Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

RICARDO DAVID FERNANDES PINTO

A IMPLANTAÇÃO DE UMA EQUIPE DE RESPOSTA À INCIDENTES DE SEGURANÇA EM UMA INSTITUIÇÃO DE ENSINO

BRASÍLIA
2017

RICARDO DAVID FERNANDES PINTO

A IMPLANTAÇÃO DE UMA EQUIPE DE RESPOSTA À INCIDENTES DE SEGURANÇA EM UMA INSTITUIÇÃO DE ENSINO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. Gilberto Oliveira Netto

BRASÍLIA
2017

RICARDO DAVID FERNANDES PINTO

A IMPLANTAÇÃO DE UMA EQUIPE DE RESPOSTA A INCIDENTES DE SEGURANÇA EM UMA INSTITUIÇÃO DE ENSINO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. Gilberto Oliveira Netto

Brasília, 19 de setembro de 2017.

Banca Examinadora

_____

Prof. Dr. Marco Antônio

_____

Prof. Dr. Gilson Ciarallo

RESUMO

Desde a introdução dos recursos informatizados nas instituições de ensino, a área de tecnologia da informação tornou-se indispensável, dinâmica e componente fundamental nas atividades de ensino e pesquisa. Entretanto, problemas como os Incidentes de Segurança têm preocupado administradores de sistema que precisam estar preparados para responder a situações de emergência e criar mecanismos de defesa eficientes para proteger sua companhia dos ataques cibernéticos. Incidente de Segurança é descrito como qualquer ato de violação à política interna, lei ou ainda ações não aceitáveis quem envolvam computadores, redes e periféricos. Uma equipe de resposta à incidentes de segurança em computadores, também conhecida pelo acrônimo em inglês CSIRT – Computer Security Incident Response Team – é composta por um conjunto de especialistas de diversas áreas da tecnologia que trabalham com o objetivo de entender incidentes ocorridos e criar soluções e processos de reposta para evitar novos acontecimentos. O escopo deste trabalho é o estudo de caso da Faculdade Segura, uma instituição de ensino de pequeno porte, semelhante a diversas outras e com características peculiares a empresas deste ramo de negócio. O objetivo é analisar as características da instituição e desenvolver um plano de tratamento de incidentes para nortear o processo de implementação do CSIRT. Como resultado foram mapeadas as informações relevantes para o tratamento de incidentes de segurança na Faculdade Segura, com informações customizadas para a realidade da empresa. Concluímos que, apesar do vasto material disponível sobre o assunto, cada empresa pode adaptar as práticas desenvolvidas no mercado à sua realidade, adicionando ou retirando etapas durante o tratamento dos incidentes de segurança da informação.

Palavras-chave: Ameaça. Vulnerabilidade. Resposta. Incidente de Segurança Instituição de Ensino.

ABSTRACT

Since the introduction of computerized resources in educational institutions, an area of information technology has become indispensable, dynamic and fundamental component in teaching and research activities. However, problems like IT Security Incidents has worried systems admins that must be prepared for dealing with emergencies and creating efficient defense mechanisms to protect your company from cyber attacks. An incident is described as any violation of policy, law, or unacceptable act that involves information assets, such as computers, networks and peripherals. A computer security incident response team, also known by the acronym CSIRT, is a group of IT experts from different areas of technology who work to understand incidents and build solutions and processes to avoid new events. The scope of this work is the case study of the Faculdade Segura, a small educational institution, similar to other ones and with some characteristic peculiar to companies in this business area. The objective is analyze the characteristics of the institution and the development of an incident treatment plan for the CSIRT implementation process. As a result, they are mapped as relevant information for the treatment of security incidents in the Faculdade Segura, with information adapted to the reality of the company. We conclude that, despite the vast amount of material available on the subject, each company can adapt the market-based practices to its reality by adding or removing steps during the handling of information security incidents.

Key words: Threat. Vulnerability. Response. IT Incidents. Education Institution.

SUMÁRIO

INTRODUÇÃO

Nos últimos anos, empresas de diversos segmentos de negócio, têm investido continuamente na implementação e ampliação de redes locais de computadores, como requisito para suportar o crescente fluxo de informações, além de permitir acesso à rede mundial de computadores para funcionários e clientes. O desafio de manter a segurança da informação em estruturas computacionais interconectadas têm incentivado administradores de sistema a criar estruturas de monitoramento e tratamento de ameaças cibernéticas. Este trabalho tem sido intensificado em função do constante lançamento de produtos para a Internet e o desenvolvimento de ferramentas de ataque cada vez mais poderosas. (NC nº 05/IN01/DSIC/GSIPR, 2009, p. 2).

A exploração de problemas de segurança em redes de computadores não é um fenômeno novo. Há registros que descrevem incidentes ocorridos no passado que resultaram em grande prejuízo a sistemas informatizados. Por exemplo, em 1988, o “Morris Worm” foi um dos primeiros malwares distribuídos pela Internet a serem identificados. A ocorrência deste incidente resultou em recomendações de órgãos de regulamentação sobre como melhorar o tratamento de incidentes de segurança na Internet. Em resposta foram criados ao redor do mundo grupos de tratamento de incidentes de segurança, conhecidos com CSIRT (Computer Security Incident Response Team). O CSIRT pode ser facilmente comparado a uma equipe de brigadistas prediais, que realizam ações preventivas contra incêndio, mas que também estão sempre prontos para apagá-los em caso de emergência. (WEST-BROWN et al., 2003, p. 1)

Segundo Gondim (2011), citada por Moreira (2011, p. 54).

> Incidentes de segurança são ações danosas, de origem maliciosa ou não, envolvendo os agentes que manipulam informações, que são as pessoas e os computadores. O tratamento e a resposta a incidentes computacionais é o processo voltado à detecção, investigação, análise, contenção e recuperação de incidentes de segurança computacional

O tratamento correto de incidentes adversos ao funcionamento normal em rede de computadores tornou-se uma obrigação para os administradores de redes e sistema em razão da importância exercida por sistemas computacionais aos negócios das empresas. A violação ou o comprometimento de informações

corporativas pode acarretar danos severos às organizações atuais. (MOREIRA, 2011).

Segundo o CERT.BR (2017), o tratamento de incidentes é composto por: notificação do incidente, análise do incidente e resposta ao incidente.

> Receber notificações de incidentes habilita o CSIRT a servir como um ponto central de contato para notificação de problemas locais. A outra parte da análise de incidentes envolve analisar a fundo uma notificação de incidente ou uma atividade observada para determinar o escopo, prioridade e ameaça representada pelo incidente, bem como pesquisar acerca de possíveis estratégias de resposta e erradicação. A resposta a um incidente pode assumir formas variadas. Um CSIRT pode elaborar e divulgar recomendações para recuperação, contenção e prevenção, que são enviadas para os membros da comunidade por ele atendida e para os administradores de redes e sistemas que serão responsáveis por implementar os passos referentes à resposta ao incidente.

Em redes de campus, compostas por múltiplos segmentos de rede, distribuídas em prédios geograficamente distantes, o tratamento de incidentes de maneira centralizada é um constante desafio a ser vencido. A quantidade de usuários e computadores potencializa os efeitos devastadores de incidentes de segurança não tratados. Obstáculos como a falta de investimentos e a falta de procedimentos bem definidos agravam situações de risco, deixando a rede vulnerável a problemas relacionados aos pilares da segurança da informação (Disponibilidade, Integridade, Confidencialidade).

Este trabalho tem por objetivo mostrar o estudo de caso de uma implementação de uma equipe de resposta a incidentes em uma instituição de ensino, apresentando um plano para indicar ações durante o processo de tratamento de incidente.

São ainda objetivos secundários:

a) Descrever o processo de gerenciamento de incidente de segurança
b) Definir o ciclo de vida de um incidente
c) Descrever os conceitos relacionados ao CSIRT
d) Apresentar os principais tipos existentes
e) Detalhar os serviços ofertados por um CSIRT

Para alcançar os objetivos deste trabalho, a pesquisa documental foi fundamental, pois diversos artigos relacionados ao tema principal foram utilizados como base para o desenvolvimento do conteúdo. Além disso, a observação, bem como a vivência e experiência profissional do autor, contribuiu para o

enriquecimento do tema, pois foi possível relacionar a teoria contida nos documentos técnicos à prática aplicada à atual atividade laboral do autor.

O presente trabalho está, então, organizado em três capítulos.

No primeiro capítulo, apresenta-se os conceitos relacionados ao tratamento de incidentes de segurança, destacando-se as principais etapas relacionados ao processo e detalhes sobre o ciclo de vida de um incidente de segurança. O segundo capítulo proporciona uma análise sobre as equipes de resposta a incidentes de segurança, conceituando os principais tipos, serviços e informações acerca da composição de um CSIRT. No terceiro capitulo é apresentando como resultado um plano de tratamento de incidente de segurança, tomando como base a experiência profissional do autor para análise de um estudo de caso de uma instituição de ensino, composto por conceitos, diretrizes e orientações sobre o processo de tratamento de incidentes de segurança numa instituição fictícia.

1 GERENCIAMENTO DE INCIDENTES DE SEGURANÇA

As organizações atuais requerem um sistema de segurança baseado em múltiplas camadas para proteger e preservar seus sistemas e sua infraestrutura. Esta estratégia requer uma abordagem técnica e organizacional para o gerenciamento de incidentes de segurança como parte do controle de riscos para possibilitar o crescimento das companhias. As organizações não querem apenas sobreviver à ataques, elas querem resiliência. (RUEFLE; VAN WYK; TOSIC, 2013).

Há inúmeras formas de se defender contra riscos e ameaças provenientes do mundo cibernético, dentre elas:

- Identificar seus ativos principais, como localização, proprietário e criticidade;
- Realizar levantamento de riscos;
- Manter sistemas atualizados com os últimos pacotes disponíveis;
- Instalar perímetro de defesa, como roteadores, firewalls e sistemas de monitoramento de rede;
- Criar e manter atualizado procedimentos e políticas de segurança;
- Prover treinamento para empregados e parceiros sobre requisitos de segurança da instituição;
- Formalizar processos para gerenciamento de incidentes de segurança;

O gerenciamento de incidentes prove as capacidades para coordenação e resolução de eventos e incidentes de segurança da informação. Isto implica no gerenciamento do início ao fim, controlando e direcionando como os eventos e incidentes devem ser manipulados. Está envolvido a definição de processos; o suporte a políticas e procedimentos; atribuição de papéis e responsabilidades; ter equipamentos, infraestrutura, ferramentas e materiais de suporte; ter uma equipe treinada para executar o trabalho com consistência, alta qualidade, e de forma repetitiva. (RUEFLE; VAN WYK; TOSIC, 2013).

