Sétima Conferência de Diretores de Tecnologia da Informação, TICAL 2017 Gestão de TIC para Pesquisa e Colaboração, San José, 3 a 5 de julho de 2017

Estabelecimento de CSIRTs e Processo de Tratamento de Incidentes de Segurança em Instituições Acadêmicas Brasileiras: estudo de caso da parceria CAIS/RNP e UFBA

Italo Valcy S. Brito[a], Yuri Alexandro[b]

[a] Universidade Federal da Bahia, Superintendência de TI
Avenida Adhemar de Barros, s/n, 40170-110, Ondina, Salvador-BA, Brasil
italovalcy@ufba.br

[b] Centro de Atendimento a Incidentes de Segurança, Rede Nacional de Ensino e Pesquisa
Av. Dr. André Tosello 209, 13083-886, Cidade Universitária, Campinas-SP, Brasil
yuri.ferreira@rnp.br

Resumo A rápida expansão da Internet em serviços oferecidos e dispositivos conectados traz consigo o aumento do número de incidentes de segurança da informação, tanto relacionados a pessoas individualmente, quanto a organizações. Em se tratando de instituições acadêmicas, onde o ambiente é naturalmente heterogêneo, considerando os diferentes perfis de acesso dos diferentes tipos de usuários, esse desafio se torna ainda maior. Aliado a isso, no Brasil existe a necessidade dessas instituições se adequarem a uma série de disposições normativas do Governo Federal, dentre elas a exigência de se ter um processo de tratamento de incidentes de segurança. Frente a isso, a RNP estruturou um projeto para apoiar o estabelecimento de CSIRTs nas organizações usuárias da rede brasileira de ensino e pesquisa, tendo a UFBA como uma das parceiras na sua aplicação. Este artigo apresenta as bases do projeto desenvolvido pela RNP, fundamentado em normas internacionais e nas melhores práticas de equipes ao redor do mundo, acerca da concepção de um CSIRT, as fases do processo de tratamento de incidentes, a metodologia de execução do projeto e os resultados obtidos pela UFBA na criação e operação do seu time de resposta a incidentes de segurança e no desenvolvimento do seu processo de tratamento de incidentes.

Palavras Chave: segurança da informação, incidentes, CSIRT, processo, tratamento de incidentes.

Eixo temático: Segurança da Informação.

1 Introdução

À medida que cada vez mais pessoas e dispositivos se conectam a Internet das mais diferentes formas, as ameaças à segurança dos dados de usuários e organizações aumentam, e lidar com os incidentes que comprometem as informações é uma tarefa ampla e complexa. Essa complexidade se torna ainda maior em uma rede heterogênea como a de ensino e pesquisa brasileira, onde, ao mesmo tempo, existem ambientes que necessitam de muita proteção – tais como informações pessoais de usuários, dados de pesquisas acadêmicas e industriais, direitos autorais e propriedade intelectual [1] – com ambientes que necessitam de acesso mais permissivo – como

projetos de inclusão digital e redes sem fio de livre acesso [2]. Tudo isso aliado a diferentes tipos de usuários – como funcionários, estudantes, professores, visitantes, pesquisadores, entre outros, cada um com suas necessidades peculiares – e uma gama de ameaças que surgem tanto interna, quanto externamente às organizações. A implantação de um processo de resposta a incidentes de segurança neste cenário não é algo simples e mostra-se como um grande desafio às instituições acadêmicas.

O trabalho dos CSIRTs, equipes responsáveis por atuar diretamente na detecção, mitigação e solução de incidentes de segurança da informação, é de fundamental importância para evitar e minimizar o impacto das ações maliciosas. Um CSIRT realiza o tratamento do incidente de segurança de maneira mais especializada, utilizando um conjunto de ferramentas de apoio, seguindo um processo e fluxos definidos, executando procedimentos específicos desde a ocorrência do incidente até após a sua resolução e fechamento [3]. Todas estas definições devem estar documentadas em um plano de gestão de incidentes, o qual guiará todas as atividades operacionais do tratamento do incidente.

Diante disto, este artigo tem por objetivo apresentar o processo de tratamento de incidentes realizado pelo ETIR UFBA, o CSIRT da Universidade Federal da Bahia, o qual foi desenvolvido com apoio do Centro de Atendimento a Resposta a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP), como resultado de um projeto voltado para as para as organizações usuárias da rede de ensino e pesquisa brasileira desenvolverem suas equipes de resposta a incidentes de segurança.

Este artigo está estruturado da seguinte maneira. Na Seção 2, é apresentado um embasamento teórico sobre o que é um CSIRT, seu objetivo e definições básicas, bem como uma fundamentação sobre o processo de gestão e tratamento de incidentes de segurança da informação. Na Seção 3, descreve-se o projeto do CAIS para apoio ao desenvolvimento de CSIRTs na rede de ensino e pesquisa brasileira. Já a Seção 4 aborda a estruturação do ETIR-UFBA e seu processo de gestão de incidentes. Por fim, a Seção 5 aponta as conclusões e trabalhos futuros.

2 Fundamentação e trabalhos relacionados

Um CSIRT (*Computer Security Information Response Team*) é uma equipe dedicada dentro de uma organização que tem por objetivo receber, analisar, resolver e responder incidentes de segurança da informação, além de desenvolver ações de prevenção e ser o ponto focal de contato sobre incidentes para toda a organização. O CSIRT deve atender a um escopo ou público específico, oferecendo um conjunto de serviços destinados aumentar a capacidade da segurança da informação da organização [4].

Para entender de forma mais clara o objetivo esperado de um CSIRT, é necessário que a organização defina o entendimento do que é um incidente de segurança. Tomando como base a definição do CERT/CC, um incidente de segurança é qualquer evento adverso, confirmado ou sobre suspeita, que possa comprometer as operações de sistemas de informação ou redes de computadores. Pode ser definido também como a violação, implícita ou explícita, de uma política de segurança da informação [5]. Exemplos de incidentes de segurança da informação são: tentativa, mal ou bem-

sucedida, de ganhar acesso não autorizado a sistemas ou dados; interrupção não planejada de serviços, alterações no funcionamento de um ativo, software ou serviço por terceiros sem autorização; propagação de códigos maliciosos por meio digital; divulgação de informações confidenciais, entre outros. Cada organização terá que definir o que deve ser considerado um incidente para a sua realidade, podendo ter abrangências e especificidades maiores ou menores.

Existem vários tipos de CSIRT, dentre os quais destacam-se para este artigo: i) os de coordenação – cujo objetivo é coordenar a ocorrência e a resposta a incidentes em um nível mais abrangente, enviando aos administradores de TIC as notificações de vulnerabilidade, atividades maliciosas e incidentes de segurança da informação relativas às suas redes e serviços, acompanhando o seu tratamento, enviando recomendações e conscientizando as organizações a ele ligadas, e ii) os internos ou corporativos – cuja função é atender direta e exclusivamente a organização que o mantém, atendendo aos seus usuários e ambiente de TIC, sendo o ponto focal de notificação e atendimento a incidentes de segurança da informação [6]. Entender o tipo de CSIRT é importante para definir corretamente as suas especificações básicas e a forma como a equipe tratará os incidentes de segurança.

2.1 Definições básicas de um CSIRT

O primeiro passo para o estabelecimento de um CSIRT é definir como ele será e como irá operar. Dentre elementos básicos que devem ser definidos para estabelecer uma equipe, estão:

Missão. Deve indicar claramente o objetivo do CSIRT, de forma breve, direta e inequívoca. Essa definição irá servir de base para todas as outras e como referência para os usuários dos serviços da equipe e outros parceiros. Geralmente são utilizados verbos de ação, representando o que a equipe deve fazer e cumprir.

