Centro Federal De Educação Tecnológica De Minas Gerais
PATRICK LEANDRO MAGALHÃES

# IMPLEMENTAÇÃO DE UM CENTRO DE TRATAMENTO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO NO DECOM/CEFET-MG

BELO HORIZONTE
2016

Centro Federal De Educação Tecnológica De Minas Gerais
PATRICK LEANDRO MAGALHÃES

# IMPLEMENTAÇÃO DE UM CENTRO DE TRATAMENTO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO NO DECOM/CEFET-MG

Trabalho de conclusão de curso apresentado ao Programa de Pós-Graduação em Administração, Análise e Desenvolvimento de Sistemas de Informação do Centro Federal de Educação Tecnológica de Minas Gerais.

Orientador: Prof. Sandro Renato Dias

BELO HORIZONTE
2016

# RESUMO

O objetivo do presente trabalho é a implementação de um centro de tratamento de incidente de segurança da informação (CSIRT) no Departamento de Computação do CEFET-MG, com o intuito de registrar, monitorar e atuar sobre os incidentes relacionados ao domínio do CEFET-MG. Realizado através de entrevista, pesquisas em sites especializados e fundamentação teórica, o trabalho permitiu avaliar os processos de segurança existentes, verificar invasões realizadas por hackers no ambiente computacional da instituição e propor uma estrutura de metodologia de desenvolvimento de um CSIRT.

**Palavras-Chave:** CEFET-MG; CSIRT; Incidentes de Segurança; Risco; Segurança da Informação.

BELO HORIZONTE

2016

# ABSTRACT

The main purpose of this work is the implementation of a *Computer Security Incident Response Team (*CSIRT) in the Computer Department of CEFET-MG, in order to register, monitor and act on incidents related to CEFET-MG domain. Conducted through interviews, research on specialized sites and theoretical foundation, the work allowed evaluating existing security processes, verify intrusions made by hackers in the computer environment of the institution and propose a structure of a CSIRT development methodology.

**Keywords**: CEFET-MG; CSIRT; Information security; Risk; Security incidents.

BELO HORIZONTE

2016

# LISTA DE FIGURAS

# LISTA DE TABELAS



BELO HORIZONTE

2016

# Sumário

BELO HORIZONTE

2016

# 1 INTRODUÇÃO

Segundo ROHR (2014) em seu texto divulgado no portal eletrônico G1, o Brasil aparece entre as 10 maiores origens de ataques cibernéticos e entre os 5 países que mais abrigam computadores zumbis, em uma lista divulgada no Relatório Anual sobre Ameaças à Segurança na Internet (Internet Security Threat Report, ou ISTR na sigla em inglês) pela empresa de segurança Symantec.

Em reportagem do TNONLINE (2015), o CERT.br conseguiu através de seus monitoramentos, registrar um aumento de 197% no número de incidentes reportados em 2014 no Brasil.

O ambiente virtual, necessário para a sobrevivência das empresas no mercado atualmente, tornou-se propício para ataques cibernéticos, fraudes, vazamentos de informações e abriga serviços essenciais para uma empresa moderna como e-commerce, comunicação por e-mail, interação entre sistemas on-line, trabalho remoto.

Em consequência do dinamismo do ambiente e virtual, no qual as empresas estão inseridas, a preocupação com os seus dados faz com que sejam necessários investimentos em infraestrutura computacional e humana para melhorar sua segurança da informação.

Segundo dados da PWC (2014), em sua Pesquisa Global de Segurança da Informação, “a média dos orçamentos de segurança da informação cresceu 51% em relação ao ano passado”. Estimativas da pesquisa apresentam o valor médio de US$ 1 milhão destinado a segurança da informação e uma representação média de 3,8% do gasto total do orçamento com a Tecnologia da Informação (TI).

Com um volume tão grande de ameaças e vulnerabilidades, juntamente com a criticidade dos dados a serem protegidos, surgem questionamentos sobre como criar uma equipe de profissionais de segurança para proteger e identificar as vulnerabilidades dos seus recursos, para diminuir os riscos e custos.

# 2 OBJETIVOS

Indagações do tipo: *Como identificar a necessidade de um Computer Security Incident Response Team (CSIRT)? E porque ter um Time de Tratamento de*

*Incidente de Segurança da Informação? Que resultados se pode esperar de um CSIRT?* São algumas das questões que motivaram o desenvolvimento deste trabalho.

# 3 FUNDAMENTAÇÃO TEÓRICA

"Para ser utilizada, a informação necessita garantir três características fundamentais: a integridade, a disponibilidade e a confidencialidade" (DANTAS, 2011), mas "adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas" no tratamento da informação (DANTAS, 2011).

Detalhando melhor a compreensão das características que compõem a informação o Comitê Gestor da Internet no Brasil (CGI.br) através de seu Núcleo de Informação e Coordenação do Ponto BR (NIC.br) Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) define:

> - "Identificação: permitir que uma entidade se identifique, ou seja, diga quem ela é.
> - Autenticação: verificar se a entidade é realmente quem ela diz ser.
> - Autorização: determinar as ações que a entidade pode executar.
> - Integridade: proteger a informação contra alteração não autorizada.
> - Confidencialidade ou sigilo: proteger uma informação contra acesso não autorizado.
> - Não repúdio: evitar que uma entidade possa negar que foi ela quem executou uma ação.
> - Disponibilidade: garantir que um recurso esteja disponível sempre que necessário.". (**CARTILHA DE SEGURANCA PARA INTERNET, 2012**)

Devido à diversidade de formas como a informação pode ser armazenada, apresentada e compartilhada, a variedade de ameaças e vulnerabilidades a qual está exposta torna-se algo preocupante para os responsáveis pela segurança da informação.

A Associação Brasileira de Normas Técnicas (ABNT) define segurança da informação como sendo "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o

retorno sobre os investimentos e as oportunidades de negócio.” (NBR ISO/IEC 27002:2005).

