofundar o estudo, e analisar como é aplicado o modelo de gestão de incidente e sua relação com os serviços prestados por aquele CSIRT.

Na Figura 8, no quadro direito, lista-se os serviços do CTIR Gov, segundo a nomenclatura do FIRST (2019). Utilizou-se o padrão estabelecido pelo FIRST por tratar-se de uma definição comum entre CSIRTs. Ressalta-se que para construir esta lista utilizou como base as informações do item 2.4, quanto os serviços divulgados e prestados pelo Centro. De forma similar, ainda na Figura 8, o quadro da esquerda retrata o modelo de gestão de incidentes, aplicados conforme o item 2.1 deste trabalho, adicionalmente ressalta-se as círculos em azul e numerados que relacionam as etapas neste modelo com os serviços, do quadro a direita, no momento em que são executados.

Figura 8: Relação da metodologia e dos serviços do CTIR Gov

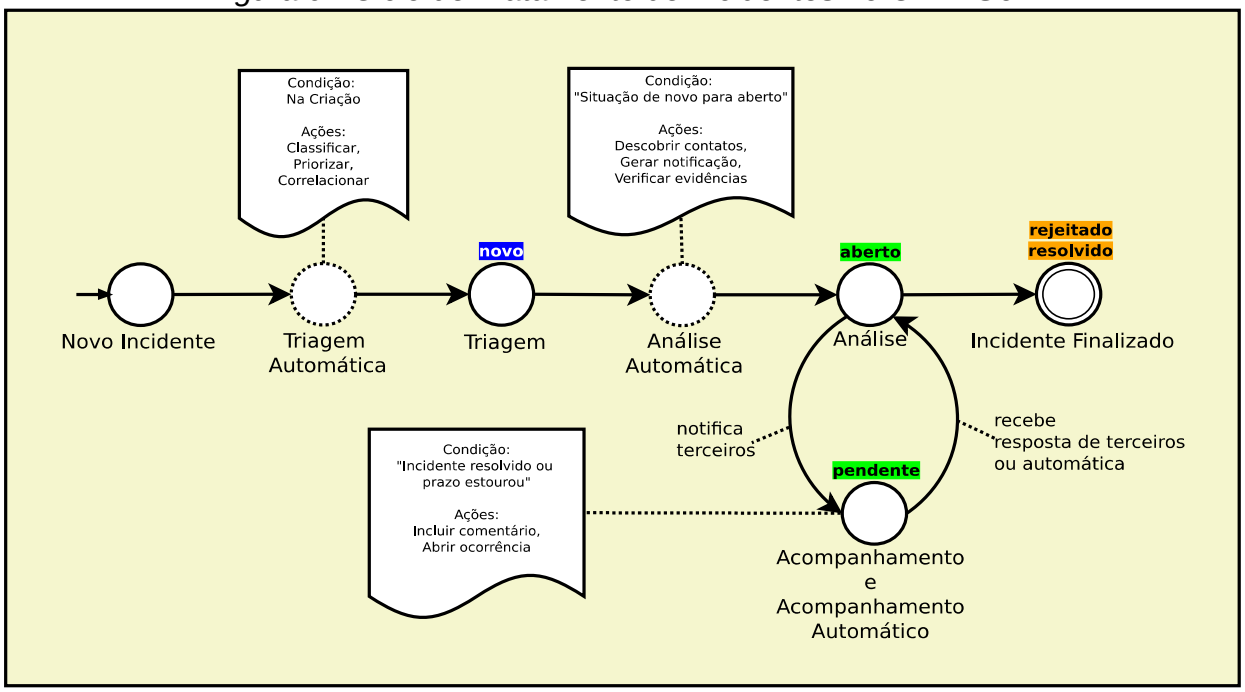


Fonte: O autor

Delimita-se em linha traceja, na Figura 8, as principais atividades realizadas pelo RT, que são aquelas dos processos de triagem e de análise e resposta, além disso a ferramenta recebe as ocorrências via notificações externas ou do processo de detecção interno, conforme descrito na Figura 7.

A Figura 9 representa um diagrama de estados que denota o ciclo de vida de uma ocorrência de incidente mais comum no CTIR Gov, incluindo os eventos executados de forma automatizada pelo RT, que foram representados pela ligação pontilhada.