O gerenciamento de incidentes inclui o tratamento e a resposta à incidentes. O tratamento é um serviço que cobre todos os processos, tarefas e funções relacionadas à manipulação de eventos e incidentes, tais como:

- Detecção e reporte: Trata-se da habilidade de receber e revisar as informações de eventos, reporte de incidentes e alertas de segurança.
- Triagem: São as ações relacionadas à categorização, priorização e atribuição de eventos e incidentes.
- Análise: Inclui as tentativas para determinar o que aconteceu; qual o impacto, a ameaça ou o dano causado; quais passos para mitigação ou recuperação devem ser seguidos;
- Resposta: São as ações tomadas para resolver ou mitigar um incidente, com informação coordenada e disseminada, seguindo procedimentos para parar o incidente e impedir que aconteça novamente.

Reposta ao incidente, como notado acima, é o último passo no tratamento do incidente. É o processo engloba planejamento, coordenação e execução de ações e estratégias de mitigação e recuperação.

1.1 Processos de Gerenciamento de Incidente

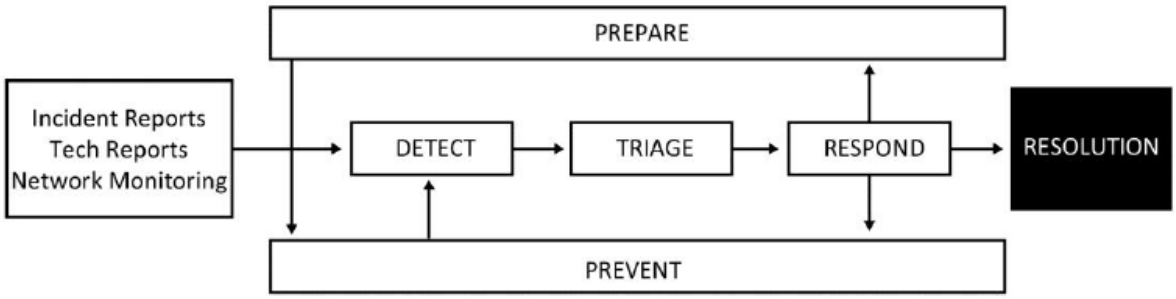
Não existe um processo obrigatório para o gerenciamento de incidentes de segurança. Há diversos guias como material de referência, que podem ser utilizados para adequação de processo interno, a ser definido pela companhia. Um destes guias englobam os 6 passos definidos pelo SANS Institute[1], que são: Preparação, Identificação, Contenção, Erradicação, Recuperação e Lições Aprendidas. Outro guia interessante, publicado pela Divisão CERT do SEI (Software Engineering Institute)[2] em 2004, define os processos macro em: Preparação, Proteção e Prevenção, Detecção, Triagem e Resposta. No decorrer deste estudo, faremos menção ao material divulgado pelo CERT.

[1] SANS Institute é uma empresa norte-americana especializada em segurança da informação e cyber segurança.
[2] A Divisão CERT é uma parte do SEI (Software Engineering Institute) dedicada ao campo de cyber segurança e é reconhecida como confiável e trabalha de forma dedicada à melhoria da segurança e da resiliência de computadores e sistemas.

A intenção do mapeamento dos processos é facilitar o entendimento das empresas sobre as atividades relacionadas ao tratamento de incidentes de segurança. Desta forma, será possível determinar o fluxo de trabalho, suas capacidades e também suas fraquezas.

Abaixo, na Figura 1, um exemplo de fluxo de trabalho para o gerenciamento de incidentes de segurança.

Figura 1 – Fluxo de Trabalho em alto-nível para gerenciamento de incidente



Fonte: New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)

1.1.1 Preparação

A preparação é a fase inicial para a implementação de um programa de resposta a incidente de segurança. Os requisitos gerais para esta etapa consistem na definição de papeis e responsabilidades dentro do processo de gerenciamento além de definir os responsáveis pela construção da infraestrutura de suporte ao programa. As seguintes atividades são realizadas nesta fase:

- Definição de políticas de segurança, procedimentos, categorias e listas de severidade;
- Definição dos componentes do grupo de resposta (CSIRT);
- Identificação dos papeis principais dentro da companhia;
- Implementação da infraestrutura de suporte (sistema de registros, ferramentas de análise, canais de comunicação)

1.1.2 Proteção e Prevenção

A proteção e a prevenção são as etapas que envolvem as ações para conter os incidentes, realizando mudanças na infraestrutura após a detecção e durante a resposta, incluindo atividades de filtragem, bloqueio e erradicação. Este processo envolve também a implementação de mudanças baseadas em incidentes anteriores, reportes técnicos ou na experiência dos analistas. Neste processo estão incluídas as atividades:

- Inventário de auditoria e varredura de vulnerabilidades
- Implementação de recomendações da indústria e melhoras práticas definidas pelos fabricantes
- Atualização das proteções de segurança nos equipamentos e softwares instalados nos perímetros externos e internos (IDS/IPS, Firewall, Antivírus, etc.)
- Definição de processos de controle de mudança nos ativos da rede

1.1.3 Detecção

A fase de detecção envolve o processo de identificação de atividades incomuns na rede, por elementos internos ou externos, que podem comprometer a disponibilidade, a integridade ou a confidencialidade das informações ou sistemas da organização. Por este motivo, é importante que cada empresa conheça sua infraestrutura e que saiba identificar uma potencial ameaça. Um evento de detecção pode ser proativo ou reativo:

- Proativo: Quando há envio de informação que pode sugerir potencial atividade maliciosa ou uma vulnerabilidade, como alertas de vulnerabilidade ou alertas de segurança de um IDS/IPS, por exemplo.
- Reativo: Quando é reportado algum comportamento incomum, interno ou externo, como a interrupção de sistemas ou alertas enviados por um especialista em segurança.

É essencial que todas as informações relacionadas ao incidente sejam gravadas e documentadas para futura investigação sobre uma atividade danosa.

1.1.4 Triagem

O processo de triagem é importantíssimo para o gerenciamento do incidente. Esta etapa é crucial pois reúne em um único ponto de contato ações para:

- Categorizar
- Priorizar
- Atribuir
- Correlacionar com outros eventos

Na triagem é coletada toda a informação disponível para determinar o escopo de um incidente, seu impacto e quais ativos estão sendo afetados. Após esta etapa, os dados são enviados para o processo de resposta.

1.1.5 Resposta

O processo de resposta envolve todas as ações necessárias para sanar ou mitigar um incidente, analisando, coordenando e distribuindo as informações. O processo de resposta implica mais do que responder tecnicamente; respostas legais ou gerenciais podem também ser requeridas em conjunto com a resposta técnica.

- Resposta técnica: contém o parecer técnico do ocorrido, com os eventos coletados, plano de resposta, ações coordenadas externa e internamente, estratégias de mitigação, reparação ou recuperação de qualquer sistema afetado, até que o caso seja encerrado;
- Resposta gerencial: contém as atividades como notificações, interações organizacionais, escalação, aprovação e etc.
- Resposta legal: contém ações associadas à interpretação legal do ocorrido, analisando regulamentos e legislações, como as que envolvem a privacidade, direito autoral, etc.

As respostas podem ocorrer simultaneamente e precisam ser coordenadas e comunicadas para ter o efeito esperado. Este processo pode incluir a participação de parceiros e outras equipes da organização.

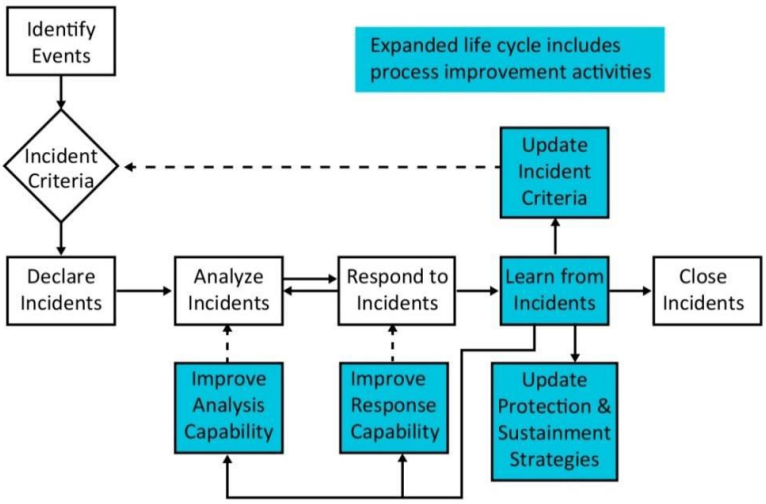
1.2 Ciclo de Vida do Incidente

Durante o tratamento de eventos incidentes, é muito importante que se saiba em que fase estão as tratativas para solucionar o incidente de segurança. Para tanto, é preciso definir quais fases são necessárias e qual o propósito de cada uma delas. Algumas organizações seguem modelos de referência, como o ITIL (IT Infrastructure Library) e ajustam os processos de acordo com sua necessidade. Não há uma forma fácil de registrar estas etapas. Uma das formas é utilizar os horários entre as trocas de e-mail, ou seja, quando o incidente foi reportado, quando foi respondido, quando foi concluído. Uma outra alternativa é utilizar um sistema de tíquete, que pode ajudar bastante o processo desde de o primeiro reporte do incidente, até sua conclusão (ENISA - Good Practice Guide for Incident Management, 2010).

O clico de vida deve ser usado para prover um controle profundo sobre a inter-relação entre os processos de detecção, análise (triagem) e resposta. O ciclo de vida é circular; as lições aprendidas através dos processos podem ser usadas para aumentar a prática em defender futuros ataques.

A figura 2, abaixo, exibe o fluxo de reporte de incidente recebido via monitoração, que checa critérios previamente estabelecidos. Caso o reporte atenda aos critérios definidos, um incidente de segurança é declarado e acionará ações de análise e remediação. Lições aprendidas são documentadas no tratamento do incidente e são compartilhadas para equalizar o conhecimento para membros da equipe.

Figura 2 – Ciclo de vida no tratamento de incidentes



Fonte: New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)

O próximo capítulo aborda uma revisão da literatura, os principais conceitos relacionados à um CSIRT, os tipos existentes e os principais serviços oferecidos à sua instituição, conteúdo este que compõe o referencial teórico que embasa este trabalho.

2 O QUE É UM CSIRT

A sigla CSIRT é o acrônimo para Computer Security Incident Reponse Team (Equipe de Resposta a Incidente de Segurança). Existem várias abreviaturas para o mesmo tipo de equipe:

- CERT ou CERT/CC (Computer Emergency Response Team / Coordination Center – Equipe de Resposta a Emergências Informáticas / Centro de Coordenação)
- CSIRT (Computer Security Incident Response Team - Equipe de Resposta a Incidentes de Segurança Informática)
- IRT (Incident Response Team – Equipe de Resposta a Incidentes)
- CIRT (Computer Incident Response Team – Equipa de Resposta a Incidentes Informáticos)
- SERT (Security Emergency Response Team – Equipa de Resposta a Emergências de Segurança)

Um CSIRT é uma equipe de analistas e peritos de segurança da informação que tem como principal atividade responder à incidentes de segurança. Presta os serviços necessários para ajudar suas organizações a prevenir e remediar violações de segurança. A fim de atenuar os riscos e minimizar o número de respostas necessárias, a maioria dos CSIRTs também prestam serviços preventivos e pedagógicos à suas companhias. Emite avisos sobre as vulnerabilidades de softwares e hardwares em uso e informa usuários sobre ameaças descobertas recentemente e que podem impactar os trabalhos da instituição (ENISA, 2006).