Diante das definições apresentadas é possível compreender que a segurança da informação visa a desenvolver estratégias e mecanismos para garantir a proteção da informação contra as ameaças mantendo suas qualidades e oferecendo maior confiabilidade ao ambiente dos negócios.

Uma estratégia bem aceita pelas empresas para cuidar das atividades relacionadas à segurança da informação é a criação de uma equipe especializada em tratamento de incidentes. Equipe esta chamada de Computer Security Incident Response Team (CSIRT) – em português, Grupo de Resposta a Incidentes de Segurança.

Segundo CERON (2014), CSIRT é “uma organização que responde a incidentes de segurança provendo suporte necessário para resolver ou auxiliar na resolução”. Podendo “desenvolver metodologias para proteger os sistemas e, na ocorrência de um evento arbitrário de segurança, esse grupo de pessoas pode prontamente interceder de forma efetiva” (CERON, 2014).

O conceito de um incidente de segurança da informação é apresentado por SISP (2015) como sendo ”um simples ou por uma série de eventos de Segurança da Informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação.”.

E por Evento de Segurança da Informação, ainda segundo SISP (2015), entende-se por uma “ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de Segurança da Informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a Segurança da Informação.”.

A Superintendência de Tecnologia da Informação e Comunicação da Universidade Federal do Rio de Janeiro (UFRJ/TIC, 2015) define incidente de segurança como “qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade”.

Para PALMA (2015) incidente é “qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de redes de

computadores”. Ainda segundo PALMA (2015), “em geral, toda situação onde uma entidade de informação está sob risco é considerado um incidente de segurança”.

## 3.1 RISCOS

Um conceito constantemente apresentado na segurança da informação é sobre o risco. Para o Instituto Brasileiro de Governança Corporativa (IBGC), risco ”trata-se da definição do conjunto de eventos, externos ou internos, que podem impactar os objetivos estratégicos da organização, inclusive os relacionados aos ativos intangíveis” (IBGC,2007).

Os riscos podem ser separados pela natureza das consequências que podem gerar. Alguns podem gerar consequências positivas e outras negativas diante da visão estratégica de uma organização.

> “Os que geram impacto negativo representam riscos que podem impedir a criação de valor ou mesmo destruir o valor existente. Os de impacto positivo podem contrabalançar os de impacto negativo ou podem representar oportunidades, que por sua vez representam a possibilidade de um evento ocorrer e influenciar favoravelmente a realização dos objetivos, apoiando a criação ou a preservação de valor” (COSO, 2007).

## 3.2 CSIRT PARA EMPRESAS

No ambiente empresarial é possível efetuar a contratação dos serviços de um CSIRT para atender a demanda de segurança da informação de uma organização. Estes CSIRTs que atendem a este nicho de mercado são chamados de CSIRT Comerciais e podem ser separados por seus ramos de atividade:os de atividades proativas e os de atividade de assistência às tecnologias de segurança da informação.

PRONER (2008) apresenta o grupo de CSIRT de atividades proativas como:

> “... especializados na resposta de incidentes e prestam serviço para àquelas organizações que o contratam. Há uma grande possibilidade de obter-se

> sucesso no tratamento de incidentes quando dentro da organização já exista uma equipe que cuide da segurança da informação. Caso essa equipe não exista o trabalho do grupo será muito maior e gastará mais tempo". (PRONER,2008).

Para o grupo de assistência, PRONER (2008) define que:

> "Muitas das organizações que vendem tecnologia como a Sun Microsystems, Microsoft, Hewlett Packard, etc. operam seus próprios grupos de resposta. Estes grupos não realizam todas as atividades comuns em um outro tipo de grupo. Elas geralmente limitam-se a analisar vulnerabilidades encontradas em seus produtos para então: documentar as características de vulnerabilidades; determinar as causas das vulnerabilidades; recomendar ações de reação; produzir atualizações; distribuir as atualizações; e analisar os prejuízos"( PRONER, 2008).

## 3.3 CSIRT PARA AMBIENTES ACADÊMICOS

A European Union Agency for Network and Information Security (ENISA), conceitua um CSIRT acadêmico como aquele que em suas atividades "presta serviços CSIRT a instituições acadêmicas e educativas, como universidades e centros de investigação, bem como aos ambientes Internet dos respectivos campi universitários" (ENISA, 2006).

No Brasil existe a Rede Nacional de Ensino e Pesquisa (RNP), que é uma organização social vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI) e pioneira como rede nacional de acesso à internet em território nacional. Seu principal objetivo são o desenvolvimento tecnológico e o apoio a pesquisas de tecnologia de informação e comunicação fornecendo uma infraestrutura de redes avançada e colaborativa às instituições públicas de pesquisa e ensino superior e tecnológico.

Os serviços de segurança da informação prestados pela RNP são realizados através do seu Centro de Atendimento a Incidentes de Segurança (CAIS), que foi o primeiro grupo de resposta da rede acadêmica brasileira e atua na resolução e prevenção a incidentes de segurança, além de promover boas práticas de segurança. Seus principais usuários são os Pontos de Presença (POPs), CSIRTs

acadêmicos, instituições governamentais, organizações parceiras e membros da comunidade de segurança e TI a nível nacional e internacional.

## 3.4 NOTIFICAÇÃO E MONITORAMENTO DE INCIDENTES

Uma instituição ao identificar um incidente de segurança da informação deve notificar os responsáveis e o centro de tratamento para contribuir com a melhoria da detecção, conter danos e prejuízos e alimentar dados e estatísticas que podem ajudar na formulação de melhores práticas de segurança e observar tendências.