Visão. Define o caminho que o CSIRT irá tomar ao longo de um período e como ele espera ser reconhecido pela organização. Ela orientará decisões estratégicas, o estabelecimento de metas a curto e médio prazo e a forma como a equipe pode contribuir à comunidade acadêmica. A visão é fortemente baseada nos valores organizacionais e na cultura de cada região, devendo se ter um entendimento claro das expectativas da organização para com a equipe.

Constituency. Determina o escopo da atuação do CSIRT, seja usuários, serviços, ou blocos de rede que a equipe irá atender. Deve ser definido, inclusive, se os diferentes tipos de serviço ou usuários irão receber diferentes níveis de atendimento. Por exemplo, um CSIRT pode atender todo o domínio administrativo da organização, ou somente uma parte da infraestrutura de serviços, dependerá da missão definida anteriormente. A correta identificação da *constituency* permite mapear as necessidades existentes, sendo, por isso, importante especificar exatamente a quem se destinarão os serviços executados pela equipe.

Serviços. Definem qual o conjunto de atividades que serão providos pelo CSIRT. Para cada serviço, é necessário criar os respectivos processos e procedimentos, determinar quando e por quem poderá ser requisitado e o SLA de atendimento. Geralmente, os serviços prestados por um CSIRT são divididos em três grupos principais: reativos, proativos e de qualidade.

- Serviços reativos são aqueles instanciados após a ocorrência de um incidente de segurança da informação. Visam solucionar o incidente em questão e investigar a sua causa. Dentre alguns serviços reativos, destacam-se: tratamento de incidentes (sendo este o principal e mandatório para todos os CSIRTs), análise forense, análise de artefatos, entre outros.
- Serviços proativos têm por objetivo prevenir a ocorrência de incidentes de segurança, desenvolvendo ações de proteção dos sistemas de modo a diminuir a probabilidade de efetivação de ataques ou de reduzir os impactos quando estes ocorrem. Exemplos de serviços proativos são: gerenciamento de vulnerabilidades, monitoramento de segurança da rede, entre outros.
- Serviços de qualidade têm por objetivo identificar limitações e implantar melhorias de ordem técnica e organizacional, acrescentando valor às iniciativas de segurança da informação. Exemplos: gestão de riscos de segurança da informação, gestão de conformidade, conscientização e disseminação da cultura em segurança da informação, entre outros.

Modelo Organizacional. Define a formatação da equipe e dedicação dos seus membros. Basicamente, existem quatro tipos principais:

- Equipe local, onde os membros são formados pela equipe de TIC existente da organização – podendo ou não ter especialistas em segurança da informação – cuja dedicação não é exclusiva, ou seja, os membros dividirão suas atividades cotidianas de TIC com a resolução de incidentes de segurança quando estes ocorrerem;
- Modelo centralizado, onde os membros fazem parte de uma equipe única, especializada, total e exclusivamente dedicada às atividades do CSIRT, realizando todo o trabalho de resposta a incidente e outros serviços oferecidos. Toda a equipe localiza-se em um mesmo local físico.
- Modelo distribuído, onde os membros também têm dedicação exclusiva às atividades do CSIRT e expertise em segurança da informação, atendem a todos os serviços, porém localizam-se de forma distribuída por diversos locais da organização, região ou país. As equipes remotas devem estar alinhadas a uma coordenação central, responsável por gerenciar as atividades, diretrizes e prioridades de ação.
- Modelo misto, que é uma combinação entre o modelo centralizado e o distribuído. Este modelo permite as equipes distribuídas tenham autonomia para gerenciar as suas atividades, cabendo a uma coordenação central a definição de tarefas no plano estratégico.

Existem aspectos impulsionadores ou dificultadores em todos os modelos, cabendo à organização definir aquele que mais se adequa às suas necessidades, de acordo com a missão definida e serviços oferecidos.

Estrutura Organizacional. Define o perfil e as respectivas atribuições das pessoas que farão parte da equipe, o organograma interno e a posição que o CSIRT terá dentro da estrutura da organização. O organograma interno permite um melhor desenho das áreas entre os serviços e uma melhor gestão das atividades de cada membro. O organograma externo, por sua vez, permite definir o nível hierárquico da equipe dentro da organização, a qual departamento interno ela estará vinculada e a quem ela

deverá se reportar. Por exemplo, quanto mais alto for o nível da equipe na hierarquia da organização, mais influência e autoridade ela terá para sugerir ou determinar ações de mitigação e combate a incidentes de segurança.

Autonomia. Define o nível de atuação, competências e obrigações da equipe perante a sua *constituency*. Isso envolve processos de decisão e ações de tratamento e recuperação de incidentes e eventos de segurança da informação, tanto de natureza reativa quanto preventiva. Basicamente existem três tipos de autonomia:

- Completa, onde as ações do CSIRT não necessitam de aprovação prévia de níveis hierárquicos superiores, devendo, entretanto, estar alinhada a diretrizes pré-estabelecidas e aprovadas pela organização;
- Compartilhada, onde o CSIRT é membro de um colegiado responsável pela tomada de decisões de ações a serem realizadas.
- Sem autonomia, onde um CSIRT não tem nenhuma autoridade sobre a infraestrutura da organização, cabendo a esta fornecer orientação, expertise e informações.

É importante que, independente da autonomia definida, o CSIRT faça parte do processo de tomadas de decisão acerca das ações de tratamento de incidentes na organização. Autonomia compartilhada permite múltiplas visões acerca do impacto do incidente. Por outro lado, autonomia completa permite maior rapidez e dinamicidade nas ações. CSIRTs de coordenação geralmente operam sem autonomia.

2.2 Processo de tratamento de incidentes

Como supracitado, o serviço de tratamento de incidentes é mandatório a todo CSIRT. Para executá-lo de forma adequada, a equipe deve ter documentado todo o processo fim-a-fim deste serviço, incluindo fluxo de ações e procedimentos necessários.

O tratamento de incidentes de segurança tem o objetivo de minimizar os impactos da ocorrência de um incidente e permitir o restabelecimento do ambiente afetado com rapidez [7]. Vários autores abordam as etapas de um processo de tratamento de incidentes. Por exemplo, Scarfone et al. [7] destaca quatro fases principais:

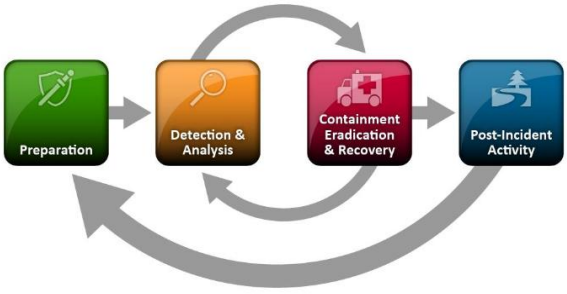


Fig. 1. Ciclo de vida do tratamento de incidentes de segurança proposto pelo NIST [7].

Esse fluxo pode se desdobrar em outras etapas mais específicas. Por exemplo, a ENISA [8] sugere um fluxo mais detalhado, conforme visto na Figura 2.

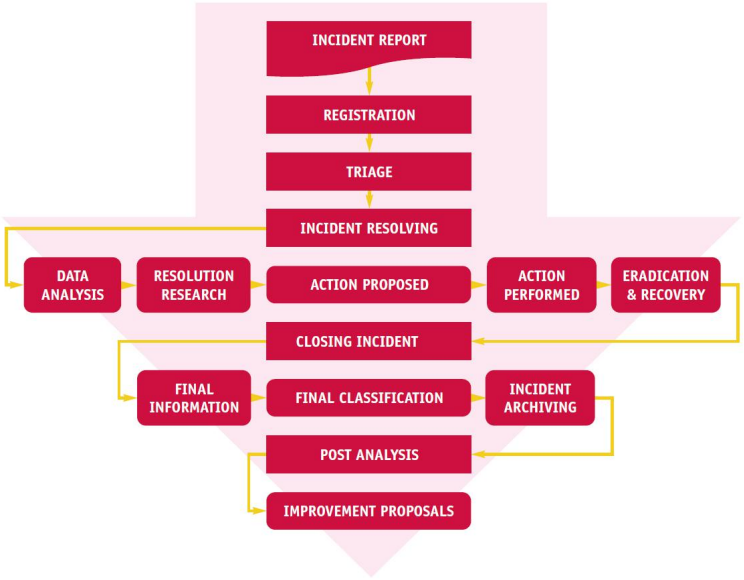


Fig. 2. Workflow de tratamento de incidentes proposto pela ENISA [8].