Figura 9: Ciclo de Tratamento de Incidentes no CTIR Gov



Fonte: O autor

Cada etapa do diagrama da Figura 9 é explicada a seguir:

- Criação do Incidente: denota a detecção de um novo incidente, pelos mecanismos de sensores do Centro ou pelo recebimento de notificação de incidentes;
- Triagem Automática: realizada pelo RT, antes da Triagem, por meio de personalização da ferramenta, executada sempre que uma ocorrência for criada, tem como objetivo classificar, priorizar e correlacionar, facilitando o execução da triagem humana que revisará as ações tomadas por essa etapa;
- Triagem: realizada por um analista, são as atividades de classificação do incidente, do estabelecimento de relação com outros incidentes e/ou vulnerabilidades, da priorização do incidente e atribuição a um outro analista que irá analisá-lo;
- Análise Automática: realizada pelo RT, antes da Análise, por meio da personalização da ferramenta, executada sempre que a situação da ocorrência passar de novo para aberto, tem como objetivo verificar as evidências, identificar os contatos dos responsáveis pela rede ou sistema afetado, criar mensagem de notificação;
- Análise: realizada por um analista, são as atividades relacionadas ao exame mais aprofundado da ocorrência, na qual revisa-se as ações da Triagem, verifica-se e coleta-se evidências e, caso se confirme o incidente e/ou vulnerabilidade, notifica-se os responsáveis pela rede ou sistema afetado;
- Acompanhamento: realizada por terceiros, após notificação a ocorrência permanece na situação pendente, até que seja solucionada e respondida pelo responsável da rede ou sistema afetado. Sempre recebe uma resposta de terceiros o RT a inclui no histórico da ocorrência e muda a situação de pendente para aberto;
- Acompanhamento Automático: realizada pelo RT, por meio da personalização da ferramenta, executada enquanto a situação da ocorrência permanece pendente, tem como objetivo verificar se as

evidências indicam que o incidente e/ou vulnerabilidade ainda não foi tratada pelos seus responsáveis. Caso a ocorrência seja solucionada o mecanismo automático muda a situação para aberto, para nova análise do analista. Ou caso o prazo de resolução da ocorrência estoure o mecanismo abre a ocorrência, para o analista realizar nova notificação aos responsáveis. Nos dois casos são criados comentários para subsidiar as ações do analista;

- Resolução do Incidente: realizada pelo analista, após interações com terceiros, e após reanálise que comprove sua resolução o analista move a ocorrência para a situação resolvida, ou rejeitada caso as evidências indiquem que se trata de um falso positivo.

A partir da Figura 9 torna-se exequível descrever e analisar mais aprofundadamente a arquitetura do RT aplicado ao negócio de um CSIRT. Destaca-se as principais customizações realizadas e suas razões, ou seja, relaciona-se as alterações no RT com os processos do modelo de gestão de incidentes, considerando ainda os serviços executados.