Mas, o que deve ser notificado? Segundo o CERT.br (2015) em seu *white paper* Recomendações para Notificações de Incidentes de Segurança deve ser notificado qualquer adversidade que viole a política de segurança ou a política de uso da instituição. CERT.br (2015) recomenda a notificação dos eventos:

> - “tentativas, com ou sem sucesso, de ganhar acesso não autorizado a um sistema ou a seus dados (ex: varreduras, ataques de força bruta SSH);
> - interrupção indesejada de serviço (ex: ataque de negação de serviço);
> - uso não autorizado de um sistema (ex: site comprometido hospedando páginas de phishing, propagando malware ou infectado com bot para ataque a terceiros/envio de spam);
> - modificações em um sistema sem o conhecimento ou consentimento prévio de seu dono (ex: desfiguração de página);
> - sistemas desatualizados ou incorretamente configurados, permitindo abuso (ex: DNS recursivo aberto, NTP permitindo amplificação);
> - uso abusivo, em desrespeito à política de uso aceitável do provedor de serviço (ex: contratação de sistema em nuvem para uso malicioso).” (CERT.br,2015).

É importante fazer a notificação aos contatos corretos a fim de não atrasar ou não descartar os incidentes. A seleção dos contatos deve ser criteriosa afim de evitar que o responsável pela origem do incidente seja alertado.

Uma sugestão de responsáveis a serem notificados de acordo com o tipo de incidente é sugerido por CERT.br (2015):

- “ ***Scan*** **de redes, tentativas de ganhar acesso não autorizado, tentativa de exploração de vulnerabilidade para execução de código remoto:** utilizar o contato do responsável pela rede e/ou AS do qual o endereço IP, identificado nos *logs* do ataque, faz parte;
- **Página maliciosa em *website* não malicioso:** caso típico de página de *phishing* ou de página para *download*/execução de código malicioso, hospedada em *website* de natureza não maliciosa (ex: *sites* de notícias, de compras, de entretenimento, de governo etc.), mas que foi comprometido por atacante/fraudador. Utilizar o contato do responsável pela rede e/ou AS da qual o endereço IP do *website* faz parte e, se disponível, o contato do responsável pelo domínio;
- **Página maliciosa em *website* malicioso:** caso típico de página de *phishing* ou de página para *download*/execução de código malicioso, hospedada em *website* de natureza maliciosa, por exemplo, cujo nome do domínio se assemelha ao domínio da instituição referenciada na fraude e, em geral, registrado há pouco tempo. Neste caso NÃO se recomenda utilizar o contato de domínio (da URL da página) pois, provavelmente, é do próprio fraudador. Deve-se utilizar o contato do responsável pela rede e/ou AS do qual o endereço IP do *website* faz parte e o contato da entidade registradora do domínio (Registrar);
- **DNS mal configurado permitindo abuso:** caso típico de DNS recursivo aberto. Utilizar o contato do responsável pela rede e/ou AS do qual o IP do DNS faz parte. Se disponível, incluir o contato do administrador do DNS (em geral encontrado no registro SOA do DNS);
- **DNS malicioso hospedado em provedor de serviços (*rogue* DNS) ou DNS comprometido:** são dois casos típicos, um em que o fraudador instala servidor malicioso em infraestrutura de terceiros, em geral provedor de serviços de hospedagem ou de nuvem, e outro em que um servidor DNS legítimo é comprometido e sua configuração é adulterada para gerar respostas maliciosas (ex: respostas autoritativas para zonas que não são de sua administração). Em ambos os casos, recomenda-se utilizar o contato do responsável pela rede e/ou AS do qual o IP do DNS faz parte;
- **Ataque de negação de serviço (DDoS):** dependendo das características do ataque, pode não ser possível identificar e notificar seus responsáveis, de forma que uma análise minuciosa do incidente deve ser conduzida. Duas situações típicas são:
    - as evidências permitem identificar os IPs participantes, por exemplo, em ataque direto por *bots* sem *spoofing* de endereços.

Neste caso notificam-se os responsáveis pelas redes e/ou ASs dos quais os IPs atacantes (*bots*) fazem parte;

- não é possível a identificação dos IPs que originaram o ataque, por exemplo, em ataque indireto via requisições com endereço adulterado (*spoofing*) disparadas a serviços abertos/mal configurados, gerando amplificação contra terceiro (alvo do ataque). Recomenda-se notificar os responsáveis pelos computadores que foram abusados para gerar a amplificação, a fim de que corrijam as vulnerabilidades que possibilitaram o abuso pelo atacante (ex: DNS recursivo aberto, NTP permitindo "monlist", SNMP aberto, serviço CHARGEN ativo e aberto, rede permitindo *spoofing*, etc);

- **Vazamento de dados pessoais (PII):** caso típico de dados pessoais (ex: endereço *e-mail*, nomes de familiares, números de documentos, de conta bancária, de cartão de crédito, etc) divulgados na Internet e obtidos a partir de servidores ou redes comprometidos. Dependendo da natureza dos dados divulgados, devem ser notificados os contatos das redes (a rede de onde os dados foram extraídos e a rede na qual os dados foram publicados), os contatos de CSIRTs das demais instituições envolvidas (ex: bancos, operadoras de cartão de crédito etc.) e o contato do domínio do *site* usado para divulgação dos dados, desde que seja evidente que o domínio não é malicioso. ” (CERT.br, 2015).

# 4 METODOLOGIA

## 4.1 PLANEJAMENTO DE IMPLANTAÇÃO DO CSIRT

Para realizar a implementação do CSIRT no Centro Federal de Educação Tecnologica de Minas Gerais (CEFET-MG), foi analisado o documento recomendado pelo CERT.br que é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, originando uma sequência de passos, divididos em 5 fases. Estas fases, por terem objetivos claros, levam ao controle e implementação mais conscientes, o que permite s uma melhor gerência do projeto pela Instituição.

### 4.1.1 Fase Pré-Inicial

Nesta fase é realizada a coleta de informações que serão utilizadas na fase de Planejamento contribuindo para a melhor adequação do CSIRT para com as normas da empresa, os padrões e melhores práticas. Permite efetuar um comparativo da eficiência no tratamento de incidentes pré e pós CSIRT.