Para este trabalho, foi desenvolvido um modelo composto por um fluxo de oito fases principais, baseado nos dois modelos citados acima.

Preparação. Na preparação, são realizadas medidas que preparam a organização tanto para responder os incidentes, quanto para evitar novas ocorrências destes, garantindo que a infraestrutura de redes e sistemas estejam suficientemente seguros. Essas ações podem ser relativas a garantir mais segurança à infraestrutura, relativas a ter recursos necessários para realizar o tratamento de incidentes (tanto de hardware, quanto de softwares e sistemas), comunicações seguras, como também relativas à conscientização dos usuários para o uso seguro dos recursos computacionais.

Notificação e detecção. Nesta fase, o CSIRT deverá identificar a ocorrência de incidentes de segurança em seu ambiente, como origem ou destino, seja por meio de sistemas que permitam a identificação de atividades maliciosas (e.g. IDS, antivírus, SIEM, análise de logs de aplicações, etc.) ou também por notificações da *constituency*, de parceiros ou de outros CSIRTs. Algumas informações essenciais devem estar contidas na notificação, como origem e destino do incidente, sistemas e serviços afetados e informações de data e horário, com o *timezone*. Esses elementos são importantes para as fases posteriores do ciclo de tratamento do incidente.

Registro. Nesta fase, o incidente deve ser catalogado de modo a permitir sua identificação unívoca e a rastreabilidade durante o seu ciclo de vida, com o registro de todas as ações realizadas. Esta ação geralmente é executada com o auxílio de um sistema de gestão de incidentes (controle de tíquetes).

Triagem e análise. A triagem determina, dentre outras coisas, a validade do incidente de segurança notificado, ou seja, se faz parte da *constituency* atendida pelo CSIRT, se o conteúdo de fato se refere a um incidente de segurança e se as informações mínimas necessárias para a análise estão contidas. Caso a notificação não

se configure um incidente ou não tenha relação com a *constituency*, ela pode ser devolvida, reencaminhada ao respectivo responsável ou até mesmo descartada. Caso seja válida, a equipe deve identificar as características do incidente, os vetores de ataque utilizados e o quanto a estrutura de negócios da organização foi afetada. É uma boa prática criar uma base de dados com o histórico de incidentes anteriores, de modo a comparar informações, identificar semelhanças e assim realizar uma análise mais eficiente, sistemática e menos propensa a erros.

Classificação. A classificação é feita baseada nas informações oriundas da triagem e análise, determinando em qual taxonomia (grupos pré-definidos de tipos de incidentes) o incidente se encaixa. Alguns CSIRTs desenvolvem seus próprios critérios para definir a taxonomia, porém existem algumas recomendações bastante úteis e de fácil aplicação, como a tabela feita pela ENISA [8]. Outra classificação necessária é sobre a criticidade do incidente, que é usada na priorização do atendimento. Pode-se medir a criticidade através da análise dos impactos técnicos e organizacionais causados pelo ataque. Quanto mais crítico, mais rápido o incidente deve ser atendido, passando a ter mais prioridade frente aos demais.

Resolução. Nesta fase são realizadas as ações para contenção, mitigação e solução do incidente, bem como de recuperação do ambiente e retorno à normalidade. A contenção visa evitar que o incidente se propague e afete outros recursos da infraestrutura da organização. A mitigação deve envolver ações que eliminem a ocorrência do incidente em questão, identificando e eliminando as vulnerabilidades que foram exploradas. Na recuperação, a equipe deve restaurar o ambiente para o funcionamento normal e confirmar a sua correta operação, identificando e, quando necessário, corrigindo outras vulnerabilidades que possam levar a incidentes semelhantes.

Fechamento. Nesta fase é feito o encerramento do incidente, onde o notificante recebe da equipe uma resposta das ações realizadas durante o tratamento do incidente, e a confirmação de que o mesmo foi tratado. Essa resposta é importante, pois geram estatísticas sobre os incidentes para outras equipes ou CSIRTs de coordenação, que podem direcionar apoio quando necessário.

Pós-incidente. Esta etapa consiste em avaliar a execução do fluxo do processo de tratamento do incidente e verificar a eficácia das soluções adotadas. O resultado dessa etapa deve retroalimentar as ações da fase de preparação. As lições aprendidas devem levar a equipe a relacionar possíveis falhas ou insuficiência de recursos, implantar melhorias nas medidas de segurança e no próprio processo de tratamento de incidentes. As lições aprendidas também devem ser divulgadas a toda a equipe e, se preciso, feitas recomendações aos usuários ou usadas para promover ações de conscientização em segurança da informação na organização.

3 Projeto CSIRTs nas Organizações Usuárias da RNP

A RNP é uma organização que provê conectividade à Internet e serviços avançados de tecnologia da informação e comunicações a instituições de ensino e pesquisa no Brasil. Nesse contexto, o CAIS é departamento da RNP que zela pela segurança da rede acadêmica, tendo por missão atuar na detecção, resolução e prevenção de

incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes. Operando desde 1997 como o CSIRT de coordenação da rede acadêmica, vem ao longo dos anos desenvolvendo projetos e ações que visam aumentar a capacidade de segurança da informação nas organizações usuárias do backbone.

Em recentes pesquisas realizadas junto a estas organizações [9], o CAIS identificou que a grande maioria não tinha métodos, procedimentos ou equipes dedicadas ao processo de tratamento e resposta aos incidentes, mesmo aquelas que possuem uma área de segurança corporativa estruturada ou analistas de segurança da informação em suas equipes de TIC. Em contrapartida, foi possível identificar que as poucas organizações que tem CSIRT possuíam melhores índices de combate à atividade maliciosa e de resposta às notificações de incidentes a elas enviadas.

De forma complementar, o Governo Federal Brasileiro possui uma instrução normativa que disciplina a gestão da segurança da informação e comunicações nas instituições da administração pública federal brasileira [10], incluindo diversas normas complementares. Uma destas normas determina a criação de equipes de tratamento de incidentes de segurança [11], com aplicação obrigatória a todos os órgãos vinculados ao governo, incluindo universidades, institutos de pesquisa, hospitais universitários e outros conjuntos de instituições vinculadas à RNP e usuárias da rede de ensino e pesquisa.

Neste sentido, o CAIS desenvolveu um projeto visando fomentar o estabelecimento de equipes de resposta a incidentes de segurança da informação, através da elaboração de um modelo de definição de equipe, processos e procedimentos, de forma a ajudar os clientes da RNP a criarem suas próprias equipes e assim aumentar a sua capacidade de resposta a incidentes de segurança da informação. Este projeto consistiu em definir um modelo básico e genérico de CSIRT, aplicável no contexto da rede de ensino e pesquisa brasileira, materializado em um guia. Esse modelo foi aplicado em fase piloto em quatro instituições: Instituto Federal Farroupilha, Universidade Federal do Amazonas, Universidade Federal da Bahia e Universidade de Campinas.

Em um trabalho colaborativo com essas instituições, foram produzidos e validados *templates* de documentações necessárias para a formalização do CSIRT dentro de uma organização, um *template* de política de gestão de incidentes de segurança, contendo todos as fases do ciclo do tratamento de incidentes de segurança da informação, um *template* de política de comunicação, e, por fim, um *check-list* para acompanhamento de todas as fases de implantação e operação da equipe.