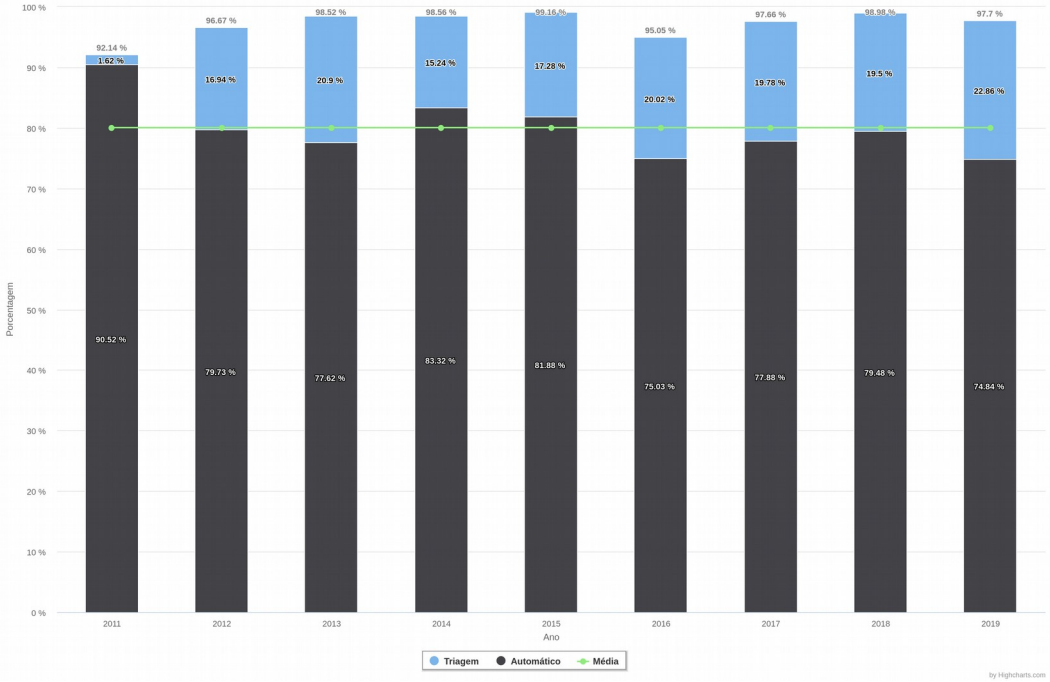
4.2. APRESENTAÇÃO DAS TAXAS DE DESEMPENHO

A partir das informações levantas no item 4.1, e do levantamento de dados das ocorrências, não disponibilizados publicamente, foi possível avaliar a efetividade da utilização do RT para o tratamento de incidentes. Ressalta-se que os dados, utilizados para se obter os resultados, foram consolidados a partir do banco de dados do RT, mais especificamente do histórico de transações das ocorrências desde a implantação do RT no CTIR Gov em 2011 até o Setembro de 2019. Este banco de dados completo trata de informações de acesso restrito, por possuir informações de incidentes nos órgãos e entidades públicas, por este motivo esses dados não são disponibilizados publicamente.

Sobre os Gráficos 1 e 2, observa-se a eficiência do processo da Triagem Automática, especificado no item 4.1. No Gráfico 1, exibe-se a taxa de acerto da classificação automática. No Gráfico 2, exibe-se a taxa de acerto da priorização automática. Durante a Triagem Automática, uma ocorrência é classificada em uma categoria de incidente, é também priorizada segundo informações contidas na

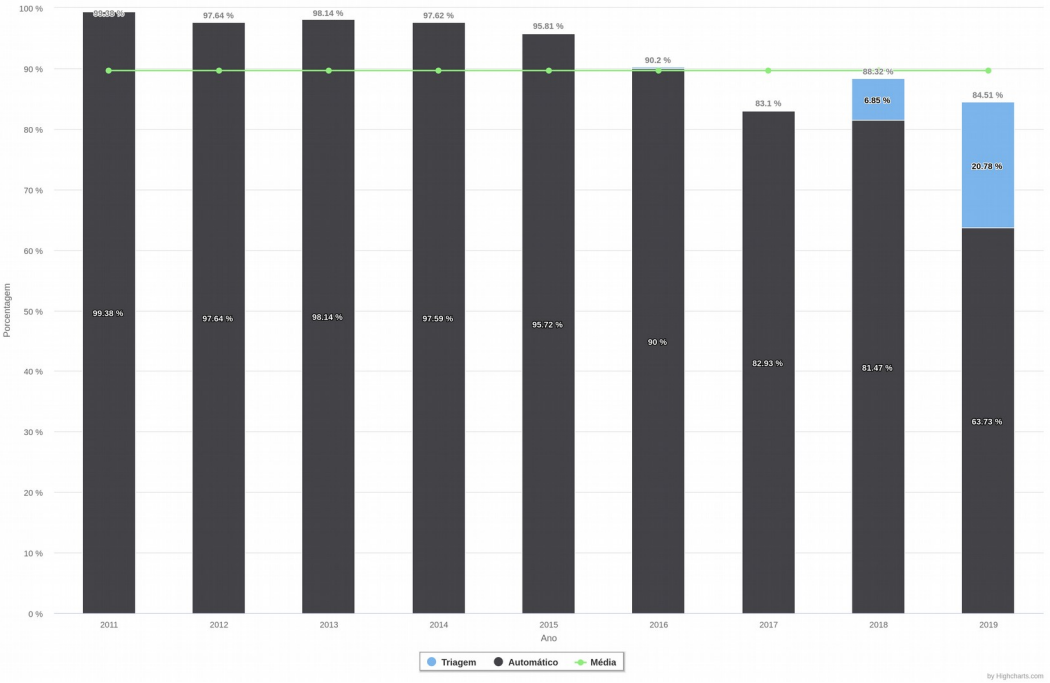
ocorrência. Com base nisso, considera-se que uma ocorrência foi classificada corretamente se durante todo o ciclo de vida, não precisou ser reclassificada, seja no processo de Triagem ou no processo de Análise. A mesma lógica foi aplicada para considerar a correta priorização.