Algumas das informações a serem analisadas são:

- levantamento e detalhamento dos processos, procedimentos operacionais, fluxo de informações, tecnologias e requisitos regulatórios existentes;
- organogramas da empresa e de unidades de negócio específicas;
- topologias de redes e sistemas da organização ou da comunidade que será atendida;
- inventários dos sistemas e recursos críticos;
- planos existentes de recuperação de desastres ou de continuidade dos negócios;
- normas existentes para comunicar violações de segurança física;
- quaisquer planos de resposta a incidentes já existentes;
- quaisquer regulamentos institucionais existentes;
- quaisquer políticas e procedimentos de segurança existentes;
- número de incidentes reportados;
- tempo de resposta ou tempo de vida de um incidente;
- número de incidentes resolvidos com sucesso;
- informações fornecidas para a comunidade sobre assuntos relativos à segurança de computadores ou atividades em andamento;
- atenção às questões de segurança dentro da organização;
- técnicas de prevenção e práticas de segurança implantadas.

### 4.1.2 Fase De Planejamento

Nesta fase prevê-se a descrição dos objetivos do projeto, do escopo, e a criação de um Planejamento Estratégico, que deverá:

- Identificar a comunidade a ser atendida. A quem o CSIRT presta serviços e suporte?

- Definir a missão e os objetivos do seu CSIRT. O que o CSIRT faz para a comunidade a que ele atende?
- Selecionar os serviços a serem prestados à comunidade (ou a outros). Como o CSIRT dá suporte à sua missão?
- Determinar o modelo organizacional. Como o CSIRT é estruturado e organizado?
- Identificar os recursos necessários. Que pessoal, equipamentos e infraestrutura são necessários para operar um CSIRT?
- Determinar o modelo de financiamento do seu CSIRT. Como o CSIRT será financiado na sua fase de implantação e durante as fases de crescimento e manutenção a longo prazo?

### 4.1.3 Fase Comunicação

A comunicação é realizada em dois estágios. Uma durante a fase de planejamento e implantação direcionada às pessoas envolvidas no projeto, visando à conscientização e à equalização do conhecimento sobre o projeto e atuação. E o outro, pós fase de implantação que é voltada para a divulgação da operacionalização do CSIRT para a comunidade, gerentes envolvidos, interessados, entre outros.

### 4.1.4 Fase De Implantação

A fase de implantação é o momento de executar e operacionalizar o CSIRT. As ações descritas no Planejamento Estratégico serão realizadas da seguinte forma:

- Contratar e treinar o pessoal inicial do CSIRT.
- Comprar os equipamentos (caso seja necessário) e instalar a infraestrutura de rede necessária para dar suporte ao grupo.
- Desenvolver um conjunto inicial de políticas e procedimentos para o CSIRT, de maneira a dar suporte aos serviços.
- Definir as especificações para o seu sistema de acompanhamento de incidentes e implementá-los.

- Desenvolver recomendações e formulários para sua comunidade sobre como reportar incidentes.

### 4.1.5 Fase Avaliação E Monitoramento

Após a operacionalização do projeto, são coletadas informações durante o seu tempo de vida, de forma que possa haver um monitoramento do andamento e qualidade dos processos de tratamento dos incidentes e uma avaliação da atuação do CSIRT e sua viabilidade e efeitos no ambiente computacional da Instituição.

A seguir estão listadas ações que visam a coleta de dados:

- benchmarking com outros CSIRTs;
- discussões com representantes da comunidade sendo atendida;
- formulários de avaliação distribuídos periodicamente para os membros da comunidade;
- definição de critérios ou parâmetros de qualidade que podem utilizados por uma auditoria ou por um grupo externo para avaliar o time;
- número de incidentes reportados;
- tempo de resposta ou tempo de vida de um incidente;
- número de incidentes resolvidos com sucesso.

## 4.2 INSTALAÇÃO DO CSIRT

O processo de implantação do CSIRT iniciou-se com uma coleta de dados e informações do ambiente computacional do Departamento de Computação do CEFET-MG (DECOM) através de uma entrevista com funcionários. A entrevista teve como objetivo obter a visão da situação atual quanto aos processos administrativos e processos de organização da infraestrutura de segurança da informação existentes no DECOM.

A entrevista foi realizada pelos alunos do curso técnico do CEFET, tendo por base as orientações e perguntas apresentadas no Apêndice A sendo que as respostas da entrevista estão contidas no Apêndice B.

Com as informações coletadas iniciou-se a fase 2, Planejamento Estratégico, do projeto de implementação do CSIRT. Nesta fase buscou-se construir um modelo de plano estratégico, descrito no Apêndice D, que seja adequado ao CEFET-MG e que contenha algumas diretrizes, definição do escopo de atuação e expectativas, modelo organizacional, modelo de financiamento, com o objetivo de melhorar o entendimento dos envolvidos na implementação do CSIRT.

A fase 3 do projeto, que é referente à comunicação, foi subdividida em duas etapas. A primeira que envolveu a comunicação com os responsáveis pela implementação durante todas as fases do projeto e uma segunda etapa que será direcionada para interação e conscientização da comunidade, a ser realizada após a criação de toda a infraestrutura. Nesta fase, foi possível realizar a comunicação e envolvimento das pessoas que atuam diretamente na implementação do CSIRT.

A fase 4 (Implantação) e fase 5 (Avaliação e Monitoramento) do projeto não puderam ser realizadas na sua totalidade devido as eventualidades provocadas pela greve dos funcionários públicos federais e incompatibilidade entre horários disponíveis dos envolvidos no projeto, o que dificultou a busca pelos dados.

No monitoramento dos incidentes de segurança, fase 5, foi usado como método de pesquisa para identificação dos sistemas que estão invadidos ou vulneráveis, a busca pelo nome do domínio de rede do CEFET-MG em sites que armazenam informações sobre invasões, hackers, e em redes sociais.

A pesquisa consiste basicamente em procurar o nome do domínio do CEFET-MG (cefetmg.br) associado com palavras usadas pelos invasores para divulgarem suas ações, como hacked, defaced, tangodown, entre outras.

Na internet os invasores comumente publicam seus feitos através de portais de segurança ou repositório de informações que contêm notícias de guerras digitais, segurança de TI, fóruns, sites desfigurados- etc. Um desses repositórios é o Zone-H.