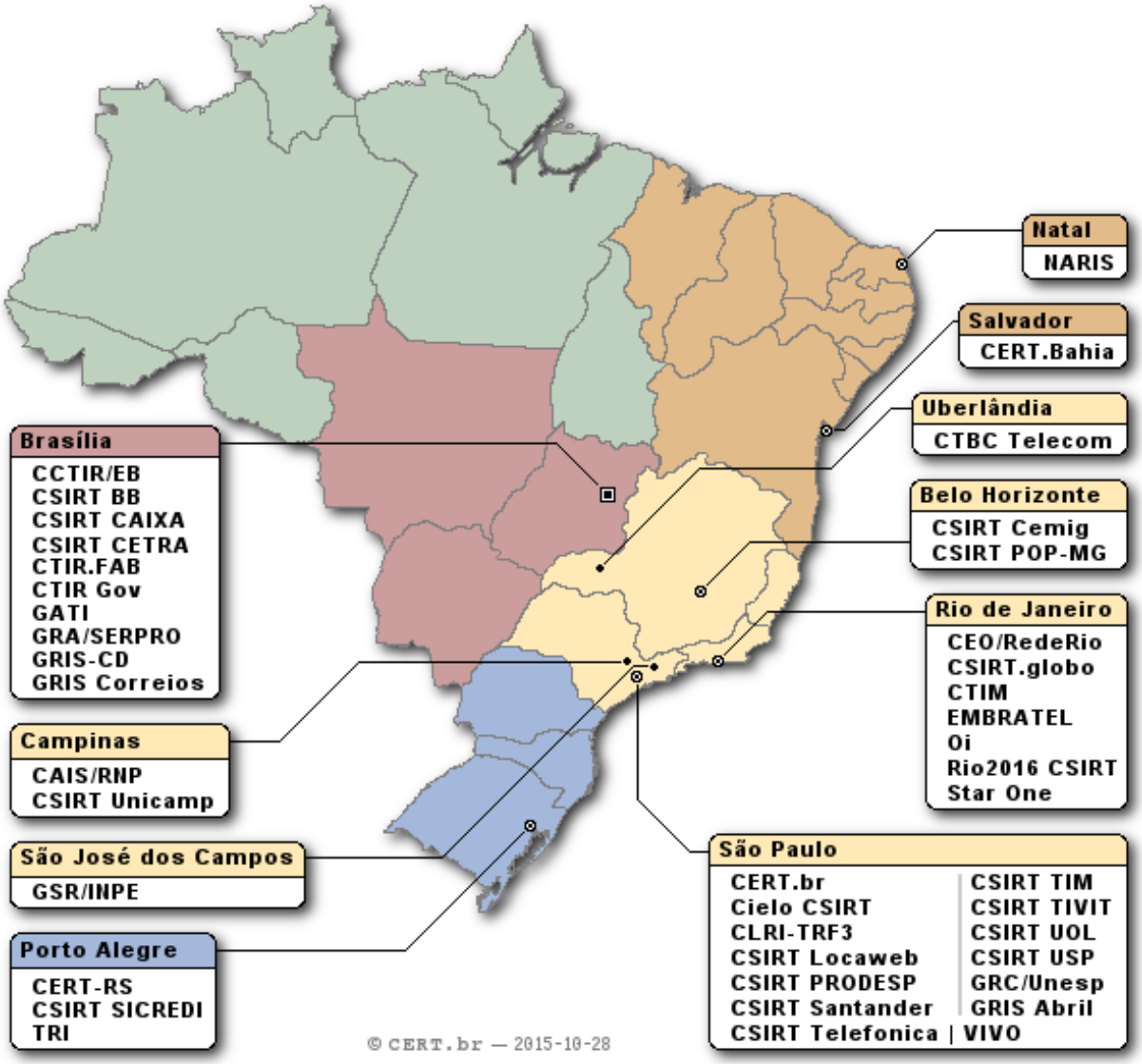
2.1 Missão

A missão do CSIRT pode variar de acordo com o setor onde este está inserido. Por exemplo, um CSIRT da polícia pode trabalhar focado em coletar evidências de crimes cibernéticos, coletando e analisando dados dos sistemas afetados ou envolvidos num incidente. Um CSIRT governamental, por outro lado, pode estar envolvido em ações de conscientização e treinamento dos aspectos relacionados à segurança da informação, mas nunca realizar atividades forenses ou investigativas. (RUEFLE; VAN WYK; TOSIC, 2013).

Independentemente de qualquer função especial, a atividade principal de um CSIRT é o tratamento de incidentes.

Na figura 3 abaixo mostra as cidades onde estão sediados os principais CSIRTs do Brasil.

Figura 3 – Mapa dos CSIRTs Brasileiros



Fonte: CERT.BR

2.2 Tipos

Durante as ações para implementação de um CSIRT é importante que se entenda qual o setor da organização que pretender instalar o CSIRT, quais tipos de clientes serão atendidos e quais serviços serão desenvolvidos. Abaixo está listado os principais tipos de CSIRT observados atualmente:

- CSIRT do Setor Acadêmico: Presta serviços para instituições de ensino, como faculdades, universidades e centros de pesquisa. Os clientes mais comuns são colaboradores e estudantes das instituições.
- CSIRT Comercial: Presta serviços de forma comercial a seus clientes e usuários. Por exemplo: um fornecedor de links de internet, que pode oferecer serviços de segurança como um serviço opcional. Os clientes normalmente pagam taxas extras por este tipo de serviço.
- CSIRT do Setor Governamental: Presta serviços para agências ou órgãos do Governo de um País. Seus clientes são geralmente os próprios cidadãos ou ainda funcionários dos órgãos do Governo onde o CSIRT atua.
- CSIRT Interno: Presta serviço apenas à companhia onde está instalado, sendo mais uma função do que um setor, propriamente dito. Instituições como Bancos ou Empresas de telefonia possuem suas próprias equipes internas.
- CSIRT Militar: Presta serviço a organizações militares responsáveis pela infraestrutura informatizada das forças de defesa nacional. Os clientes são usuários destas organizações ou empresas intimamente ligadas a estas instituições.
- CSIRT Nacional: Trata-se de uma equipe de nível nacional e é considerada um ponto de contato de segurança no País. Este tipo de CSIRT não tem clientes diretos uma vez que desempenha apenas um papel intermediário para equipes de todo um país. (ENISA, 2006).

2.3 Serviços

Um dos primeiros problemas a serem endereçados durante a criação de um CSIRT é a tomada de decisão de quais serviços o CSIRT irá prover à sua

organização. Este processo envolve nomear e definir cada serviço provido, o que nem sempre é uma tarefa fácil de fazer.

A equipe precisa tomar muito cuidado ao descrever quais serviços irá oferecer a seus clientes. A lista destes serviços irá determinar quais recursos, conhecimentos técnicos e parcerias o time irá precisar para exercer suas funções com propriedade. A seleção dos serviços deverá, primeiramente e a acima de tudo, estar ajustada com as necessidades do negócio onde está inserida. Além disso, a definição dos serviços precisar ser realística e honesta quanto ao tamanho da equipe e o nível de conhecimento dos profissionais. É preferível oferecer poucos serviços, mas bem executados, do que um grande número de atividades, executadas pobremente. A partir do momento em que o CSIRT ganha confiança e respeito de seus clientes, este ganha espaço para ampliar seu escopo de atuação (STELVIO, 2002).

2.3.1 Categorias

Há diversos serviços que um CSIRT pode oferecer. Cada CSIRT é diferente e provê serviços baseados na sua missão e nos clientes atendidos pela equipe.

Os serviços de um CSIRT podem ser agrupados em três categorias:

- **Serviços reativos:** Estes serviços são acionados por um evento ou requisição, como um reporte de um computador comprometido com vírus; relatórios de análise de vulnerabilidades; ou algo identificado por uma ferramenta de IDS/IPS ou sistema de análise de log. Serviços reativos são o núcleo de uma equipe de resposta a incidentes de segurança.
- **Serviços proativos:** Estes serviços proveem assistência e informações necessárias para ajudar a preparar, proteger e manter seguro os sistemas e computadores da sua organização, se antecipando à ataques, problemas ou eventos. A performance destes serviços está diretamente ligada ao número de incidentes reportados no futuro.
- **Serviços de gerenciamento de qualidade da segurança:** Estes serviços ampliam a existência de outros serviços de gerenciamento bem estabelecidos dentro da organização, que são tradicionalmente executados por outras

áreas, como o setor de auditoria ou departamento de controles internos. A participação do CSIRT pode auxiliar a geração de relatórios sob outro ponto de vista e pode contribuir para melhorar o nível de segurança dentro da instituição, diminuindo a exposição a riscos e evitando ameaças desnecessárias. Estes serviços são geralmente proativos e podem contribuir indiretamente para redução do número de incidentes.

Abaixo o quadro 1 com os principais serviços, divididos por categoria.

Quadro 1 – Principais serviços de um CSIRT

Serviços reativos	**Serviços proativos**	**Serviços de gerenciamento de qualidade da segurança**
Alertas e informativos Tratamento de incidentes Análise de incidente Resposta a análise incidente Tratamento de vulnerabilidades Análise de vulnerabilidades Reposta à análise de vulnerabilidades Tratamento de artefatos Análise de artefatos Resposta à análise de artefatos	Comunicados Estudos de novas tecnologias Inventário e auditorias de segurança Configuração e manutenção de ferramentas de segurança, aplicações ou infraestruturas Desenvolvimento de ferramentas de segurança Sistemas de detecção de intrusão Disseminação de informação relacionada à segurança	Análise de risco Plano de continuidade de negócios Plano de recuperação Consultoria de segurança Conscientização interna Educação / Treinamento Certificação ou avaliação de produtos

Fonte: New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)

2.3.2 Descrição dos serviços

- **Serviços reativos – alertas e informativos:** Este serviço envolve a disseminação de informação que descreve um ataque de intrusão; uma vulnerabilidade de segurança; um alerta de intrusão; um vírus de computador; provendo recomendações rápidas sobre ações de mitigação e resolução dos problemas. O alerta ou informativo é enviado como reação à um problema em andamento, para notificar os usuários sobre a atividade e promover direcionamento para proteger seus computadores ou recuperar os sistemas já afetados. Esta informação pode ser criada pelo CSIRT ou distribuída por outros parceiros, como empresas ou especialistas em segurança ou até outras áreas membros da organização.