Gráfico 1: Taxa de Acerto da Classificação por Ano



Fonte: O autor

Gráfico 2: Taxa de Acerto da Priorização por Ano

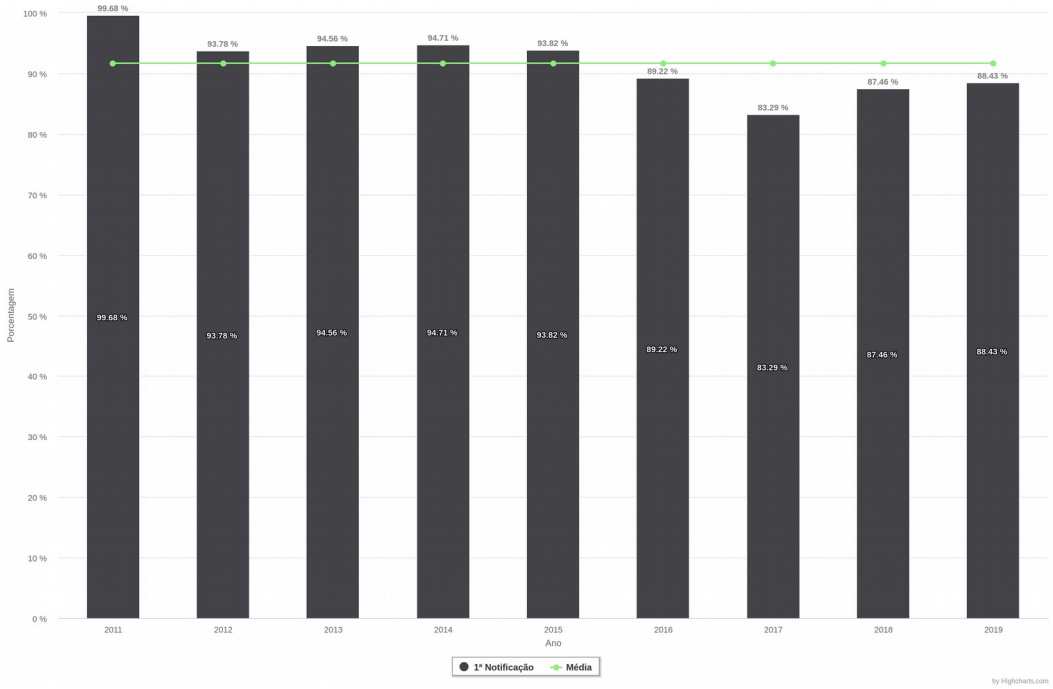


Fonte: O autor

No Gráfico 1, verifica-se uma média de 80% de acerto do processo automatizado quanto a classificação dos incidentes, enquanto na Triagem são reclassificados em média 17% dos incidentes. De maneira análoga, no Gráfico 2, verifica-se uma média de 90% de acerto do processo automatizado quanto a priorização dos incidentes, uma taxa média alta, porém tem ocorrido uma queda da taxa, ano contra ano desde 2014, no ano de 2019 a taxa encontra-se em 64%. Em 2019 foram corrigidas as prioridades de cerca de 21% dos incidentes no processo de Triagem, contra uma média de apenas 3% por ano.