Neste repositório, quando uma informação de desfiguração de site é submetida, a equipe do Zone-H verifica se a informação é verdadeira, e disponibiliza provas da invasão através de prints das páginas, do ambiente etc.

A busca em seus arquivos é realizada através do endereço http://www.zone-h.org/archive/special=1. O site possui tradução em várias línguas, incluindo o português, que é acessível pelo endereço http://br.zone-h.org/archive/special=1.

Foi realizada uma pesquisa no dia 06/11/2015. Nesta pesquisa foi encontrado um histórico de invasões ocorridas no domínio do CEFETMG.BR desde o ano de 2001, conforme pode ser observado na Figura 1.

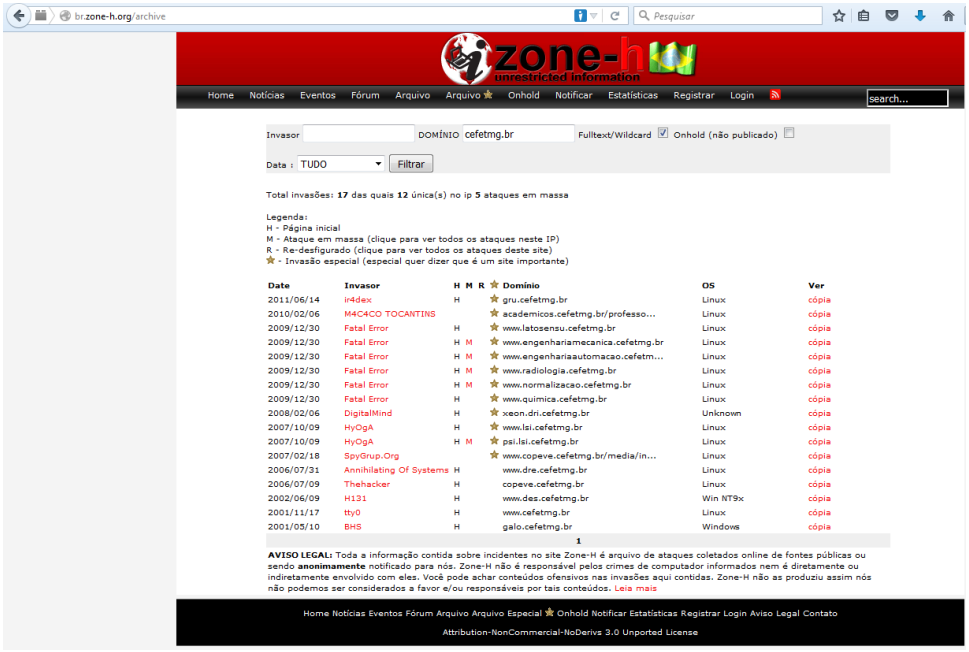


*Figura 1 – Histórico de invasões do domínio cefetmg.br no Zone-H*

Também foi identificado na seção de informações em análise para publicação, uma invasão mais recente, datada de 26 de setembro de 2015, conforme apresentado na Figura 2.

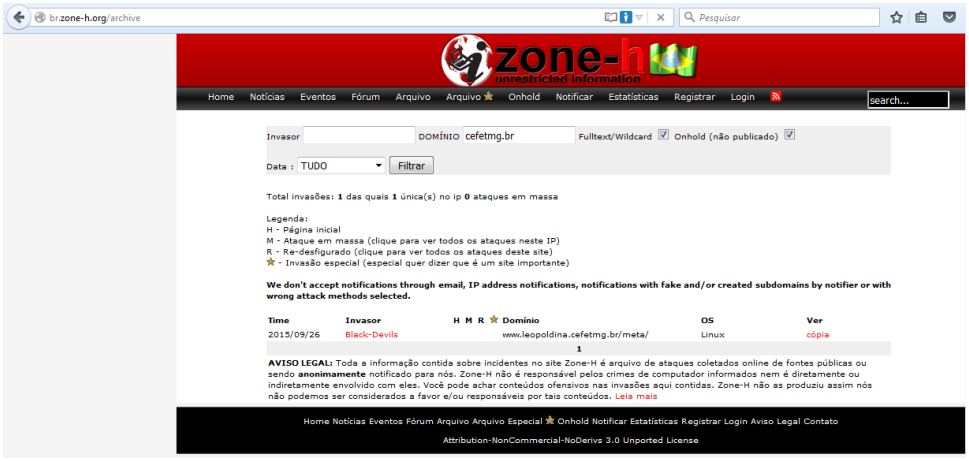


*Figura 2 - Consulta por domínio Cefetmg.br no Zone-H*

Outros portais de notícias de segurança com artigos, *screenshots* de sites hackeados, avisos de segurança e detalhes de vulnerabilidades mais recentes, foram usados para buscar informações referentes ao domínio CEFETMG.BR, tais como Xatrix, acessado através do endereço http://www.xatrix.org/defac.php?e=26 e o H4CK M1RROR acessado pelo endereço http://www.hack-mirror.com/search.html. Porém nestes portais, não foram encontradas evidências de invasão no domínio.

### 4.2.1 Analise Em Redes Sociais

#### *4.2.1.1 Facebook*

Além dos sites específicos para publicação de notícias de segurança da informação, é interessante também pesquisar nas redes sociais os perfis dos grupos de hackers. Um dos principais grupos é o Anonymous, que possui atuação internacional e em diversas frentes ativistas. No Brasil, o grupo possui alguns perfis no facebook acessados pelos endereços https://www.facebook.com/AnonHackBrazil2/?ref=br_rs , https://www.facebook.com/AnonymousHackerBrazil/?ref=br_rs , https://www.facebook.com/DkBrazilHackteam?filter=1 , https://www.facebook.com/AnonBRNews?fref=ts.

#### *4.2.1.2 Twitter*

O Twitter, por ser uma rede social que permite interação entre os usuários, através de mensagens com quantidade limitada de caracteres (140), é dinâmico, podendo as mensagens ser publicadas por softwares específicos, website etc.