- **Serviços reativos – tratamento de incidentes:** O tratamento de incidente envolve as ações para recebimento, triagem, análise e resposta às requisições e reportes de eventos e incidentes. As respostas deste processo podem incluir:
  - Execução de ações para proteger sistemas e segmentos de rede, afetados ou ameaçados por atividade de intrusão
  - Promoção de soluções e estratégias de mitigação provenientes de recomendações de segurança ou alertas do mercado
  - Observação de atividades de intrusão em outras partes da rede
  - Implementação de filtros no tráfego de rede
  - Atualização ou reparação de sistemas
  - Desenvolvimento de outras respostas ou estratégias de contorno
- **Serviços reativos – tratamento de vulnerabilidades:** O tratamento de vulnerabilidades envolve o recebimento de informações e reportes sobre vulnerabilidades em hardware e software, analisando a natureza, os mecanismos e os efeitos destas vulnerabilidades; e desenvolvendo estratégias de resposta para detectar e reparar estas vulnerabilidades.
- **Serviços reativos – tratamento de artefatos:** Um artefato é um arquivo ou objeto encontrado em um sistema que pode ter sido envolvido em atividade maliciosa ou ataque a sistemas informatizados. Os artefatos podem incluir, mas não se limitar, a vírus de computador ou qualquer outro tipo de malware conhecido. A análise de artefato envolve o recebimento de informação sobre o incidente relacionado além de cópias do objeto suspeito. Uma vez recebido, o artefato é submetido à analises quanto a sua natureza, mecanismos, versão, uso e técnicas de desenvolvimento descobertas (ou sugeridas) para viabilizar estratégias de resposta, defesa e remoção.
- **Serviços proativos – comunicados:** Esta ação envolve o envio de avisos, alertas e recomendações para clientes e parceiros sobre novas implementações de médio e alto impacto, assim que descobertas por análises de vulnerabilidade ou ferramentas de intrusão. Esta ação permite que clientes se protejam de vulnerabilidades encontrados internamente antes delas serem de fato exploradas.

- **Serviços proativos – estudos de novas tecnologias:** O CSIRT deve monitorar e observar novas implementações tecnológicas, que envolvam atividades de intrusão, ou que estejam relacionadas à uma futura ameaça. Este serviço envolve a leitura frequente de boletins de segurança, sites de segurança web e notícias relacionadas à segurança da informação.
- **Serviços proativos – inventário e auditorias de segurança:** Este serviço prevê uma revisão detalhada sobre a infraestrutura de segurança da instituição, baseada em requerimentos definidos pela própria organização, ou por padrões de indústria aplicáveis a realidade da empresa. Isto pode abranger uma revisão constante de práticas de segurança interna.
- **Serviços proativos – Configuração e manutenção de ferramentas de segurança, aplicações ou infraestruturas:** Este serviço identifica e provê direcionamento apropriado de como configurar e manter ferramentas, aplicações, e a infraestrutura usada pelo CSIRT para responder a seus clientes e ao próprio CSIRT. Através deste serviço, podem ser realizadas configurações das políticas de software, manutenções e atualizações necessárias em componentes como, IDS/IPS, Antivírus, AntiSpam, Firewalls e mecanismos de autenticação. O CSIRT pode inclusive prover estes serviços como parte de seus serviços principais. Além disso, pode estar incluso a configuração de sistemas de segurança em servidores, desktops e laptops.
- **Serviços proativos – Desenvolvimento de ferramentas de segurança:** Neste serviço está incluso o desenvolvimento de qualquer solução de segurança especifica para a organização, como por exemplo patchs de correção customizados para implementação interna, usados em casos de recuperação de hosts vulneráveis. Além disso, scripts que estendem funcionalidades de ferramentas de segurança já existentes, como um novo plug-in para o scanner de rede, ou ainda scripts para facilitar o uso de tecnologia de criptografia.
- **Serviços proativos – Sistemas de detecção de intrusão:** O CSIRT deve realizar revisão constante dos logs de IDS/IPS para iniciar resposta sempre que um evento atingir um valor definido. A análise de logs de detecção pode ser uma tarefa desanimadora, mas é importante para determinar onde colocar os sensores e o que fazer com o montante de logs capturados. Ferramentas especializadas ou experiência de profissionais capacitados pode ser requerida

para sintetizar e interpretar as informações coletadas para identificar falsos-positivo e criar maneiras de eliminar ou minimizar esse tipo de evento. Algumas organizações escolhem terceirizar esta atividade para outras empresas com mais conhecimento e expertise para resolução de problemas desta natureza.

- **Serviços proativos – Disseminação de informação relacionada à segurança:** Este serviço prevê a disseminação de material de fácil entendimento aos clientes e usuários da organização atendida pelo CSIRT buscando o aumento da segurança no seu elo mais suscetível a ameaças.
- **Serviços de gerenciamento de qualidade da segurança – Análise de risco**: O CSIRT pode ser capaz de adicionar valor a análises de risco, aumentando a capacidade da organização de avaliar ameaças reais e prover críticas qualitativas e quantitativas dos riscos a que está submetida.
- **Serviços de gerenciamento de qualidade da segurança – Plano de continuidade de negócios:** Baseado em ocorrências passadas e em previsões futuras de incidentes e tendências de segurança, mais e mais incidentes tem potencial para resultar em sério dano ou degradação dos negócios de uma companhia. Desta forma, o CSIRT deve planejar e considerar experiências e recomendações para melhor responder a incidentes catastróficos e garantir a continuidade dos negócios da sua empresa. Este serviço prevê a definição de um plano de continuidade de negócios, que norteará as ações da equipe durante eventos ou ameaças desta natureza.
- **Serviços de gerenciamento de qualidade da segurança – Consultoria de segurança:** O CSIRT pode ser usado para prover recomendações de implementação das melhores práticas de segurança as suas companhias. Neste caso, o time pode ser consultado durante processos de especificação e aquisição de novas soluções de tecnologia, como computadores, dispositivos de rede ou aplicações. Este processo inclui ainda o auxílio e o direcionamento de aspectos de segurança para a definição de políticas e normas internas.
- **Serviços de gerenciamento de qualidade da segurança – Conscientização interna:** O CSIRT pode ser capaz de identificar com seu público interno quais assuntos requerem mais informações para oferecer melhor treinamento sobre as políticas e práticas de segurança adotadas por sua organização. Aumentar o

conhecimento do público interno, não somente auxilia no entendimento geral sobre o tema segurança, como facilita a condução das atividades do dia-a-dia de uma maneira mais segura. Este trabalho está diretamente ligado à redução dos índices de ataques bem-sucedidos. É realizado com a disseminação da informação via e-mail, artigos, notícias ou outros recursos que explicam as melhores práticas de segurança e provê conselhos e precauções a serem tomadas.

- **Serviços de gerenciamento de qualidade da segurança – Educação / Treinamento:** Este serviço prevê a disseminação de conhecimento por meio de seminários, workshops, cursos e tutoriais. Pode estar incluso tópicos relacionados às ferramentas utilizadas, métodos de resposta apropriados, métodos de prevenção e outras informações necessárias para proteger, detectar, reportar e responder à incidentes de segurança computacionais.
- **Serviços de gerenciamento de qualidade da segurança – Certificação ou avaliação de produtos:** Neste serviço o time do CSIRT pode realizar atividades para avaliação de produtos, como ferramentas ou aplicações, para certificar sobre a adequação às necessidades da organização. (RUEFLE; VAN WYK; TOSIC, 2013).

2.4 Recursos

2.4.1 Equipe técnica

A composição do time de resposta a incidente de segurança é fundamental para o sucesso do CSIRT. A melhor equipe é aquela composta por talentos com variedade de habilidades. Eles devem ser: dedicados, inovadores, detalhistas, flexíveis, solucionadores de problemas, bons comunicadores e devem ter habilidade para trabalhar sob pressão ou em situações estressantes. Um dos aspectos mais importantes que um time CSIRT deve ter é integridade. Além disso, os membros precisam saber trabalhar em grupo, saber contornar situações de conflito em busca da melhor solução para a organização (RUEFLE; VAN WYK; TOSIC, 2013).

As habilidades podem incluir:

- Pessoais
    - Habilidades comunicativas
    - Inter-relacionamento
- Técnicas
    - Experiência na administração de redes e sistemas
    - Expertise em plataformas UNIX, Windows e Macintosh
    - Entendimento básico sobre protocolos de internet
    - Entendimento básico sobre ataques e vulnerabilidades comuns
- Treinamento em Segurança
    - Experiência em tratamento de incidentes
    - Habilidades em resolução de problemas
    - Pensamento crítico e habilidades de análise
    - Ameaças cibernéticas e conhecimento em técnicas de ataque
    - Análise forense e habilidades para análise de malware

2.4.2 Infraestrutura

Uma infraestrutura de CSIRT deve incorporar todas as precauções conhecidas que forem fisicamente e financeiramente possíveis. O time deve servir de modelo para outras organizações. Precisa-se ter certeza de que a companhia está segura e todos os dados sensíveis estão protegidos. Esta visão deve incluir infraestruturas físicas e lógicas da rede. O acesso à equipe do CSIRT deve ser tão rigoroso quanto o acesso às informações que o time trabalha. (RUEFLE; VAN WYK; TOSIC, 2013).

Para executar suas funções, a equipe precisa de acesso à sistemas básicos de computação e comunicação. Isto inclui, caso necessário, estações de trabalho no escritório e em casa, além de laboratório para testes e equipamentos de análise avançada de vulnerabilidades e malwares.

Uma infraestrutura de suporte para a operação do CSIRT e suas várias atividades de análise é altamente recomendada, como alternativa de utilização da rede principal da organização. Entretanto, nem sempre é possível devido a custos, logística ou conhecimento técnico disponível.

Recomendações e considerações que uma infraestrutura de suporte ao CSIRT deve incluir:

- Uma rede separada para o CSIRT
- Configurações seguras e rede protegida
- E-mail separado; acesso web, DNS e outros servidores e serviços dedicados
- Sistemas atualizados e versões de software consistente
- Métodos padronizados para instalação de patchs e atualizações
- Rede de laboratório e dispositivos para testes
- Intranet segura para comunicação interna da equipe CSIRT
- Sistema robusto para registro e rastreio de tickets de incidentes
- Mecanismo de comunicação confiável, com funcionalidades de áudio e vídeo conferência.
- Sistema de acesso remoto eficiente e seguro
- Ferramentas de análise, correlação e visualização de logs

3 TRATAMENTO DE INCIDENTES EM INSTITUIÇÃO DE ENSINO

3.1 Contexto

Nos dias de hoje, cada vez mais, as instituições de ensino têm incorporado recursos de tecnologia da informação em suas diversas áreas de atuação. A informática tem se tornado um componente indispensável nas atividades relacionadas à ensino e pesquisa. Mais do que processadores de informação, os computadores têm função imprescindível na maioria das atividades acadêmicas, seja no desenvolvimento de conteúdo, seja na apresentação de novas metodologias de ensino interativas. A tecnologia tem ajudado na redução do custo das atividades acadêmicas. Os computadores, softwares e periféricos estão cada vez mais acessíveis, poderosos e portáteis. Esta evolução tem impacto quantitativo e qualitativo nos processos das instituições de ensino. Além disso, o advento dos dispositivos móveis, permitiu que serviços computadorizados sejam acessados de qualquer lugar, diminuindo os limites entre espaços específicos para os computadores e suas configurações. A internet também trouxe mudanças substanciais no uso dos computadores, e transformou-se num meio para comunicação e expressão pessoal. Entretanto, na contramão desse fenômeno crescente e dinâmico estão os incidentes de segurança da informação, que estão obrigando administradores de sistemas a se atentar quanto à segurança de seus aplicativos e serviços (FOMBONA; RODRÍGUEZ; BARRIADA, 2012).