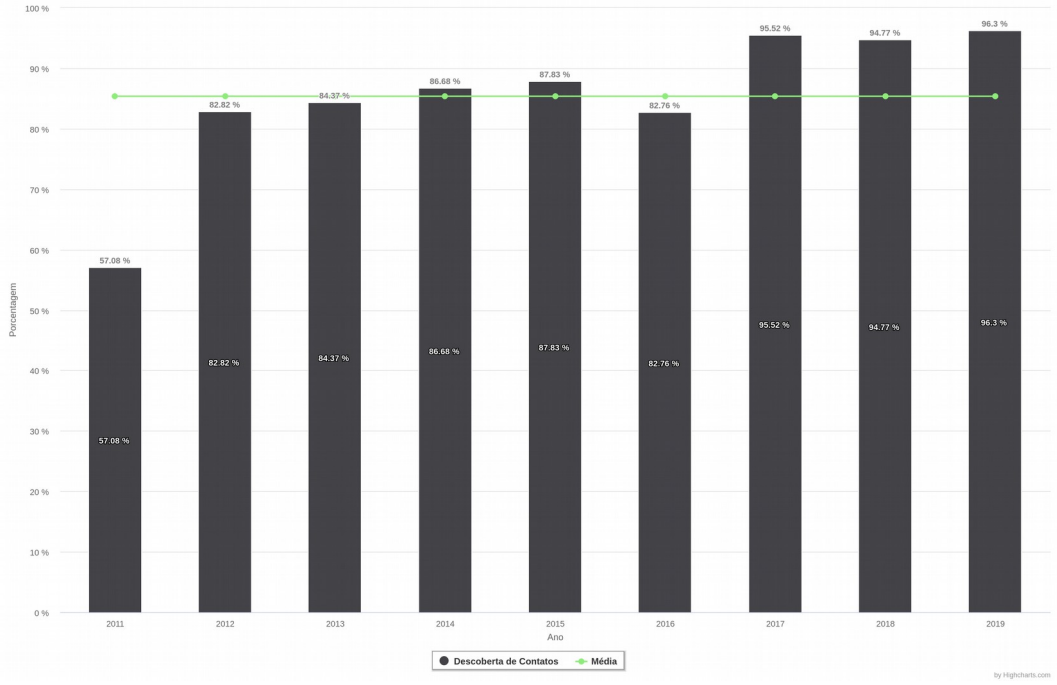
Quanto aos Gráficos 3 e 4, nota-se a eficiência do processo de Análise Automática, especificado no item 4.1. Durante a Análise Automática, é gerada uma mensagem notificação e descoberto os contatos pela resolução dos incidentes, os responsáveis pelas redes ou sistemas afetados pelo incidente. Pois, no processo de Análise a ocorrência é examinada e caso identifique-se evidências que o incidente ocorreu ou ainda está em curso, o incidente é reportado por meio da notificada gerada aos responsáveis identificados. Com base nisso, optou-se por medir a eficiência da geração automática das notificações por meio da taxa de resolução de incidentes na primeira notificação, como forma de medir a qualidade e efetividade das mensagens geradas. Enquanto, para medir a eficiência da descoberta automática de contatos considerou-se que um contato foi bem obtido corretamente se durante todo o ciclo de vida da ocorrência, não foi necessário alterar manualmente o contato dos responsáveis. Desta forma no Gráfico 3, exibe-se a taxa de resolução de incidentes na primeira notificação. No Gráfico 4, exibe-se a taxa de acerto na descoberta automática dos contatos.

Gráfico 3: Taxa de Resolução de Incidentes na 1ª Notificação por Ano



Fonte: O autor

Gráfico 4: Taxa de Acerto na Descoberta Automática de Contatos por Ano



Fonte: O autor

No Gráfico 3, verifica-se, que em média, 92% dos incidentes são resolvidos na primeira notificação realizada pelo CTIR Gov, no entanto, exibe-se uma taxa abaixo da média nos últimos quatro anos. No Gráfico 4, verifica-se que em média, 85% dos incidentes são notificados somente com a descoberta automática dos

contatos, ou seja, em média apenas 15% dos incidentes precisam de inclusão manual dos endereços de e-mail dos responsáveis pela resposta aos incidentes.

5. DISCUSSÃO DOS RESULTADOS

O papel da gestão de incidentes computacionais é prover resiliência ao negócio da organização, por meios dos seus processos, boas práticas e um conjunto de serviços bem definidos e plenamente executados (KILLCRECE, 2005). A capacidade de resposta a incidentes tem como benefícios: resposta coesa e sistemática a incidentes, mitigação dos danos e melhoria contínua (NIST, 2012).

Com base nestas premissas, este estudo buscou descrever, no item 4.1, como a gestão de incidentes é aplicada no CTIR Gov, com o intuito de avaliar qualitativamente a sua aderência às boas práticas. Para tal, percorreu-se três níveis: arquitetura computacional para a operação do tratamento de incidentes, a metodologia e serviços; finalizando operação e personalização do RT.

Sobre a arquitetura descrita no item 4.1, percebe-se que todos os incidentes são tratados de forma sistemática, os e-mails são enviados ao RT, os analistas tratam os incidentes recebidos da mesma forma por meio da interface do RT, todas as notificações enviadas saem pelo mesmo e-mail do Centro. Por fim, todas as ocorrências de incidentes compõe uma base de dados única que além de ser utilizada como fonte de conhecimento para apoiar o tratamento de novos incidentes, é utilizada para se analisar tendências e fornecer estatísticas de forma pública. Percebe-se que a arquitetura computacional, utilizada pelo CTIR Gov, é comparável a arquitetura básica do RT, exibida na Figura 5, e atende os seus requisitos mínimos.