A pesquisa por termos e palavras-chave utilizada pelos invasores, nos permite visualizar a notificação das atividades realizadas pelos principais grupos de hacker.

As pesquisas realizadas para este trabalho estão listadas no Apêndice C e possuem em sua sintaxe algumas palavras que estão relacionadas na Tabela 1.

*Tabela 1 – Palavras-Chave e Perfis utilizados por Hackers no Twitter*

| **Alguns Termos Usados por Hackers** | |
|---|---|
| **#anonymous** | **#tango** |
| **#tangodown** | **#hacked** |
| **#anonymous** | **#deface** |
| **#antisec** | **#ProtestoBH** |
| **#OpHacking** | **#ProtestoBR** |
| **#tangodown** | **#PrimaveraBrasileira** |
| **#down** | **#sambahack** |
| **Alguns Perfis do Twitter de Hackers** | |
| **@youranonnews** | **@AnonymousIRC** |
| **@theanonirc** | **@YourAnonNews** |
| **@anon_central** | **@HADESUnsekurity** |
| **@havittaja** | **@TheAnonyBay** |
| **@mindsector** | **@HighTech** |
| **@AnonHfg** | **@LulzSecBrazil** |
| **@AnonRio** | **@anonymousOIC** |

# 5 RESULTADOS

A coleta de informações, obtidas neste trabalho, anteriores à aplicação do CSIRT, possibilita a comparação com dados após sua implantação, o que permite verificar a evolução dos processos e a melhoria do ambiente em questões de segurança.

Os resultados da entrevista apresentada no Apêndice B demonstram uma fragilidade do DECOM quanto aos processos administrativos, recursos e processos de segurança da informação, além de uma defasagem na padronização dos processos operacionais.

O departamento não possui uma politica de segurança da informação própria, seguindo as normas da Secretaria de Governança da Informação do CEFET-MG (SGI) e também não possui uma politica de acesso por meio físico ao

ambiente computacional, que pode ser acessado por todos que frequentam o departamento, o que imprime uma dificuldade de identificação em caso de incidente.

Foi identificado que em seu ambiente computacional ficam hospedados a página virtual do CEFET-MG e o cluster de servidores, protegidos por um antivírus e um antispam, além de possuir serviços de *backup* para os servidores. As tomadas de decisão quanto aos aspectos de segurança são baseadas nas normas do SGI, que também é o setor informado em caso de incidente. A abertura do processo de comunicação de um incidente é realizada de maneira informal, o que dificulta a rastreabilidade e métrica dos registros dos incidentes de segurança.

Não há um sistema no DECOM que realize os registros e métricas de incidentes de segurança e também não há prazo determinado para atendimento dos mesmos pelo SGI. Tampouco existe documentação para o fluxo de informação, plano de continuidade ou recuperação, ocasionando maior probabilidade de atraso na recuperação do ambiente em caso de incidentes.

Em caso de ocorrência de incidentes que indisponibilizem os sistemas hospedados no DECOM, o departamento não possui plano de comunicação com a comunidade usuária dos serviços.

Uma das contribuições deste trabalho foi a estruturação de um método de busca por incidentes de segurança da informação em ambientes externos ao CEFET-MG, através do cruzamento de palavras-chave comumente utilizadas pelos hackers para divulgação dos seus ataques com palavras relacionadas ao domínio CEFET-MG. No item 4.2 e no Apêndice D são apresentados exemplos de endereços eletrônicos que podem ser consultados periodicamente para monitoramento de invasões nos sistemas hospedados no DECOM.

Outra contribuição foi a elaboração de um modelo de Plano Estratégico para ser utilizado pelo CSIRT com o objetivo de orientar e documentar as atividades e processos de segurança do DECOM. A estruturação mais detalhada do Plano Estratégico é apresentada no Apêndice D.

# 6 CONCLUSÃO

A partir deste trabalho conclui-se que o DECOM necessita aprimorar os processos relacionados à segurança da informação e sistematização dos processos operacionais.

Foi observado que nas atividades de monitoramento de incidentes é necessária a contínua atuação da equipe responsável por um período de, no mínimo, seis meses a um ano. Pois assim é possível a captura de incidentes que possuem sazonalidade, ou seja, acontecem em períodos específicos.

A importância de um CSIRT fica evidenciada pelo histórico de invasões ocorridas desde o ano de 2001 ao ambiente do CEFET-MG, que foi identificado através da pesquisa realizada em meios externos ao da Instituição.

A estruturação do Plano Estratégico mostrou-se fundamental para delinear as atividades e estratégias utilizadas pelo CSIRT, de forma a otimizar e conscientizar a comunidade da importância da sua implementação e melhor adequação aos objetivos estratégicos da instituição.

Visando a continuidade do projeto propõe-se:

- Mapear o fluxo de comunicação entre o DECOM e a comunidade.
- Constituir uma equipe de segurança composta por no mínimo dois alunos do ultimo e dois do penúltimo ano dos cursos técnicos do CEFET-MG, de forma que sempre haja um repasse de conhecimento das atividades para os novatos. Isso possibilitará um aumento no tempo de vida do CSIRT, além de oportunizar aos alunos um ambiente de ensino e aprendizagem.
- Criar modelos de documento para comunicação de incidentes a partir das sugestões do CERT.br em sua publicação Recomendações para Notificações de Incidentes de Segurança, disponível pelo endereço < http://www.cert.br/docs/whitepapers/notificacoes/>, buscando a melhoria da documentação e rastreabilidade dos incidentes.
- Fazer o monitoramento do tráfego nos principais equipamentos da rede através de ferramentas de monitoração da rede - como PRTG, DUDE, entre outros – com o objetivo de obter uma visão do consumo dos recursos, contribuindo para a identificação de incidentes de segurança através das variações dos indicadores.
- Efetuar o monitoramento das possíveis vulnerabilidades no ambiente da rede interna, coletando as informações de um software de

inventário de computador. O que possibilitará ter uma visão dos softwares e equipamentos que estão mais defasados e mais pré-dispostos a sofrer avarias de acordo com a sua utilização.