O guia foi desenvolvido para servir de referência às instituições no processo de estabelecimento das suas equipes, abordando desde a sua concepção, implantação e operação. Seguindo as disposições obrigatórias estabelecidas pelos organismos normativos [12] e baseado nas melhores práticas de atuação de outros CSIRTs no Brasil e no mundo, o guia contém um passo-a-passo explicativo de todas as fases, sugestões e ferramentas necessárias. Foi também levada em consideração particularidades e especificidades de cada tipo de instituição e região do país, não sendo, portanto, um modelo fechado e definitivo, e sim abrangente o suficiente para que cada organização tenha autonomia em aplica-lo da melhor forma possível, de acordo com o contexto que ela se encontra.

A metodologia utilizada foi baseada no método PDCA [13], fundamentada em um ciclo de atividades planejadas e recorrentes, sendo elas: planejamento, desenvolvimento, implantação e operação.

Planejamento. Determinou as bases estratégicas para o estabelecimento do CSIRT, identificando os principais *stakeholders* e tendo o claro entendimento do cenário, particularidades e necessidades da organização. Nesta fase, foi realizada também uma análise SWOT [14], cujo objetivo era avaliar os pontos fortes e fracos no ambiente interno da organização, oportunidades e ameaças no ambiente externo. Os resultados obtidos ao final da análise da matriz no processo de criação da equipe trouxeram aspectos positivos aproveitados como impulsionadores, como, por exemplo, a ciência da importância do desenvolvimento da equipe por parte da alta direção de algumas organizações, o aproveitamento de uma infraestrutura interna robusta, entre outras. Assim como também foi possível superar aspectos negativos que se configuraram como limitantes, como, por exemplo, as diferenças de conhecimento técnico em segurança entre alguns membros da equipe de TIC puderam ser mapeadas e trabalhadas em treinamentos específicos.

Desenvolvimento. Nesta fase, foram determinados os elementos básicos da equipe: missão, visão, *constituency*, serviços, modelo, estrutura organizacional e autonomia. Todas estas definições levaram em consideração os cenários e necessidades internas das organizações, utilizando também os resultados trazidos na análise SWOT.

Implantação. Consistiu na preparação do CSIRT para seu funcionamento, em 4 eixos principais: infraestrutura, formação dos membros da equipe, financiamento e documentação de políticas e procedimentos.

Em relação à infraestrutura, foram definidos e implementados os recursos de hardware, rede de dados, softwares e sistemas necessários para a operação do CSIRT, como o servidores e desktops, e-mail institucional da equipe, portal web, sistema de gestão de incidentes, incluindo todas as configurações de segurança, como a separação lógica da rede e proteção das VLANs, uso de chaves PGP, uso de SSL nos sistemas de comunicação, entre outras. Nesta fase também foram estabelecidos os perfis profissionais dos membros da equipe e os critérios para contratação, planos de desenvolvimento profissional da equipe, bem como os procedimentos que devem ser realizados em função do desligamento de um membro. No aspecto de financiamento, foram definidas as fontes de recursos financeiros utilizadas na manutenção das atividades da equipe. Por fim, foram definidos e elaboradas as políticas, normas e procedimentos técnicos necessários para a operação do CSIRT, dentre eles o plano de gestão de incidentes e o plano de comunicação.

Operação. A primeira ação da fase de operação consistiu na formalização do CSIRT dentro da organização, através da publicação de uma portaria que estabeleceu a equipe como responsável pelo tratamento de incidentes e outros serviços de segurança. A partir daí, foram desenvolvidas ações de divulgação da equipe para a sua *constituency*, reforçando a imagem de ponto focal para contato em casos de ocorrência de incidentes de segurança da informação.

Outra fase importante da operação é a análise crítica dos resultados do trabalho da equipe, através da avaliação das estatísticas de incidentes e dos indicadores de desempenho. As estatísticas são relativas ao quantitativo dos incidentes, e revelam o cenário de segurança da informação da organização. A partir dele, pode-se detectar índices relevantes de um determinado tipo de incidente e possíveis tendências. Uma

boa prática sugerida foi o desenvolvimento de relatórios periódicos com os números consolidados de incidentes, pois permite a realização de análises comparativas sobre os incidentes em períodos definidos, e assim investir em melhorias ou capacitação, se necessário. Já os indicadores de desempenho são importantes para avaliar a eficácia e eficiência do processo de gestão de incidentes. Ajudam a definir onde deve haver melhorias e necessidades de mais investimentos.

Por fim, a análise dos indicadores ajuda no processo de avaliação da operação da equipe, podendo indicar melhorias que devem ser feitas a fim de corrigir problemas, aprimorar processos e potencializar ações. Os resultados obtidos com a análise crítica devem conduzir novamente à etapa de planejamento, onde pode estas melhorias podem ser mapeadas e desenvolvidas ao longo das fases seguintes, seguindo então um fluxo cíclico de implementação.

O CAIS acompanhou e apoiou as instituições nos seus processos de estabelecimento e melhoria das equipes. Um dos *cases* relevantes foi a reestruturação do CSIRT da Universidade Federal da Bahia, o ETIR-UFBA, uma das equipes nas quais foi desenvolvido o projeto piloto.

4 Estudo de caso na UFBA

A UFBA vem adotando, ao longo dos anos, um conjunto de medidas para construir e manter um Processo Organizacional de Segurança da Informação e Comunicações (SIC). Esse processo inclui, dentre outras dimensões, o estabelecimento de equipe com foco específico em SIC e a melhoria contínua no plano de gestão de incidentes de segurança. Nesse sentido, o arcabouço proposto pelo CAIS no projeto de CSIRTs nas organizações usuárias trouxe oportunidades de revisão e aperfeiçoamento no Processo Organizacional de SIC da UFBA. Nesta seção, serão apresentados dois dos principais resultados do trabalho realizado em parceria com o CAIS na UFBA. Em especial, a subseção 4.1 apresenta os elementos básicos do ETIR-UFBA, ao passo que a subseção 4.2 discorre sobre o plano de gestão de incidentes de segurança da UFBA.

4.1 Elementos básicos do CSIRT ETIR-UFBA

Em conformidade com as normas específicas do Governo Federal, bibliotecas internacionais de gestão de TI e com as boas práticas apresentadas pelo CAIS, a UFBA iniciou uma revisão dos elementos básicos da sua equipe de segurança. Estes elementos refletem o escopo, os objetivos estratégicos e a forma de trabalho, de maneira ampla, da equipe de segurança. A listagem abaixo aponta alguns dos elementos aperfeiçoados:

Missão - A ETIR/UFBA é a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da UFBA, responsável pela prevenção, detecção e tratamento de incidentes de segurança, bem como pela criação e disseminação de práticas para uso seguro das Tecnologias de Informação e Comunicação.

Visão - Ser uma equipe de excelência que promove o fortalecimento da segurança da informação na UFBA, além de contribuir para construção de um ambiente cada

vez mais confiável, disponível e íntegro na Universidade, sendo referência no contexto local, regional e nacional.

Valores - Ética; Privacidade dos usuários; Cooperação e Colaboração; Compromisso e Comprometimento; Inovação e Pioneirismo; Agilidade; Transparência; Respeito.

Constituency - O público alvo do ETIR/UFBA são todos os usuários dos serviços de Tecnologia da Informação e Comunicação da UFBA, endereços IP e domínios da organização, e membros da comunidade acadêmica, tais como: servidores técnico-administrativo, docentes, pesquisadores, alunos, bolsistas, estagiários, prestadores de serviço e outras pessoas que mantiverem vínculo institucional com a Universidade.