Portanto, sob essa perspectiva observa-se atividades do processo de preparação, conforme o item 2.1.1, de forma coesa e consolidada. Além disso, nota-se a dinâmica e a interdependência de alguns serviços, tais como o recebimento de notificações de incidentes, monitoramento e detecção e a comunicação da consciência situacional, conforme o item 2.2. Entretanto, apesar da análise da arquitetura contextualizar a aplicação do RT numa situação real e palpável, a observação somente desta visão não contempla aspectos sobre todos os processos e as boas práticas, por este motivo, apresenta-se em seguida a análise da metodologia e serviços.

Quanto a aplicação da metodologia e seus serviços, o trabalho descreveu o diagrama que exibe o modelo de gestão de incidentes adaptado a

realidade daquele Centro. Comparando os diagramas das Figuras 2 e 8, observa-se que a metodologia do CTIR Gov aplica grande parte das boas práticas estabelecidas por Killcrece (2005). Destaca-se a plena execução dos processos de triagem e análise por meio do RT; do processo de preparação, por meio de sua infraestrutura e atividades de melhoria continua e do processo detecção por meio de sensores em fontes abertas. Nota-se algumas divergências: o CTIR Gov não realiza monitoramento de redes, pois não tem autonomia das redes e sistemas que fornece seus serviços; outra divergência é forma como executam seus processos de proteção, no CTIR Gov atua como um provedor de informações sobre ameaças e tendências para seus clientes e parceiros, enquanto o referencial teórico propõe a execução de tarefas elevação da resiliência das redes e sistemas. Essas divergências acontecem pois o CTIR Gov é um CSIRT de coordenação, por esse motivo atua apoiando outras equipes a realizarem atividades como o monitoramento e proteção dos seus próprios ativos computacionais, ou seja, realiza estas atividades de forma indireta por meio dos órgãos que apoia.

Finalizando a análise qualitativa, concentra-se no ciclo de vida do tratamento de incidentes, realizado pelo RT. Ainda no item 4.1, descreve-se o diagrama de estado, que apresenta o fluxo de tratamento de incidentes dentro do RT, do qual destacam-se os processos de triagem e análise, além do acompanhamento do incidente. Comparando os diagramas das Figuras 6 e 9, observa-se que por padrão o RT não realiza tarefas automatizadas que corroboram substancialmente para o tratamento de incidentes conforme as boas práticas, e que as mudanças percebidas na Figura 9 incluem melhorias na automatização de atividades previstas nos itens 2.1.4 e 2.1.5. Essas mudanças foram realizadas por meio de customizações implementadas no RT, e teve como resultado maior coesão dos incidentes tratados, aumentou a capacidade de processamento da equipe. Esses resultados são sustentados pela análise quantitativa realizada no item 4.2.

Este trabalho propôs-se também analisar de forma quantitativa a efetividade da gestão de incidentes por meio do RT. Desta forma, optou-se por avaliar a intervenção automatizada em relação ao processo manual. Este estudo foi realizado no item 4.2, onde elegeu-se quatro métricas descritas a seguir.

Para avaliar a triagem automatizada, obteve-se a taxa de acerto da classificação e da taxa de acerto da priorização, que teve como resultados índices médios, respectivamente, de 80% e 90%. Esses índices elevados colaboram para

demonstrar a maturidade e consistência da implementação do RT e da operação do CTIR Gov quanto ao processo de triagem.

Diante da piora a taxa de acerto da priorização automatizada, nos últimos anos, sobretudo em 2019, e considerando a metodologia aplicada no Centro, pode-se inferir que esta queda deve-se a mudanças implantadas desde 2017 com intuito aperfeiçoar o processo de triagem manual, pudesse ser mais criterioso na priorização dos incidentes recebidos.

Para avaliar as tarefas automatizadas executadas antes da análise, utilizou-se a taxa de resolução de incidentes na primeira notificação e da taxa de acerto na descoberta dos contatos dos envolvidos no incidente, como resultado obteve-se índices médios, respectivamente, de 90% e 85%. Esses indicadores reforçam os dados obtidos na primeira fase dos resultados, em 4.1, pois demonstra que sem as implementações nesta fase, grande parte dos trabalhos teriam que ser feitos manualmente ou por reiteradas vezes, o que diminuiria substancialmente a velocidade do tratamento dos incidentes.