O ambiente de uma instituição de ensino é formado por pessoas de diferentes classes sociais e culturais. Com isso, os recursos de TI são utilizados por uma variedade de usuários e para finalidades diversas, transformando o espaço acadêmico único em cada instituição. Além disso, o contexto acadêmico direciona tais recursos para experimentação e aprendizado, onde vários usuários compartilham o mesmo computador. Ao mesmo tempo, isso leva a realizações acadêmicas inovadoras e a usos inadequados, avarias e desvios dos objetivos educacionais definidos. A interação próxima entre os usuários e os computadores, e o alto potencial para o acontecimento de incidentes, determina que diretrizes operacionais são necessárias. Por este motivo, as instituições precisam publicar normas, políticas e regulamentos internos para embasar o comportamento de colaboradores e clientes.

No passado, os computadores eram concentrados em salas especificas, como laboratórios, onde os estudantes tinham acesso em horário determinado ou quando as atividades requeriam o uso de computadores. Estes ambientes eram concebidos para serem fechados e isolados. Desta forma, os computadores eram conectados à rede local, onde impressoras e outros serviços poderiam ser compartilhados. Hoje, com o surgimento das redes sem fio, os computadores estão em todos os lugares além de estarem abertos para comunicação com a rede local e com a internet. Outro detalhe é o fato de que os aplicativos estão cada vez mais online, disponíveis em servidores remotos, hospedados na nuvem, sem que haja necessidade de instalação e manutenção local destes programas.

O objetivo inicial de um departamento de tecnologia de uma instituição de ensino é dar o suporte adequado para permitir que os usuários realizem suas atividades acadêmicas e administrativas. Entretanto, é possível que o uso do computador seja desvirtuado pelos usuários, para uso em atividades com propósito indefinido, como atividades recreativas por exemplo. Por este motivo, algumas instituições implementam regras rigorosas para uso da rede de computadores. Em outros casos, outras instituições defendem o acesso irrestrito, aberto à exploração e inovação. De qualquer forma, a instituição precisa estar preparada para um novo perfil de usuário, que já nasceu na era digital, que tem a capacidade de fazer múltiplas tarefas ao mesmo tempo, sem perder a atenção em nenhuma delas ou precisar de mais tempo para fazê-las. Este novo contexto é amplo e difícil de delimitar. As instituições devem oferecer a seus usuários a oportunidade de usar hardware e software com certas restrições e sob regras específicas. É fundamental estabelecer o próprio conjunto de aplicativos autorizados para uso nos computadores e quais estarão disponíveis para estudantes, visitantes e funcionários administrativos (FOMBONA; RODRÍGUEZ; BARRIADA, 2012).

3.2 Cenário

A Faculdade Segura[3] é uma instituição de ensino da Cidade de Brasília, no Distrito Federal. Seus funcionários e alunos estão distribuídos em 3 campus, nos bairros de Taguatinga, Sobradinho e Guará. A instituição está em constante crescimento, investindo substancialmente em recursos informatizados para a melhoria dos processos internos e nos serviços oferecidos a seus clientes e funcionários. Para facilitar o entendimento do público interno desta instituição, este pode ser agrupado em 3 diferentes tipos: alunos (9.000), professores (700) e colaboradores administrativos (300) totalizando cerca de 10.000 usuários. Não há divisão rígida entre os 3 tipos de usuário, pois em algumas situações, alunos e professores compartilham o mesmo computador, e em outras ocasiões, professores podem realizar tarefas administrativas ou gerenciais nos computadores dos colaboradores administrativos.

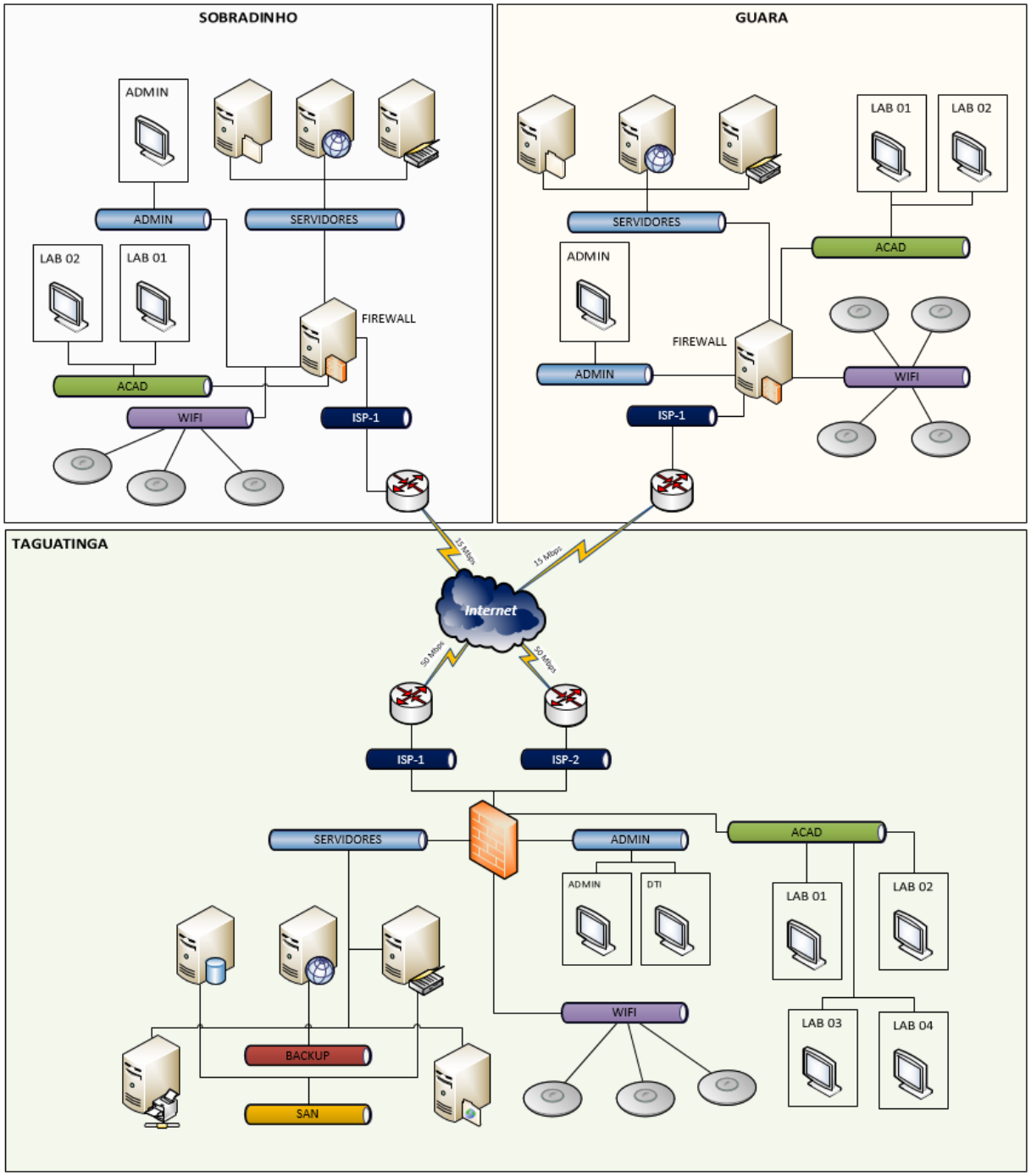
A equipe do Departamento da Informática é composta da seguinte forma:

- 8 Técnicos de Suporte
- 4 Analistas de Desenvolvimento
- 2 Analistas de Banco de Dados
- 2 Administradores de Rede
- 1 Gerente de Projetos
- 1 Diretor de TI

A rede de dados da instituição inclui cerca de 2.000 computadores, além de pontos de acesso sem fio, por onde é disponibilizado acesso à internet para professores e alunos. Os 3 campi são interligados via VPN (Virtual Private Network) e todos os computadores compõe um mesmo segmento lógico, conforme topologia ilustrada na figura 4 abaixo.

[3] Instituição fictícia criada pelo autor para apresentação do cenário do estudo de caso.

Figura 4 – Topologia da Rede da Faculdade Segura



Fonte: Elaborado pelo autor do trabalho.

Os usuários têm acesso à rede por meio de credenciais de uso pessoal, cadastradas e sincronizadas com o sistema de gestão corporativa. A autenticação é validada em um banco de dados centralizado. Os acessos são controlados e limitados com base na necessidade de cada tipo de usuário. Todos os acessos são

registrados e uma trilha de auditoria é gravada, para permitir o rastreio das informações, em caso de incidente.

A demanda por recursos tecnológicos tem acompanhando o crescimento da empresa. Constantemente o departamento de informática é acionado para implementar soluções de TI para à área acadêmica. Os alunos da instituição, cada vez mais digitalmente inseridos, pressionam a companhia para que sejam implementadas soluções inovadoras para seus problemas.

A instituição não possui processos definidos para o tratamento de incidentes de segurança. Não há um sistema de registros de incidentes ocorridos no passado. O investimento em soluções de segurança é sempre um desafio para o departamento de informática, que precisa justificar minunciosamente com a direção da instituição os altos custos nas ferramentas e serviços disponíveis no mercado.

3.3 Estudo de Caso

O plano de tratamento de incidentes proposto no próximo tópico foi desenvolvido a partir da análise do cenário da Faculdade Segura. A definição do conteúdo originou-se do estudo de registros de incidentes passados, mas que não haviam sido considerados incidentes de segurança. Além desta ação, foi realizada consulta aos funcionários da área de tecnologia da instituição, que contribuíram com a definição do plano, descrevendo os principais tipos de incidentes e os papeis e responsabilidades de cada profissional durante o ciclo de vida do incidente.

A definição do plano baseou-se também na observação do autor quanto às melhores práticas a serem adotadas para o tratamento de futuros incidentes de segurança. Foi utilizado material de referência publicado por órgãos que são responsáveis por normatizar temas semelhantes para a comunidade na Internet, como o CERT CC e o CERT.BR. O plano foi apresentado e aprovado pela Diretoria de TI da Faculdade Segura e será implementado após aprovação pelo conselho Diretor da instituição.

3.4 Plano para o Tratamento de Incidentes de Segurança

3.4.1 Propósito

O principal objetivo deste plano é descrever os processos para reportar e gerenciar os dados relacionados a incidentes de segurança que podem ser originados de fontes internas ou externas. Também é objetivo deste plano esclarecer as formas para o reporte de vulnerabilidades na segurança observadas por agentes internos (funcionários e clientes) ou externos (auditores e a comunidade).