Serviços – Os serviços do ETIR-UFBA são categorizados da seguinte maneira:

- **Reativos**: Tratamento de Incidentes de Segurança; Análise Forense; Envio de notificações de segurança; Ações corretivas e de mitigação.
- **Proativos**: Distribuição de Alertas, Recomendações e Estatísticas; Monitoramento e prevenção de atividade maliciosa; Gestão de Vulnerabilidades; Auditoria de Sistemas de Informação; Desenvolvimento de Ferramentas.
- **Qualidade**: Cooperação com outras equipes de segurança da informação; Gestão de riscos de segurança da informação; Disseminação da cultura de segurança da informação; Apoio na definição e escrita de normas e políticas de segurança da informação.

A revisão destes elementos permitiu um maior alinhamento entre a atuação da equipe de segurança e as metas de SIC da organização. Um dos elementos que reflete bem esse alinhamento após a revisão foi a missão da ETIR-UFBA, que originalmente em sua portaria de criação era dada pelo seguinte texto: "[...] terá a responsabilidade de receber, analisar e responder a notificações e atividades a incidentes de segurança em computadores". Embora a definição anterior estivesse em acordo com as referências legais do CSIRT, a revisão da missão buscou incorporar princípios preventivos e proativos para o tratamento de incidentes. Assim, a equipe, mesmo quando atua de forma reativa a um incidente de segurança, busca identificar oportunidades de melhoria para evitar novas ocorrências daquele incidente ou aprimorar sua identificação e tratamento.

Outro item favorecido pela revisão foi a lista de serviços oferecidos pela ETIR-UFBA. Durante a execução do projeto junto ao CAIS, a equipe da ETIR-UFBA relacionou o conjunto de serviços com base no que já era executado, mas também com uma visão de futuro do que a alta gestão demandava para a organização e do que a equipe percebia como necessidades ou oportunidades. Dessa maneira, surgiram propostas de serviços de gestão de vulnerabilidades, auditoria de sistemas, gestão de riscos, disseminação da cultura, dentre outros. Apesar de alguns destes serviços ainda não estarem com o modelo de operação bem definido, eles já são listados no plano de ações da ETIR-UFBA, com atividades pontuais sendo executadas.

4.2 Plano de Gestão de Incidentes de Segurança da UFBA

O plano de gestão de incidentes de segurança da informação visa garantir o tratamento e resposta eficazes aos eventos de segurança da informação que afetam os

princípios básicos da SIC (i.e. disponibilidade, integridade, confidencialidade e autenticidade) associados aos ativos e sistemas de informação e comunicações da organização. Além disso, o plano tem por objetivo definir funções e responsabilidades, documentar as ações e medidas necessárias para o tratamento de incidentes de forma rápida e eficiente, limitando seu impacto, e, assim, protegendo os ativos e as informações.

Antes do projeto de revisão da ETIR-UFBA, não existia formalmente um plano de gestão de incidentes, apenas fluxos de trabalho que eram executados pela equipe e que variavam ligeiramente em cada caso ou de acordo com o analista que o executava. A formalização do plano de gestão de incidentes buscou uniformizar o fluxo de trabalho, fundamentar o processo de tratamento em metodologias conhecidas e testadas e incorporar requisitos peculiares do contexto em que o CSIRT está inserido. A construção do plano tomou como base, portanto, as normas e legislações nacionais, guias produzidos por outros grupos de segurança e padrões internacionais para serviços de TIC, além das recomendações produzidas pelo CAIS/RNP.

4.2.1 Estrutura do Plano de Gestão de Incidentes de Segurança

O plano de gestão de incidentes de segurança da UFBA foi estruturado da seguinte maneira: 1) Objetivo; 2) Papéis e Responsabilidades; 3) Processo de gestão de incidentes de segurança; 4) Disposições finais.

Na seção "Papéis e Responsabilidades" foram abordadas as atribuições e escopo de cada um dos principais atores no processo de tratamento de incidentes de segurança da UFBA. Em particular, apresentou-se o papel do Gestor de SIC, da Equipe de Tratamento de Incidentes de Redes (ETIR), da Central de Serviços de TI, do Administrador de rede ou de sistema e do Responsável pelo ativo de informação. Associado aos papéis identificados é importante planejar estratégias de comunicação entre eles durante o processo de tratamento de incidentes, dando ciência a cada parte envolvida e solicitando ações ou informações inerentes.

Já na seção que descreve o processo de tratamento de incidentes, tomou-se como base o fluxo ilustrado na Figura 3. Cada etapa foi detalhada, esboçando o conjunto de entradas e saídas previstas e referenciando políticas ou procedimentos específicos.

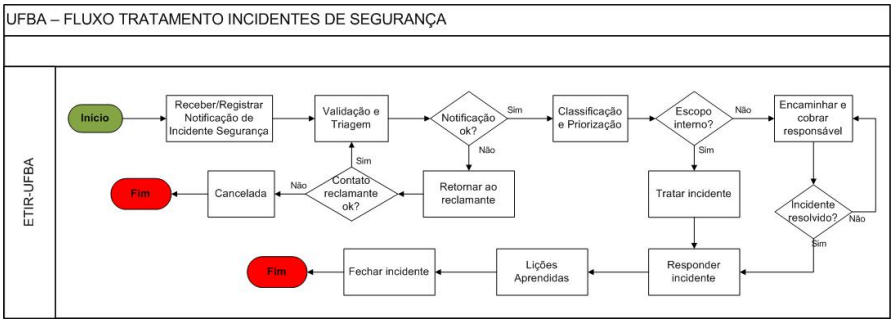
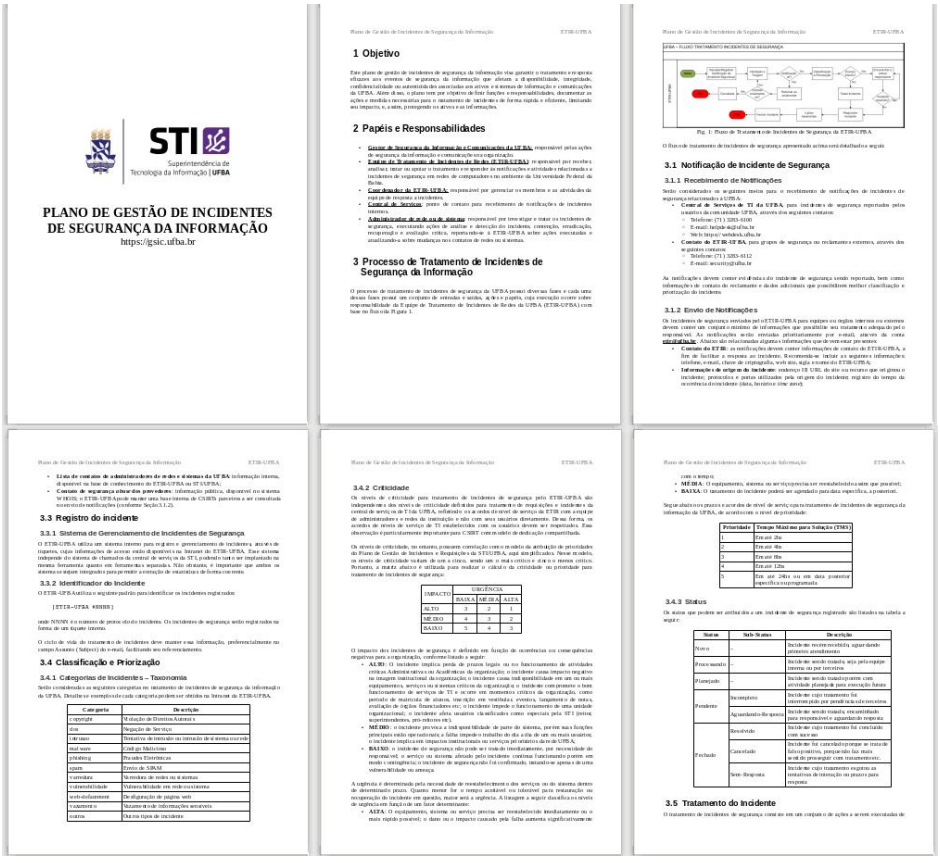


Fig. 3. Fluxo de Tratamento de Incidentes de Segurança da ETIR-UFBA.