No Gráfico 3, que exibe a taxa de resolução de incidentes na primeira notificação, exibe-se uma taxa abaixo da média nos últimos quatro anos. Levantou-se algumas hipóteses sobre a causa desta piora: modelos de notificação desatualizados, sendo necessário revisá-los ou a quantidade de modelos não atendem as variações de incidentes, sendo necessário construir novos modelos de notificação. No Gráfico 4, que exibe a taxa de acerto na descoberta dos contatos, percebe-se uma significativa melhora nesta métrica nos últimos três anos, com uma média superior a 95% das ocorrências neste período.

6. CONCLUSÃO

Iniciou-se este artigo contextualizando o ambiente cibernético que vive a sociedade, proporcionando por um lado facilidades e por outro criando uma dependência, portanto sendo necessário mais segurança e resiliência no ambiente computacional. Após a contextualização, foram descritos os diversos conceitos relevantes à pesquisa dos quais destaca-se o conceito de incidente cibernético, o conceito e importância do modelo de gestão de incidentes, contemplando suas etapas e características; o conceito de CSIRT, suas características, seus tipos e sua forma de atuação, bem como a descrição dos diversos serviços exercidos pelos CSIRTs;

descreveu-se as características dos ITS e sua aplicação na resolução de ocorrências, sendo detalhado as capacidades do RT; por fim foram descritas a estrutura e características do CTIR Gov, objeto deste estudo de caso.

Este artigo então, mostrou em uma primeira etapa a aderência das atividades do CTIR Gov as boas práticas na gestão de incidentes computacionais. Podendo extrair adicionalmente, quais são os principais processos e serviços realizados e quais destes são executados por meio do RT. Na sequência, como segunda etapa, validou-se a primeira etapa, por meio do levantamento de métricas e dados de uso do RT, que permitiu avaliar de forma quantitativa a efetividade do tratamento de incidentes operacionalizado por meio do RT.

Para encerrar este artigo, realizou-se a discussão dos resultados obtidos com a pesquisa, por meio do qual foi possível concluir que a metodologia aplicada pelo CTIR Gov, é calcada nas boas práticas e que a operação dos seus principais serviços por meio do RT, já alcançaram um nível de maturidade capaz de atender as demandas de incidentes detectados ou notificados àquele Centro. Ainda assim foram propostas algumas melhorias na personalização da ferramenta, dentre estas destaca-se a inclusão da análise de efetividade como funcionalidade da ferramenta, para suporte ao processo de melhoria continua.

Portanto, conclui-se que este trabalho alcançou seu objetivo em analisar a efetividade do tratamento de incidentes por meio do RT, pois comparou qualitativamente a sua aplicação em relação ao referencial teórico e depois utilizou indicadores para avaliar a eficiência das personalizações na ferramenta, que aprimoram o tratamento de incidentes executado pelo CTIR Gov.

Quanto ao processo de triagem automatizada, este trabalho propõe como sugestão para elevar a taxa, a atualização do processo automatizado de priorização, com a construção de uma matriz de prioridade baseado no processo realizado atualmente de forma manual. Desta forma, espera-se que a priorização automatizada volte a ser tão eficiente quanto a sua média histórica.

Apesar de ter alcançado seus objetivos o presente trabalho teve alguns obstáculos. Durante a realização desta pesquisa, o principal óbice encontrado foi a dificuldade de obter mais indicadores sobre o desempenho do RT, isso deveu-se pelo fato que a regra de negócio do CTIR Gov não foi concebida para a realização dessa

análise de efetividade, e alguns dados, julgados importantes para a análise, não são registrados. Outro fator crítico, que impactou em um primeiro momento o estudo, foi o pouco tempo disponível para realização desta pesquisa, isto impactou inicialmente a descoberta de artigos científicos correlatos a este trabalho.

Além das dificuldades expostas, este trabalho possui algumas limitações tais como: os dados utilizados para obtenção dos indicadores, que foram utilizados para análise de efetividade, possuem acesso restrito, o que reduz a possibilidade de outros trabalhos validarem ou ampliarem o presente estudo; não houve análise comparativa dos indicadores utilizados e um referencial teórico, o que também restringe validação mais consistente do trabalho.