É importante que os incidentes de segurança e as vulnerabilidades reportadas sejam devidamente investigadas e gerenciadas. Em algumas circunstâncias talvez seja necessário que autoridades policiais sejam acionadas. Desta forma, evidências devem ser coletadas e armazenadas pois podem servir de provas em processos judiciais. Uma investigação detalhada de uma atividade suspeita pode facilmente identificar uma vulnerabilidade ou deficiência nos computadores da Faculdade Segura. Este processo garante que estas vulnerabilidades ou deficiências sejam tratadas tão logo que sejam descobertas diminuindo o risco e prevenindo o impacto de incidentes futuros.

3.4.2 Escopo

Este plano descreve papéis, responsabilidades e processos relacionados ao tratamento de incidentes com a intenção de garantir agilidade na contenção e resolução de todos os incidentes de segurança e vulnerabilidades reportadas aos sistemas e ativos da Faculdade Segura.

3.4.3 Definições

Um incidente de segurança da informação pode ser definido como:

- Um evento ou situação adversa associada a qualquer serviço de TI que exponha a Faculdade Segura ou seus sistemas a ameaças contra a Integridade, Confidencialidade ou Disponibilidade;
- Qualquer evento que pode resultar em perda ou dano à ativos de TI;

- Qualquer ação que pode ser considerada uma violação as normas e políticas de segurança, incluindo os acontecimentos acidentais.

3.4.4 Papéis e responsabilidades

Os seguintes papeis e responsabilidades estão relacionados a este plano são:

- **Comitê de Segurança e Risco**
  - Analisar todos os achados relevantes em relatórios de auditoria;
  - Analisar ações baseando-se em incidentes identificados que podem representar vulnerabilidades na segurança;
  - Garantir que ações de melhoria são encomendadas as equipes responsáveis;
  - Revisar todos os incidentes reportados e notificar instâncias superiores, quando necessário.
  - Conduzir revisões pós-incidentes e coordenar a resolução dos incidentes.
  - Acionar o time de resposta a incidentes e envolver recursos externos na resolução, quando necessário.
  - Comunicar o progresso de resposta aos incidentes a todos os envolvidos (internos e externos).
  - Gerenciar e classificar todos os incidentes e ações corretivas.
  - Apresentar relatórios pós-incidentes ao Comitê de Segurança para discussão.
- **Diretor**
  - Aprovar o envolvimento de recursos externos durante a resolução de incidentes críticos
  - Aprovar comunicações internas relevantes e notificar a Reitoria da Instituição, caso necessário.

- **Equipe de Resposta a Incidentes**
    - Prover suporte e orientação para detectar e resolver incidentes de segurança.
    - Reportar incidentes ou vulnerabilidades conhecidas ao Comitê de Segurança e Risco, quando necessário.
    - Conduzir a resolução de incidentes de segurança através do fluxo normal de incidentes de TI, incluindo o registro numa ferramenta de gerenciamento de tickets.
    - Executar ações corretivas para resolver incidentes de segurança.
    - Elevar requisições importantes para mudanças, quando necessário.

3.4.5 Comunicações

Durante a reposta a incidentes é vital que todos os envolvidos, internos e externos da instituição, sejam informados sobre o andamento da resposta. Inicialmente, os detalhes técnicos e os achados devem ser mantidos de forma confidencial e as informações divulgadas somente para os diretamente envolvidos ou impactados pelo incidente.

Em um evento de segurança de alta prioridade, pode ser apropriado notificar agentes externos, que podem incluir:

- Agencias importantes do governo e ou forças policiais (para prover assistência adequada, caso necessário)
- Público externo (comunidade, empresas parceiras)

O comitê de segurança e risco deve indicar quem precisa ser notificado durante e no encerramento de um incidente. Todas as notificações precisam ser aprovadas pelo Diretor.

3.4.6 Tipos de Incidente

Os tipos de eventos e incidentes de segurança devem incluir (Quadro 2):

Quadro 2 – Tipos de Incidente

Tipo	Definição
Incidente Malicioso	Qualquer ação intencional que leve, ou possa levar, a perda, dano ou corrupção dos ativos de TI da Faculdade Segura
Violação de Acesso	Uso não autorizado de sistema de TI, incluindo mau uso de contas e senhas, visando ataques que vão de encontro a uma política de segurança
Roubo / Furto	Roubo ou furto de qualquer equipamento de TI ou informação de propriedade da instituição
Uso inapropriado	Mau uso de facilidades para acessar conteúdo inapropriado
Acidente	Qualquer falha acidental ou não intencional decorrente da não observação de política de segurança
Incidente Operacional	Evento de falha de sistema ou mudança em uma configuração que resulte em perdas de disponibilidade ou integridade de sistemas ou informações

Fonte: Adaptado de *Incident Management Procedure, Flinders University*

3.4.7 Prioridades

Os incidentes devem ser priorizados de acordo com as seguintes definições (Quadro 3):

Quadro 3 - Prioridades

Prioridade	Descrição	Exemplo de Incidente	Resposta Esperada
Baixa	Um evento de baixo impacto com pouco ou nenhum efeito operacional e que requer pouco esforço para gerenciar e resolver	• Incidente de vírus em um único computador ou dispositivo • Diversas tentativas mal sucedidas de obter acesso não autorizado	Resolvido por agentes da equipe de resposta com ações já mapeadas.
Média	Possível brecha de segurança que requer investigação e envolvimento do Comitê de Segurança para resolução	• Acesso não autorizado a uma conta de serviço • Tentativa de acesso à sala de servidores • Escaneamento de portas em rede interna ou externa • Múltiplos incidentes de vírus	Precisa ser escalado para o Comitê de Segurança e Risco para coordenação, investigação e resolução

Alta	Evento com impacto significante a serviços críticos de TI ou informações, dano a equipamento físico ou à pessoas	• Violação em larga escala de dados sensíveis a pesquisa, dados financeiros ou pessoais • Pichação do website da instituição • Acesso não autorizado à sala de servidores • Comprometimento de dados de pagamento	Precisar ser escalado ao Diretor e ao Comitê de Segurança Imediatamente Todos os envolvidos precisam ser notificados Uma revisão pós-incidente precisa ser realizada

Fonte: Adaptado de *Incident Management Procedure, Flinders University*

3.4.8 Notificação de Incidente

Os incidentes podem ser notificados por qualquer usuário interno ou ainda de fontes externas, como clientes e parceiros. O canal preferencial é o e-mail csirt@facsec.edu.br ou pelo telefone (61) 3451-0000. Estes canais devem ser amplamente divulgados para facilitar o registro de atividades suspeitas ou de incidentes já identificados.

3.4.9 Armazenamento de Documentos e Evidências

Durante o tratamento de um incidente todas as evidências relevantes precisam ser coletadas e armazenadas. Além disso todas as ações devem ser registradas, para permitir análise posterior por parte de autoridades ou outras pessoas autorizadas.

As evidências podem incluir, mas não se limitar a:

- Logs de auditoria
- Arquivos de malware
- Dados e e-mail
- Alertas de Segurança

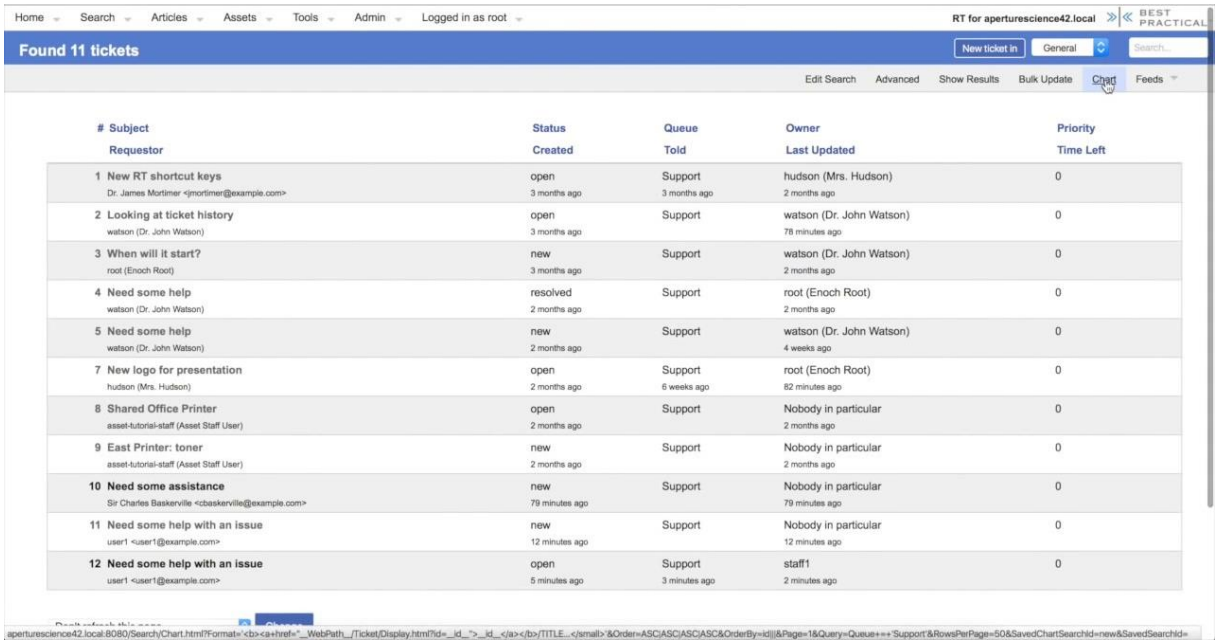
- Dados sobre os sistemas comprometidos
- Imagem de disco virtual

Todos os incidentes devem ser bem documentados na ferramenta *RT-Request Tracker*, ferramenta gratuita da empresa *Best Practical*, que está parametrizada para o registro e o acompanhamento dos incidentes. As informações obrigatórias no registro de um incidente são:

- Todas as informações repassadas pelo usuário
- Ações tomadas pelo time de resposta
- Resultadas do processo de investigação
- Informações acerca do contato com os envolvidos