- Utilizar ferramentas de correlacionamento de eventos para detecção de ameaças de segurança da informação no ambiente computacional do DECOM. Um exemplo dessas ferramentas é Open Source Security Information and Event Management (SIEM) – OSSIM, da AlienVault.

# 7 REFERÊNCIAS BIBLIOGRÁFICAS

**CARTILHA DE SEGURANCA PARA INTERNET**, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acessado em:

CERON, João. **Tratamento de Incidentes de Segurança**/ João Ceron. – Rio de Janeiro: RNP/ESR, 2014. 208 p. :il. ; 27,5 cm.

CERT.br. **Recomendações para Notificações de Incidentes de Segurança.** Versão: 1.0 -- 09/06/2015. Disponível em: <http://www.cert.br/docs/whitepapers/notificacoes/>. Acessado em: 15 de outubro de 2015.

COSO (2007) - Committee of Sponsoring Organization of the Treadway Commission. **Gerenciamento de Riscos na Empresa – Estrutura Integrada: Sumário Executivo.** Disponivel em: <http://www.coso.org/documents/coso_erm_executivesummary_portuguese.pdf>. Acessado em: 15 dezembro de 2015.

DANTAS, Marcus Leal. **Segurança da informação: uma abordagem focada em gestão de riscos.** / Marcus Leal Dantas. – Olinda: Livro Rápido, 2011.

ENISA, Agência Europeia para a Segurança das Redes e da Informação. **Abordagem gradual de criação de um CSIRT.** Versão WP2006/5.1 (CERT - D1/D2). 2006

IBGC - Instituto Brasileiro de Governança Corporativa. **Guia de orientação para o gerenciamento de riscos corporativos / Instituto Brasileiro de Governança Corporativa**; coordenação: Eduarda La Rocque. São Paulo, SP: IBGC, 2007 (série de cadernos de governança corporativa, 3).

NBR ISO/IEC 27002:2005. **Associação Brasileira de Normas Técnicas (ABNT). – Tecnologia da informação – Código de prática para a gestão da segurança da informação.** Rio de Janeiro: ABNT, 2005. Disponível em: <http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf>. Acessado em: 12 de setembro de 2015.

PALMA, Fernando. **Incidentes de Segurança da Informação: conceito, exemplos e cases.** Portal GSTI. Disponível em: <http://www.portalgsti.com.br/2014/01/incidentes-de-seguranca.html>. Acessado em: 17 de maio de 2015.

PRONER, Lucas Fabiano. Uma proposta de Modelo de CSIRT para o BESC. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas. 2008. Joinville, SC. Disponível em: <http://pergamum.udesc.br/dados-bu/000000/000000000009/000009C6.pdf>. Acessado em: 15 de maio de 2015.

PWC. **Pesquisa Global de Segurança da Informação 2014**.Disponível em: <https://www.pwc.com.br/pt_BR/br/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf>. Acessado em: 07 de maio de 2015.

ROHR Altieres. **Brasil é 8° país em ranking de origem de ataques cibernéticos.** Portal G1. Tecnologia e Games. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/04/brasil-e-8-pais-em-ranking-de-origem-de-ataques-ciberneticos.html>. Acessado em: 07 de maio de 2015.

SISP. **Segurança da Informação: Tratamento de Incidentes.** Disponível em: <http://www.sisp.gov.br/faq_segurancainformacao/one-faq?faq_id=13972023>. Acessado em: 17 de maio de 2015.

TNONLINE. **Incidentes de segurança na Internet crescem 197% no Brasil.** Disponível em: <http://tnonline.com.br/noticias/geral/58,328568,11,04,incidentes-de-seguranca-na-internet-crescem-197-no-brasil.shtml?refresh=true>. Acessado em: 07 de maio de 2015.

UFRJ/TIC. **Incidentes de Segurança da Informação.** Superintendência de Tecnologia da Informação e Comunicação da Universidade Federal do Rio de Janeiro. Disponível em: <http://www.tic.ufrj.br/index.php/o-que-sao-incidentes>. Acessado em: 17 de maio de 2015.

# 8 APÊNDICE

## 8.1 APÊNDICE A

Fase Pré-Inicial

Nesta fase é realizada coleta de informações que serão utilizadas na fase de planejamento contribuindo para a melhor adequação do CSIRT para com as normas da empresa, os padrões e melhores práticas. Permite efetuar um comparativo da eficiência no tratamento de incidentes pré e pós CSIRT.

1. Levantar e detalhar os processos, procedimentos operacionais, fluxo de informações, tecnologias e requisitos regulatórios existentes.

*Verificar se o DECOM e o CEFET-MG possuem alguns dos itens acima citados.*

2. Organogramas da empresa e de unidades de negócio específicas.

*Identificar o organograma do DECOM e do CEFET-MG. No organograma do CEFET-MG, caso seja necessário, destaque a posição do DECOM.*

*(Importante para identificarmos a hierarquia e os órgãos que devem ser comunicados de acordo com a criticidade e o contexto dos incidentes)*

3. Topologias de redes e sistemas da organização ou da comunidade que será atendida.

*Identificar os principais ambientes de rede, servidores com serviços importantes. Quem é atendido por estes serviços? (funcionários, estudantes, público geral).*

4. Inventários dos sistemas e recursos críticos.

*Listar os principais sistemas críticos para o DECOM e o CEFET-MG. Quais sistemas causam mais impacto em uma indisponibilidade?*

5. Planos existentes de recuperação de desastres ou de continuidade dos negócios.

*Existe algum plano de continuidade? Existe plano de recuperação dos sistemas críticos?*

*Quando acontece algum problema, qual o nível de interrupção do serviço?*

*(Existem políticas de Backups, arquivos com configurações salvas? Armazenamento de log para auditoria?)*

6. Normas existentes para comunicar violações de segurança física.

*Existe política de acesso físico ao ambiente do CEFET-MG? Ao DECOM? Ao ambiente dos servidores? A política de acesso é única? Como é realizada a comunicação em caso de uma violação? Quem avalia?*