Por exemplo, na etapa de recebimento ou envio de notificações de incidentes, foram mapeados os canais de comunicação internos e externos, em conformidade com padrões específicos [15], bem como, considerando o contexto em que a UFBA está inserida, contatos de outros grupos de segurança que precisam ser copiados em notificações de incidentes externos. Dentre eles, destacam-se: o CAIS, uma vez que a UFBA é instituição cliente da RNP; o CTIR.Gov, pois a UFBA é entidade da Administração Pública Federal; o CERT.br, que é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.

Na etapa de classificação e priorização, a título de exemplo complementar, foram definidas as categorias de incidente (taxonomia), a matriz de criticidade – tomando como base a urgência versus impacto – e a matriz de acordos de nível de serviço – que define o tempo máximo de solução para cada nível de prioridade mapeado.

A Figura 4 ilustra o plano de gestão de incidentes de segurança da UFBA produzido em parceria com o CAIS. O documento está disponível para compartilhamento com outras instituições interessadas.


PLANO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1 Objetivo

2 Papéis e Responsabilidades

3 Processo de Tratamento de Incidentes de Segurança da Informação

3.1 Notificação de Incidente de Segurança

3.3 Registro do incidente

3.4 Classificação e Priorização

3.5 Tratamento do Incidente

Fig. 4. Plano de Gestão de Incidentes de Segurança da UFBA (recorte)

4.2.2 Ciclo de tratamento de incidentes

Uma das etapas mais importantes do processo de gestão de incidentes é a execução das tarefas do ciclo de tratamento de incidentes para analisar, tratar e responder aos incidentes de segurança reportados a instituição.

As tarefas a serem executadas no ciclo de tratamento de um incidente variam de acordo com cada organização e com cada ativo de informação envolvido no incidente. Abaixo serão apresentadas as ações que compõem o ciclo de tratamento de incidentes da UFBA de forma geral, sendo necessária a definição de procedimentos específicos para cada serviço:

- **Preparação**: esta fase inicial envolve o treinamento de todos que estarão envolvidos com o tratamento de incidentes, aquisição ou configuração de ferramentas, além de verificação de procedimentos e acessos necessários. Algumas medidas são essenciais de serem adotadas nessa fase para o sucesso do tratamento do incidente nas fases seguintes, dentre elas: armazenamento seguro das trilhas de auditoria (logs) dos sistemas; atualização dos ativos de informação e contatos dos responsáveis (e.g. processo de inventário); revisão de topologias e arquitetura dos serviços da organização; dentre outras;
- **Detecção e Análise**: consiste em realizar a análise e detecção do incidente, determinando a sua natureza e extensão, além de prover detalhes dos sistemas comprometidos. Deve-se contemplar: sistemas e serviços afetados, impacto e risco, eventos correlatos e responsáveis. A correlação do incidente com eventos passados pode ajudar a identificar semelhanças e possíveis soluções. Nessa etapa, a equipe de segurança pode identificar as áreas da organização que atuarão em conjunto com a ETIR para contribuir com informações úteis durante o processo. Por fim, inicia-se a execução de um *Plano de Investigação de Incidentes de Segurança*;
- **Contenção**: nessa etapa o responsável pelo tratamento do evento deverá executar um *Plano de Contenção de Incidentes de Segurança*, limitando ou atenuando os danos causados;
- **Preservação de evidências**: antes de se iniciar as ações para restaurar o ambiente, é necessária a preservação de provas e evidências para a identificação correta da causa raiz do incidente e ações futuras;
- **Recuperação**: consiste em recuperar o sistema ou rede em questão, retornando ao seu estado normal de operação através de um *Plano de Recuperação de Incidentes de Segurança*. Deve-se restaurar a integridade do sistema e garantir sua disponibilidade. Em alguns casos, é possível partir para a etapa de Erradicação ou Mitigação sem necessidade de Recuperação, porém devem-se garantir as propriedades de integridade e disponibilidade mencionadas anteriormente;
- **Erradicação ou Mitigação**: nessa etapa o responsável pelo tratamento do evento deverá executar um *Plano de Correção, Mitigação ou Erradicação do incidente*, eliminando sua causa raiz. É importante remover a fragilidade de segurança utilizada para causar o incidente em questão. Idealmente todas as ameaças e riscos devem ser removidos do sistema ou da rede antes que seja reestabelecido online. É importante também validar as correções com as

áreas afetadas e verificar se os componentes afetados retornaram à situação de normalidade;

- **Documentação**: consiste em avaliar e documentar o incidente, apresentando evidências, caracterizando as vulnerabilidades exploradas, o ambiente comprometido, as ações de contenção e correção adotadas, dentre outros. É importante identificar características do incidente para treinar a equipe no tratamento de novos eventos e, quando cabível, levantar informações a serem usadas em processos legais. Deve-se produzir ao final do incidente um breve relatório sobre o seu tratamento, registrando-o junto à ETIR-UFBA;

Scarfone et al. [7] apresenta um *checklist* para direcionar os grupos de tratamento de incidentes na execução das tarefas acima descritas. Este *checklist* deve ser customizado com as peculiaridades de cada organização, eliminando itens que não condizem com o cenário em questão e acrescentando ou modificando outros. Em particular, a UFBA adaptou as ações específicas de cada tarefa de acordo com sua realidade, culminando no *checklist* descrito na Tabela 1.

Tabela 1. Checklist do ciclo de tratamento de incidentes de segurança.

	Ação	Status
	Preparação	
1.	Definir um plano de gestão de incidentes (ex: fluxos, processos, categorias e priorização)	
2.	Definir um plano de comunicação emergêncial (ex: contatos, criptografia, sala crise)	
3.	Ferramentas e equipamentos para tratamento do incidente (storage p/ evidências, software forense, laptops)	
3.1.	Definir área de armazenamento para evidências de incidentes	
3.2.	Elencar/Adquirir conjunto de ferramentas para análise forense e documentação de uso	
3.3.	Mapear equipamentos ou materiais necessários (ex: laptop, quadro branco, HD externo etc.)	
4.	Estabelecer recursos para análise de incidentes (KB, sistema de logs, inventário e topologias do ambiente)	
4.1.	Garantir coleta e armazenamento centralizado de logs de Firewall/NAT, Proxy, Autenticação	
4.2.	Implantar sistema de registro e acompanhamento de incidentes de segurança	
4.3.	Garantir a existência e atualização de inventário e topologias do ambiente	
4.4.	Implantar solução de Base de Conhecimento (KB) e registro de Lições Aprendidas	
5.	Estabelecer recursos de contenção do incidente	
6.	Estabelecer recursos de recuperação do incidente	
	Detecção e Análise	
7.	Confirmar a ocorrência do incidente	
7.1.	Analisar eventos reportados e indicativos	
7.2.	Realizar a correlação de informações	
7.3.	Pesquisar e levantar informações (ex: buscadores, KB)	
7.4.	Ao confirmar o incidente, iniciar documentação e coleta de evidências	
8.	Definir as prioridades no tratamento do incidente (ex: impacto funcional, abrangência, tendência de agravamento)	
9.	Reportar o incidente para equipe interna e grupos externos	
	Contenção, Erradicação e Recuperação	
10.	Coletar, preservar e documentar evidências	
11.	Conter o incidente	
12.	Erradicar o incidente	
12.1.	Identificar e mitigar as vulnerabilidades exploradas	
12.2.	Remover código malicioso e conteúdo impróprio ou ilegítmo	
12.3.	Caso identifique mais ativos afetados pelo incidente, repetir as ações de Detecção e Análise, seguindo para contenção e erradicação	
13.	Recuperar os ativos	
13.1.	Normalizar e retornar os sistemas afetados	
13.2.	Confirmar o correto funcionamento dos sistemas afetados	