Em razão do exposto, sugere-se como trabalhos futuros: aprofundar análise de efetividade, realizando-a por tipo de incidente e/ou incluindo novas métricas; sistematizar a análise de efetividade, incluindo-as como relatório no RT, possibilitando uma análise em tempo real; realizar um estudo comparativo dos resultados obtidos neste trabalho com o tratamento de incidentes realizado por outros CSIRTs de coordenação, tal como os CSIRTs militares.

REFERÊNCIAS

BBC. **Cyber-attack: US and UK blame North Korea for WannaCry.** Dez 2017. Disponível em: <https://www.bbc.com/news/world-us-canada-42407488>. Acesso em: 25 Jul 2019.

BEST PRACTICAL. **RT 4.4.4 Documentation**. Mar 2019. Disponível em: <https://docs.bestpractical.com/rt/4.4.4/index.html>. Acesso em: 18 Set 2019.

BRASIL. Decreto nº 9.668, de 2 de janeiro de 2019. **Estrutura Regimental e Quadro de Cargos do Gabinete de Segurança Institucional da Presidência da República.** Diário Oficial da República Federativa do Brasil, Brasília, 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9668.htm>. Acesso em: 11 Set 2019.

BRASIL. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009. **Criação de Equipes de Tratamento e Resposta de Incidentes em Redes Computacionais – ETIR**. Departamento de Segurança da Informação (DSI/GSI/PR), Brasília, 2009. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_05_etir.pdf>. Acesso em: 6 Jul 2019.

CALDAS, Tiago de Barros. **Análise da Instalação da Ferramenta Request Tracker no CTIR Gov**. UnB: Brasília, 2011. 73 p. Monografia (especialização) – Universidade

de Brasília. Instituto de Ciências Exatas. Departamento de Ciência da Computação, 2011.

CAMBRIDGE DICTIONARY. **Exploit Meaning**. Out. 2019. Disponível em: <https://dictionary.cambridge.org/dictionary/english/exploit>. Acesso em: 05 Out 2019.

CERT.br. **Estatísticas dos Incidentes Reportados ao CERT.br**. Jan. 2019. Disponível em <https://www.cert.br/stats/incidentes/>. Acesso em: 31 Ago 2019.

CTIR Gov. **Sobre o CTIR Gov**. Set 2019. Disponível em: <https://www.ctir.gov.br/sobre/>. Acesso em: 22 de Set de 2019.

CTIR Gov. **CTIR Gov Em Números**. Set 2019. Disponível em: <https://emnumeros.ctir.gov.br>. Acesso em: 27 de Set de 2019.

DOROFEE, Audrey. et al. **Incident Management Capability Assessment.** Carnegie Mellon University: Pittsburgh, 2003. Disponível em: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538848>. Acesso em: 31 Ago 2019.

FIRST. **CSIRT Services Framework.** Version 2, jun. 2019. Disponível em: <https://www.first.org/education/csirt_services_framework_v2.0>. Acesso em: 28 Ago 2019.

KILLCRECE, Georgia. et al. **State of the Practice of Computer Security Incident Response Teams (CSIRTs)**. Carnegie Mellon University: Pittsburgh, 2003. Disponível em: <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=6571>. Acesso em: 12 Jul 2019.

KILLCRECE, Georgia. **Incident Management**. Carnegie Mellon University: Pittsburgh, 2005. Disponível em: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=295919>. Acesso em: 02 Ago 2019.

META CPAN. **Extensões do RT**. Set 2019. Disponível em <https://metacpan.org/search?q=RT::Extension>. Acesso em: 18 Set 2019.

MINICK, Brian. **Facing Cyber Threats Head On: Protecting Yourself and Your Business**. EUA: Rowman & Littlefield, 2017.

NIST. **Computer Security Incident Handling Guide:** Recommendations of the National Institute of Standards and Technology. Rev 2, p. 79, Ago 2012. Disponível em: <http://dx.doi.org/10.6028/NIST.SP.800-61r2>. Acesso em: 17 Set 2019.

SANTOS, Luiz Paulo Lopes dos. O comportamento humano. **O Comunicante**, [S.l.], v. 8, n. 1, p. 43-49, jan. 2018. ISSN 2594-3952. Disponível em: <http://ebrevistas.eb.mil.br/index.php/OC/article/view/1115>. Acesso em: 25 Jul 2019.

SOFTWARE ENGINEERING INSTITUTE. **CSIRT Services**. Carnegie Mellon University: Pittsburgh, 2002. 12 p. Disponível em: <https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf>. Acesso em: 14 Set 2019.