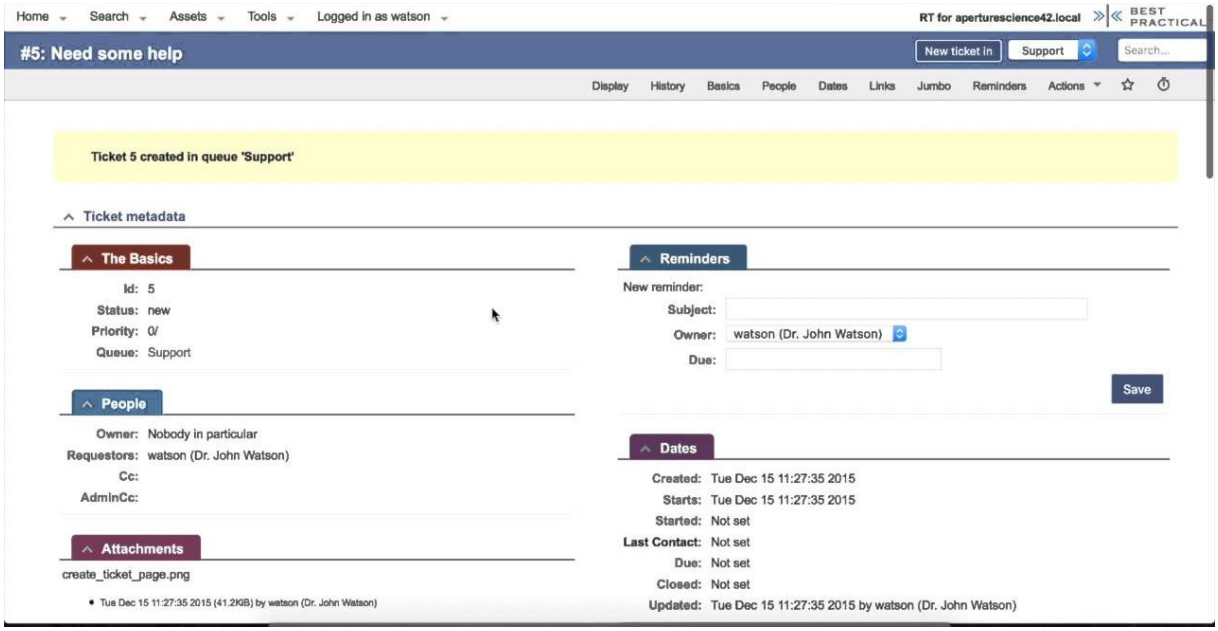
As figuras 5 e 6 abaixo mostram o exemplo de uma fila de tratamento de *tickets*, registrados no *Request Tracker*. A ferramenta é utilizada para documentar as interações do time de resposta durante o atendimento de um incidente.

Figura 5 – Exemplo de Fila no RT



Fonte: Elaborado pelo autor do trabalho.

Figura 6 – Exemplo de Ticket no RT



Fonte: Elaborado pelo autor do trabalho.

Durante o tratamento de incidentes, os usuários devem ser orientados a não realizar nenhuma alteração ou modificação nos sistemas comprometidos até que a equipe de resposta a incidentes autorize.

3.4.10 Checklist de Tratamento de Incidentes

Quadro 4 – Checklist (ações para incidentes de baixa prioridade)

Ação		Responsável
Ações comuns		
1.	**Procedimento para tratamento de notificação de incidente** • Reporte deve ser recebido via e-mail ou telefone • Todos os detalhes precisam ser registrados, incluindo detalhes de contato, e o ticket deve ser atribuído para um membro da equipe de resposta	Equipe de resposta a incidente
2.	**Revisar detalhes e atribuir prioridade** • A equipe de resposta precisa revisar os dados iniciais da notificação de incidente para determinar a criticidade e deve atribuir uma prioridade para o caso	Equipe de resposta a incidente
Incidentes de baixa prioridade		
3.	**Contenção ou remoção de ameaça** • O incidente deve ser atribuído a um membro da equipe de resposta a incidente e deve ser tratado com uma solução já mapeada	Equipe de resposta a incidente

	• O membro responsável deve seguir a orientação descrita em roteiros já mapeados • As ações podem conter a remoção de vírus, reset de conta de usuário ou ainda o contato direto com o usuário impactado. • Se um computador contiver um vírus de baixo impacto, o dispositivo deve ser desconectado da rede para prevenir a propagação. Outros computadores devem ser analisados para verificação de comprometimento.	
4.	**Recuperação/restauração dos sistemas afetados** • Uma vez que a causa do incidente foi solucionada, o computador ou a conta de usuário deve ser recuperada. • Em eventos em que há comprometimento de sistemas, como numa infecção de vírus ou outra vulnerabilidade, o sistema operacional deve ser reinstalado para remover todos os traços da infecção. Após este processo, a máquina pode ser reconectada à rede.	Equipe de resposta a incidente
5.	**Documentação dos resultados** • Toda a investigação e as ações de recuperação precisam ser registradas no sistema RT. • Todos os detalhes relacionados a como o incidente foi resolvido deve ser anotado	Equipe de reposta a incidente

Fonte: Adaptado de *Incident Management Procedure, Flinders University*

Quadro 5 – Checklist (ações para incidentes de média prioridade)

Ação		**Responsável**
Ações comuns a incidentes de alta e média prioridade		
6.	**Investigação Inicial** O comitê de segurança precisa revisar um incidente antes de ser considerado médio ou alto, afim de validar as informações e definir quais os paços iniciais para iniciar a investigação. Os seguintes fatores precisam ser considerados ao elevar a prioridade de um incidente para Alta: • Dados pessoais ou privados foram comprometidos? • O impacto é visivelmente público? • O incidente pode impactar negativamente a reputação da Faculdade, de alunos ou funcionários?	Comitê de Segurança e Risco
Incidentes de média prioridade		
7.	**Contenção ou remoção de ameaça** • Os incidentes devem ser atribuídos a um membro do Comitê de Segurança que pode acionar qualquer outro funcionário, caso necessário. • O comitê precisa determinar se algum computador	Comitê de Segurança e Risco

	será confiscado até que a investigação seja realizada. Em algumas circunstancias, o computador precisa ser desligado da rede até que se tenha um parecer favorável ao restabelecimento pela equipe técnica. • Todos os vírus, material improprio ou outras causas de um incidente devem ser removidos durante a contenção para previr a propagação ou o comprometimento de outros sistemas.	
8.	**Remediar vulnerabilidades identificadas** • A investigação de um incidente pode revelar fraquezas ou vulnerabilidades nos processos de controle de segurança • O comitê deve identificar, documentar e tomar ação para remediar as fraquezas e as vulnerabilidades implementando ou improvisando controles para prevenir a recorrência do mesmo evento • A remediação pode se estender para análise de violações a políticas de segurança, e nestes casos o Comitê deve prover a conscientização ao usuário envolvido	Comitê de Segurança e Risco
9.	**Recuperação/restauração dos sistemas afetados** • Uma vez que a causa do incidente foi solucionada, o computador ou a conta de usuário deve ser recuperada. • O objetivo desta recuperação é restabelecer os sistemas afetados de forma a evitar futuros incidentes semelhantes. • O comitê definirá se o sistema operacional deve ser reinstalado ou um backup disponibilizado para permitir a recuperação. • Uma vez que isto ocorra, o sistema pode ser reconectado à rede, para retorno a suas atividades normais	Equipe de reposta a incidente
	Condução de revisão e relatório pós-incidente • O comitê deverá rever a documentação e as evidências coletadas para determinar a causa raiz além de prover recomendações para prevenir a recorrência deste incidente. • Recomendações levantadas devem ser entregues em relatório pós-incidente para o Diretor. • O comitê deve informar os usuários impactados diretamente e os que reportaram problema inicial	Comitê de Segurança e Risco

Fonte: Adaptado de *Incident Management Procedure, Flinders University*

Quadro 6 – Checklist (ações para incidentes de alta prioridade)

Ação		Responsável
Incidentes de média prioridade		
10.	**Acionamento do Time de Resposta** Dado o tamanho de um incidente de alta prioridade, o Diretor será responsável por acionar e coordenar os trabalhos dos especialistas necessários. Isto irá permitir a coordenação centralizada das ações para resposta ao incidente com o intuito de evitar impacto negativo à instituição. A comunicação entre os envolvidos é fundamental para permitir a rápida resposta. A força tarefa pode ser dividida em três frentes: Investigação: Identificar a causa, motivação, usuários envolvidos e o dano causado pelo incidente Contenção: Implementação de ações de monitoração e de controles de correção para reduzir o impacto durante um incidente Restauração: Recuperação dos sistemas impactados ou ativação de plano de recuperação de desastres para restaurar os serviços para um estado seguro	Diretor
11.	**Designar um coordenador de comunicação** O Diretor irá definir um coordenador de comunicação, para garantir eficácia e eficiência na comunicação com os usuários impactados e todos os outros envolvidos no incidente.	Diretor
12.	**Notificar envolvidos relevantes** Em eventos de alta prioridade, o coordenador de comunicação nomeado irá trabalhar com o Diretor para determinar quem precisa ser notificado do incidente: • O mantenedor da instituição • Funcionários e clientes • Agências do governo • Empresas parceiras • Comunidade	Coordenador de comunicação
13.	**Condução de revisão e relatório pós-incidente** • O diretor deverá conduzir um processo formal de revisão do ocorrido apresentando uma breve discussão sobre a causa raiz do incidente, provendo feedback sobre a resposta dada para resolução do problema e sobre as recomendações de melhoria	Diretor
14.	**Revisão dos resultados** O diretor deve promover ações de melhoria para que novos incidentes sejam evitados O diretor deve avaliar todo o processo de tratamento em busca do aperfeiçoamento das ações tomadas para contenção e erradicação do incidente	Diretor

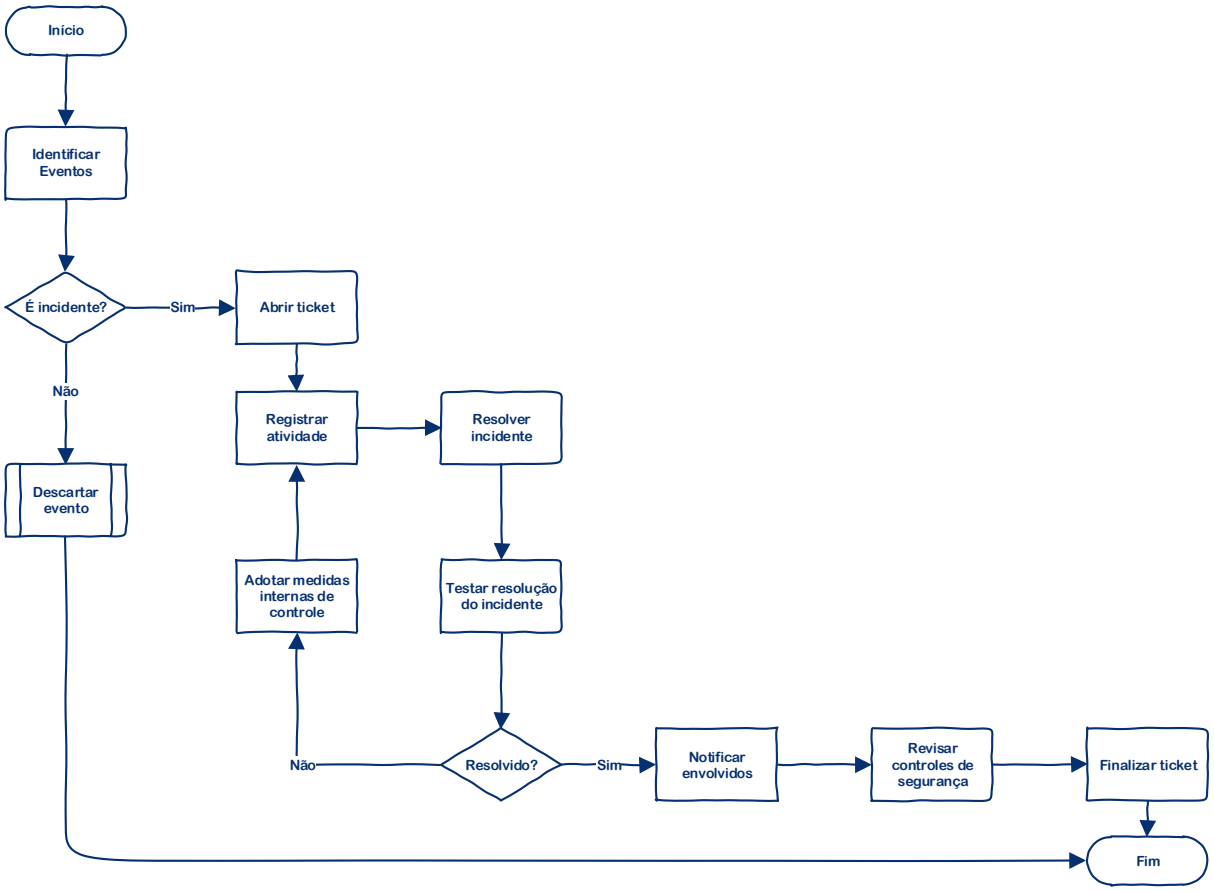
Fonte: Adaptado de *Incident Management Procedure, Flinders University*