4.2.3 Ferramentas desenvolvidas para apoio no tratamento de incidentes

Ao longo da operação do ETIR-UFBA, diversas ferramentas foram desenvolvidas para dar suporte às ações de tratamento de incidentes de segurança. Todas as ferramentas nasceram a partir de problemas específicos de uma rede acadêmica *multicampi*, com múltiplos perfis de usuários e recursos tecnológicos, como é a Rede UFBA. Essas particularidades deram espaço para o desenvolvimento de soluções modulares e configuráveis, a fim de que atendessem não apenas as necessidades da UFBA, mas também de outras organizações do mesmo setor, fomentando-se, assim, a colaboração e cooperação entre equipes de TIC. Nas subseções seguintes, algumas dessas ferramentas serão apresentadas.

4.2.3.1 TRAIRA – Tratamento de Incidentes de Redes Automatizado

O TRAIRA (Tratamento de Incidentes de Redes Automatizado) é uma ferramenta de apoio ao tratamento de incidentes de segurança que permite o registro e acompanhamento de notificações de incidente, automatizando as principais etapas do ciclo de tratamento de incidentes de segurança e fornecendo estatísticas e métricas para avaliação do desempenho e qualidade do processo [16].

Duas fases importantes do tratamento de incidentes podem ser facilmente automatizadas no TRAIRA: detecção e análise; contenção. A primeira etapa que o TRAIRA executa é o *Parser* das notificações recebidas, que consiste em identificar o tipo de incidente de acordo com o conteúdo do e-mail e extrair as informações relevantes para o seu tratamento. Na fase de detecção e análise, o TRAIRA consulta as bases de registro de trilhas de auditorias configuradas na fase de Preparação para fazer a correlação dos dados enviados na notificação com hosts internos na rede. Essa correlação em redes IPv4 geralmente depende dos registros de NAT (*Network Address Translation*) gerados pelo equipamento de Firewall. Assim, o TRAIRA realiza a busca em bases de registro necessárias e faz o mapeamento dos hosts contidos na notificação original com os hosts internos causadores do incidente.

Na fase de Contenção o TRAIRA emprega políticas de cessação da atividade maliciosa através do isolamento da máquina comprometida como, por exemplo, bloqueio no switch gerenciável ou roteador mais próximo.

Por fim, o TRAIRA pode ser usado para geração de estatísticas. A Figura 5 ilustra algumas destas estatísticas. Nessa figura é possível ter uma visão sobre a quantidade de incidentes recebidos e tratados, distribuição de incidentes por VLAN ou por grupo de responsabilidade e também uma visão de máquinas reincidentes.

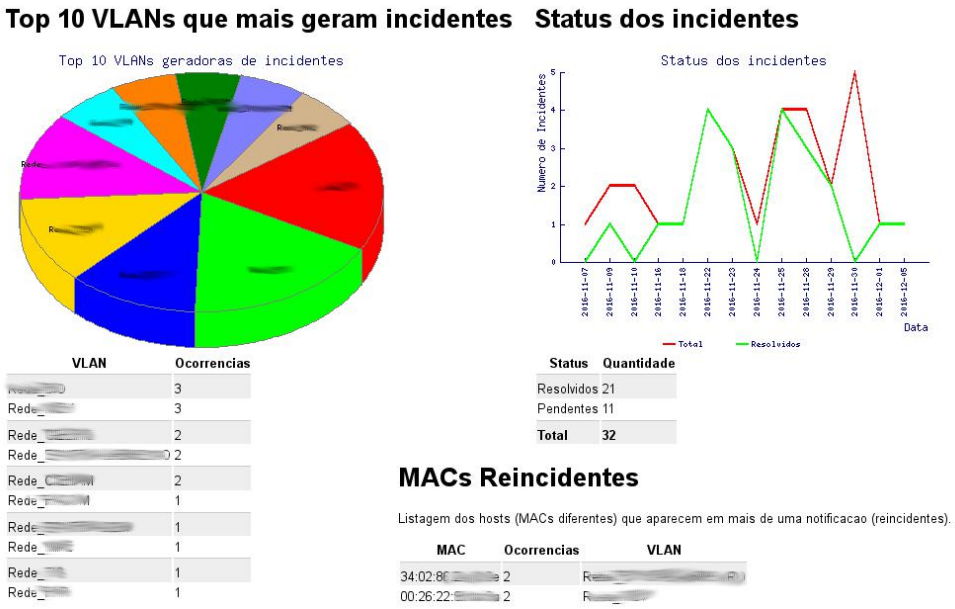


Fig. 5. Visão das estatísticas de incidentes no TRAIRA.

O TRAIRA pode ser obtido através do endereço https://certbahia.pop-ba.rnp.br/projects/traira/, onde também está disponível a documentação de instalação e uso.

4.2.3.2 L2M – Layer 2 Manager

Uma informação importante para o tratamento de incidentes de segurança é a associação entre endereços IP (v4 e v6) e hosts (máquinas). Mesmo em redes que utilizam configuração estática, o computador pode ser configurado para ter mais de um IP global e isso pode impactar na identificação dos hosts envolvidos em incidentes de segurança. Nas redes dinâmicas, baseadas em DHCP ou RA, outro desafio é manter o histórico de correção IP/host ao longo do tempo, visto que os incidentes de segurança podem ser relativos a momentos passados. Para tratar essa questão, a UFBA desenvolveu a aplicação L2M (Layer 2 Manager) cujo objetivo é coletar, armazenar e apresentar as informações de relacionamento IP/host ao longo do tempo.

Uma visão geral do funcionamento da ferramenta pode ser visto na Figura 6. Nessa figura é possível observar dois módulos do L2M: a consulta de MAC/IP e as estatísticas de quantidade de hosts por VLAN. Na primeira função (consulta de IP/MAC), o administrador pode visualizar qual o endereço MAC associado com determinado IP em determinado momento, ou vice-versa. A ferramenta disponibiliza também uma API REST, para integração com outras ferramentas, retornando um JSON com as informações consultadas. A segunda funcionalidade permite ter uma visão da capacidade da rede completa ou por VLAN ao longo do dia, mês e ano. A funcionalidade de contenção, embora não demonstrada na figura, é de fundamental

importância para o tratamento de incidentes, pois é possível consultar, bloquear ou liberar determinada máquina no ambiente de quarentena ou contenção da organização.

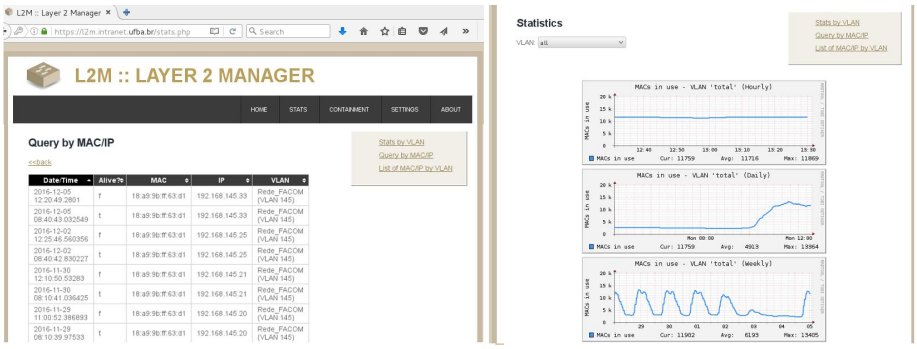


Fig. 6. Interface web do L2M: a) na esquerda, a consulta por IP ou MAC; b) na direita, estatísticas de quantidade de hosts por VLAN.

A coleta de dados do L2M é feita de duas formas: via script ou via SNMP. Embora a consulta via SNMP seja mais eficiente para obtenção dos dados, alguns fabricantes de equipamentos de rede não suportam apresentar as informações da tabela ARP ou *Neighbor Discovery* via SNMP. Para esses casos, é possível fazer a consulta via scripts com auxílio da biblioteca Expect. A ferramenta L2M já foi homologada com diversas soluções de rede, dentre elas: Cisco, Juniper, Extreme, Brocade, D-Link, Linux, Freebsd/PFSENSE.

A ferramenta L2M está publicamente disponível em https://certbahia.pop-ba.rnp.br/projects/l2m/.

4.2.3.3 Registro de eventos de NAT para IPTables/Netfilter e PFSENSE

Com o esgotamento de endereços IPv4, uma das abordagens amplamente utilizadas pelas organizações e provedores é o NAT (*Network Address Translation*). A técnica de NAT visa traduzir os endereços IP utilizados na rede interna em um endereço IP (ou faixa de endereços) utilizado na rede externa (Internet). No que tange ao tratamento de incidentes de segurança, a principal dificuldade adicionada pelo NAT consiste em determinar com precisão o endereço IP interno que foi traduzido no endereço IP externo, uma vez que as notificações de incidentes recebidas de fontes externas (e.g. outros CSIRTs) contêm apenas o endereço IP externo.

Para o tratamento de incidentes de segurança a seguinte tupla de informações é necessária: `<IP e porta de origem originais; IP e porta de origem traduzidos; IP e porta de destino; protocolo; data/hora de início; data/hora de fim>`. Muitas vezes, a informação de IP e porta de destino não são necessárias, sendo omitida em algumas soluções. Outras vezes, a data/hora de início e fim são calculadas a partir da data/hora de registro do evento nas trilhas de auditoria e da duração daquela tradução.

Algumas soluções de Firewall não possuem recursos nativos para fazer o registro em trilhas de auditoria das conexões NAT. Esse é o caso, por exemplo, de duas

soluções *opensource* amplamente utilizadas: IPTables/Netfilter e PFSENSE. Visando prover uma solução para essa lacuna, foram desenvolvidas duas ferramentas que mantém controle sobre o estado das traduções NAT e realiza o registro em trilhas de auditoria desses eventos:

- **NFCT-SNATLOG**: Ferramenta desenvolvida para o IPTables/Netfilter que registra-se na tabela de conexões do kernel Linux (network conntrack) e registra eventos de criação e finalização de tradução NAT. A partir desses eventos, são geradas as informações necessárias para tratamento de incidentes via *syslog*. A ferramenta está disponível em https://certbahia.pop-ba.rnp.br/projects/nfct-snatlog/;
- **PFNATTRACK**: de forma equivalente ao NFCT-SNATLOG, essa ferramenta monitora os estados de conexão do PF/Freebsd e gera registro de auditorias para conexões envolvidas na tradução de endereços IP. A saída gerada pode ser facilmente redirecionada para um host remoto via *syslog*, ou armazenada localmente. A ferramenta está disponível em https://certbahia.pop-ba.rnp.br/projects/pfnattrack/;

5 Conclusões e Trabalhos Futuros

O crescimento atual da Internet tem alavancado o número de incidentes de segurança da informação. Devido aos prejuízos causados por tais incidentes e sua dificuldade de prevenção, é necessário estabelecer políticas eficientes de tratamento e resposta a incidentes de segurança, bem como dispor de equipes dedicadas e preparadas para essa atividade. Este artigo apresentou um projeto proposto pelo CAIS/RNP para desenvolvimento de CSIRTs em organizações clientes da rede acadêmica brasileira, bem como um estudo de caso da aplicação dessa metodologia para aperfeiçoamento do processo institucional de segurança da informação na UFBA.

As recomendações de boas práticas, definições, modelos e ferramentas apresentadas podem servir de base para outras organizações implantarem ou aperfeiçoarem seus times de segurança e resposta a incidentes. O modelo apresentado é flexível o suficiente para ser customizado para cada organização, o que demonstra sua viabilidade de sua aplicação prática em ambientes complexos e heterogêneos, realidade comum nas instituições acadêmicas de ensino e pesquisa brasileiras.

Como trabalhos futuros espera-se: i) ampliar a quantidade de instituições participantes do projeto; ii) estruturar treinamentos para capacitação das equipes de TI em instituições que não possuem CSIRT; e iii) desenvolver novas ferramentas em colaboração com os CSIRTs para apoio no tratamento de incidentes de segurança.

Referencias

1. Politzer K.: Aspectos e fatores da produtividade em pesquisa, desenvolvimento e inovação. Quim. Nova, Vol. 28, Suplemento, S76-S78 (2005)

2. Cordeiro, SFN.: Tecnologias digitais móveis e cotidiano escolar: espaços/tempos de aprender. Tese de douturado em educação, Repositório Institucional da Universidade Federal da Bahia. (2014)
3. Brown MW., Stikvoort D., Kossakowski K., Killcrece G., Ruefle R., Zajicek M.: Handbook for Computer Security Incident Response Teams (CSIRTs). Software Engineering Institute, CMU/SI-2003-HB-002. (2003)
4. Alberts C., Dorofee A., Killcrece G., Ruefle R., Zajicek M.: Defining incident management process for CSIRTs: A work in progress. En: 10th IEEE International Symposium on High Performance Distributed Computing, pp. 181 a 184. IEEE Press, New York (2001)
5. CERT Coordination Center.: Computer security incident response team (CSIRT) frequently asked questions (FAQ). <http://cert.org/csirts/csirt_faq.html>. (2002)
6. Killcrece G., Kossakowski K., Ruefle R., Zajicek M.: State of the practice of computer security incident response teams (CSIRTs). Software Engineering Institute, CMU/SEI-2003-TR-001. (2003)
7. Scarfone K., Cichonski P., Millar T., Grance T.: Computer security incident handling guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61 Revision 2. (2012)
8. ENISA.: Good practice guide for incident management. European Network and Information Security Agency. (2010)
9. CAIS/RNP.: Pesquisa de Segurança da Rede Acadêmica Brasileira. Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa. <https://www.rnp.br/servicos/seguranca/educacao-e-conscientizacao-seguranca>. (2009, 2012)
10. DSIC/GSI/PR.: Instrução normativa GSI/PR nº 1. Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações, Presidência da República. <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. (2008)
11. DSIC/GSI/PR.: Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Norma complementar nº 05/IN01/DSIC/GSIPR. Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações, Presidência da República. <http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf>. (2009)
12. DSIC/GSI/PR.: Gestão de ETIR: Diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da administração pública federal. Norma complementar nº 08/IN01/DSIC/GSIPR. Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações, Presidência da República. <http://dsic.planalto.gov.br/documentos/nc_8_gestao_etir.pdf>. (2010)
13. Andrade, FFD.: O método de melhorias PDCA. Dissertação Mestrado em Engenharia Civil. Universidade de São Paulo. Escola politécnica. DOI 10.11606/D.3.2003.tde-04092003-150859. (2003)
14. Oliveira, DPR.: Planejamento estratégico - Conceitos, Metodologias e Práticas. 12A.ed. São Paulo: Atlas (2004)
15. Crocker, D.: "RFC 2142: Mailbox names for common services, roles and functions." Network Working Group, May. (1997)
16. Brito, IV.: “TRAIRA: uma ferramenta para o Tratamento de Incidentes de Rede Automatizado” In. XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg) - Brasília – DF. <https://www.pop-ba.rnp.br/files/papers/traira-sbseg2011.pdf>. (2011)