Nestes quadros estão descritos os passos macro para a manipulação de incidentes de acordo com a prioridade descrita anteriormente. Os procedimentos podem ser ajustados para adequar-se às características de cada tipo de incidente. Além disso, as ações recomendadas devem ser melhoradas continuamente e ajustadas para otimizar o processo, afim de estabelecer a melhor forma de contenção e erradicação de incidentes.

3.4.11 Fluxo Básico para Tratamento do Incidentes

Na figura 7 abaixo está descrito as etapas básicas durante o processo de tratamento de incidentes de segurança.

Figura 7 – Fluxo de Tratamento de Incidentes



Fonte: Elaborado pelo autor do trabalho.

CONCLUSÃO

Ao longo do desenvolvimento deste trabalho, o objetivo proposto inicialmente foi aperfeiçoado e moldado para se adequar à realidade da Faculdade Segura. O estudo permitiu compreender que, apesar das inúmeras referências disponíveis, os processos, as atividades e os serviços oferecidos pelo CSIRT precisam se ajustar às necessidades da cada instituição. Desta forma, o produto gerado ao final deste trabalho contempla um plano de resposta a incidentes de segurança, com as informações necessárias para o tratamento de incidentes durante seu ciclo de vida, especificamente para a Faculdade Segura. Este documento foi gerado a partir da análise de eventos anteriores, registrados em memória digital e armazenados para a geração de estatísticas, mas que ainda não haviam sido analisados sob o aspecto da segurança.

Os objetivos específicos também foram plenamente atingidos e um descritivo foi exposto sobre uma equipe de resposta a incidente, seus aspectos gerais, os tipos existentes e os serviços frequentemente oferecidos às organizações. Este conteúdo foi fundamental para viabilizar a definição do plano de tratamento de incidentes da Faculdade Segura. A proposta para essa documentação é permitir que a empresa tenha mecanismos para tratar futuros incidentes, além de dar insumos para saber evita-los ou mitiga-los com mais eficiência.

Desta forma, espera-se que a equipe de resposta a incidentes de segurança da Faculdade Segura saiba responder questões como: quem, o que, onde, porque e como um evento desencadeou um incidente de segurança e qual o impacto desta ação para os negócios da empresa. Espera-se ainda que, ao final de cada ocorrência, estejam disponíveis as informações como:

- Quando o problema foi detectado primeiro e por quem
- O escopo do incidente
- Como foi contido ou erradicado
- O trabalho gerado durante o restabelecimento dos serviços
- Áreas onde o CSIRT foi mais efetivo
- Áreas que precisam de melhorias

A extração dos dados registrados no sistema de registro de incidentes permitirá a geração de informação valiosa para a companhia, pois promoverá a visibilidade de incidentes antes não observados. Isto permitirá o amadurecimento da empresa e proporcionará mais confiabilidade nos sistemas informatizados, o que com certeza beneficiará seus clientes, cada mais existentes e atentos às tecnologias disponíveis no mercado.

Ao observar o comportamento de diversas equipes de resposta a incidente foi possível observar que o compartilhamento de informações com equipes de instituições semelhantes é importante para a prevenção e o aprendizado dos principais problemas enfrentados, além de viabilizar o estreitamento da relação com as companhias que implementam soluções de TI e vivenciam os mesmo problemas e desafios.

Embora o objetivo do trabalho tenha sido atingido, as ações para implementação do CSIRT têm que prosseguir. As atividades previstas no plano de tratamento precisam ser implementadas. Além disso, as ferramentas necessárias para viabilizar o serviço da equipe de resposta a incidentes de segurança, precisam ser implantadas.

Conforme analisado durante a revisão literária, as atividades para repensar os processos e aprimorar as ações da equipe de resposta a incidentes deve ser realizada de forma constante. O ciclo deve sempre conter etapas de planejamento, execução e revisão das atividades previstas durante o tratamento de incidentes.

REFERÊNCIAS

CERT.BR. CSIRT FAQ. Disponível em <https://www.cert.br/certcc/csirts/csirt_faq-br.html>. Acesso em: 7 ago. 2017.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY - ENISA. *Good Practice Guide for Incident Management*, 2010. Disponível em: <https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management>. Acesso em: 12 ago. 2017.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY - ENISA. *Abordagem gradual de criação de uma CSIRT*, 2006. Disponível em: <https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-portugese>. Acesso em: 12 ago. 2017.

FINNIS, Aaron. *"Flinders University: Information Security – Incident Management Procedure"*, 2015. Disponível em: <http://www.flinders.edu.au/fms/documents/Information%20Security%20Incident%20Management%20Procedure%201_2.pdf>. Acesso em: 16 jul. 2017.

FOMBONA, Javier; RODRÍGUEZ, Celestino; BARRIADA, Calorina. Information Technology Incident Management: A Case Study of the University of Oviedo and the Faculty of Teacher Training and Education, 2012. In: Innovation and Good Practices in University Government and Management [online dossier]. *Universities and Knowledge Society Journal (RUSC)*. v. 9, n. 2, p. 280-295. Disponível em: <http://rusc.uoc.edu/rusc/ca/index.php/rusc/article/download/v9n2-fombona-rodriguez-barriada/1399-3919-1-PB.pdf>. Acesso em: 10 ago. 2017.

GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA – GSI. Norma complementar nº 05/IN01/DSIC/GSIPR, de 17 de agosto de 2009: Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf>. Acesso em: 28 jul. 2017.

HOEPERS, Cristine. *Projeto e implementação de uma infra-estrutura para troca e análise de informações de honeypots e honeynets*. São José dos Campos: INPE, 2008.

MOREIRA, Juliana Rocha Munita. *A arquitetura e-PING – Padrões de Interoperabilidade de Governo Eletrônico e a Gestão da Segurança da Informação na e-PING*: Um Estudo de Caso. 2011. Monografia (especialização) – Universidade de Brasília. Instituto de Ciências Exatas. Departamento de Ciência da Computação, Brasília, 2011. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_2009_2011/38_Juliana.pdf>. Acesso em: 12 jul. 2017.

RAMOS, Anderson et al. *Security Officer 1* – Guia Oficial para Formação de Gestores em Segurança da Informação. 2. Ed. Porto Alegre, RS: Zouk, 2008.

RUEFLE, Robin; VAN WYK, Ken; TOSIC, Lana. *New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs).* New Zealand National Cyber Security Centre, 2013. Disponível em: <https://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf>. Acesso em: 12 ago. 2017.

STELVIO, B. V. Creating and Managing Computer Security Incident Handling Teams (CSIRTs), Carnegie Mellon University, 2002. Disponível em: < https://www.first.org/resources/papers/conference2008/killcrece-georgia-slides.pdf>. Acesso em: 11 ago. 2017.

WEST-BROWN, Moira J. et al. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Technical report, CMU/SEI-2003-HB-002. Carnegie Mellon University, 2003. Disponível em: <https://www.sei.cmu.edu/reports/03hb002.pdf>. Acesso em: 12 ago. 2017.

APÊNDICE A – Exemplos de Incidentes Mais Comuns

Exemplos dos tipos mais comuns de incidentes estão listados abaixo:

Incidente Operacional

- Perda de serviço
- Mal funcionamento de sistema
- Mudanças não controladas em sistemas

Incidente Malicioso

- Computador infectado com vírus ou outro tipo de malware (spyware ou adware por exemplo)
- Escaneamento de portas de rede não autorizado
- Alteração em dados por pessoa não autorizada
- Recebimento ou encaminhamento de correntes, incluindo alertas de vírus, phishings e outros tipos de e-mails que estimular o compartilhamento com outros usuários
- Mensagens de Spams contendo conteúdo malicioso
- Engenharia social – pessoa desconhecida perguntando sobre informações que podem conceder acesso a dados da instituição
- Divulgação não autorizada de informações sensíveis ou confidenciais da instituição, por meio eletrônico, impresso ou verbal
- Falsificação ou destruição de registros institucionais
- Danificação ou interrupção proposital de serviços ou equipamentos da organização
- Conexão de qualquer equipamento terceiro à rede da organização
- Uso ou acesso não autorizado à informação
- Repasse de informação sensível ou confidencial para pessoal não autorizada, por meio eletrônico, impresso ou verbal
- Impressão ou cópia de dados sensíveis ou confidenciais sem o devido armazenamento

- Pichação de site

Violação de Acesso

- Divulgação de logins para pessoa não autorizada
- Escrever senha em papeis ou deixar a mostra para que outra pessoa encontre facilmente
- Acesso a sistemas usando credenciais de outra pessoa
- Compartilhamento inapropriado de dispositivos de segurança, como tokens
- Outros tipos de comprometimento de usuário, como por exemplo dar acesso a outra pessoa a credenciais de pessoa autorizada
- Acesso à ambiente restrito, como a sala de servidores

Uso inapropriado

- Acesso a material inapropriado na internet
- Envio de e-mails com conteúdo inapropriado
- Praticas não autorizadas em ambiente de trabalho ou que não estejam em conformidade com políticas da empresa
- Material falsificado ou que infringe direitos autorais
- Mal-uso de facilidades para benefício pessoal

Roubo / Furto

- Roubo ou furto de dados – impressos ou por meio eletrônico
- Roubo ou furto de qualquer tipo de equipamento da instituição

Acidente

- Envio de e-mail com informação confidencial para todos os funcionários por engano
- Recebimento de material não solicitado com natureza ofensiva ou contendo pornografia, racismo ou material violento

- Recebimento de e-mail não solicitado requerendo dados pessoais
- Recebimento de informação não autorizada
- Envio de informação confidencial para o destinatário errado