7. Quaisquer planos de resposta a incidentes já existentes.

*Existe algum plano de resposta a incidentes? O que acontece quando há um incidente? Quem é comunicado? Como se dá essa comunicação? Isso é registrado e é de conhecimento geral?*

8. Quaisquer regulamentos institucionais existentes.

*Quais são os documentos que regulamentam as atividades do CEFET-MG e do DECOM? Quem pode acessar estes regulamentos?*

9. Quaisquer políticas e procedimentos de segurança existentes.

*Existe algum documento de segurança de informação no DECOM? No CEFET-MG?*

10. Número de incidentes reportados e número de incidentes resolvidos com sucesso.

*Existe alguma métrica quanto a quantidade de incidentes reportados, identificados, resolvidos etc.?*

*Como são identificados os incidentes?*

*Existe algum sistema que cataloga estes incidentes?*

11. Tempo de resposta ou tempo de vida de um incidente.

*Tentar identificar o tempo de resposta. Quando há um incidente tem que comunicar quem? Quando começa a atuação? Há algum prazo? Ficam pessoas de disponíveis (plantão) para caso aconteça algum incidente?*

12. Informações fornecidas para a comunidade sobre assuntos relativos à segurança de computadores ou atividades em andamento.

*Há alguma comunicação com relação à segurança? Como ela é feita?*

13. Atenção às questões de segurança dentro da organização

*Há uma preocupação com a segurança? Como estas questões são tratadas? Tem alguma prioridade no tratamento?*

14. Técnicas de prevenção e práticas de segurança implantadas.

*Existe alguma prática de prevenção? (Anti vírus, antispam, atualizações constantes de sistemas operacionais dos servidores e de computadores dos usuários finais? Etc)*

*Nas tomadas de decisões de uma implantação de um sistema ou para manutenção segue-se alguma melhor prática de segurança?*

Para ficar melhor organizado, criem tabelas com as informações. Tentem montar mais perguntas para fazer uma entrevista melhor de acordo com o conhecimento de vocês e com o que surgir na hora ao conversar com o funcionário do DECOM. Registrem as perguntas em tabelas, documentos para poder ser anexado ao final na monografia.

## 8.2 APÊNDICE B

**Procedimentos, regras e implantações do sistema**

**1 - O DECOM possui padronização de processos e procedimentos operacionais relacionados ao fluxo de informações? Como é feita essa padronização?**

*O DECOM não possui padronização nenhuma dos processos ou procedimentos relacionados ao fluxo de informações.*

**2 - Quais são os documentos que regulamentam as atividades do DECOM? Quem pode acessá-los?**

*Não há documentação para regulamentação das atividades do DECOM.*

**3 - Qual a política de acesso físico ao ambiente do DECOM? Como é feita política de acesso físico ao ambiente dos servidores? Como é realizada a comunicação no caso de uma violação?**

*Não há politica de acesso físico: qualquer um pode acessar os prédios do departamento. Os laboratórios são vigiados pelos próprios bolsistas ou coordenadores de laboratório. No caso de violação, o chefe de departamento é acionado.*

**4 - Existe algum sistema de métrica quanto à quantidade de incidentes reportados, identificados, resolvidos etc.?**

*Não existe sistema de métrica em relação aos incidentes.*

**5 - Existem políticas e procedimentos de Segurança da Informação no DECOM? Se sim, quais?**

*Não há politicas de SI no DECOM. Algumas regras da Secretaria de Governança da Informação (SGI) do CEFET-MG são seguidas.*

**6 - Existem práticas de prevenção (Antivírus, Firewall, AntiSpam, etc.)? Quais? Nas tomadas de decisões para implantações no sistema, seguem-se práticas de segurança?**

*O departamento conta com um anti-vírus e anti-spam para o domínio decom.cefetmg.br. Nas tomadas de decisão senguem-se as práticas da SGI.*

**7 - Existe algum plano de resposta a incidentes? O que acontece quando há um incidente? Isso é registrado e é de conhecimento geral?**

*Não há planos de resposta a incidentes de segurança. Quando ocorre alguma coisa, a SGI é acionada através de uma conversa informal: não há documentação, os incidentes não são registrados e não há preocupação em alertar os usuários da rede.*

**8 - Existe um time de especialistas disponíveis para resposta aos incidentes? Há um prazo para lidar com um incidente, depois de identificado?**

*O time que lida com os incidentes é a equipe do SGI, entretanto, eles não são especialistas dedicados a essa função. Não há prazos para lidar com os incidentes.*

**9 - Existe algum plano de continuidade? Existe plano de recuperação dos sistemas críticos? Quando acontece algum problema, qual o nível de interrupção de serviço? Existem políticas de backups e logs? Como são feitas?**

*Existe apenas o serviço de backup. Além disso, não há planos de continuidade ou recuperação, visto que não há documentação regulamentadora do departamento.*

**10 - Há algum plano de comunicação com os usuários em relação à segurança da informação? Como ele é feito?**

*Não há plano de comunicação com os usuários.*

**Infraestrutura da rede do DECOM:**

**11 - O CEFET-MG possui um organograma do qual o DECOM faz parte? O DECOM possui um organograma interno?**

*O CEFET-MG possui um organograma que coloca o DECOM subordinado à diretoria do CAMPUS II. O DECOM possui seu organograma próprio disponível no site do departamento.*

**12 - Quais são os sistemas mais críticos para a rede?**

*Os sistemas mais críticos para a rede são a página do CEFET-MG e o Cluster.*

**Obs: Se possível, gostaríamos de ter acesso ao desenho da infraestrutura da rede, contendo as divisões internas, os servidores, os terminais, o desenho do cabeamento estruturado, etc.**

*R: Devemos nos orientar através do organograma pois não temos acesso ao projeto de rede.*

## 8.3 APÊNDICE C

### Pesquisa na Rede Social Twitter

Relação das pesquisas realizadas no Twitter utilizando as palavras-chave e termos comuns usados por invasores de computadores e o domínio cefetmg.br.

Endereço de pesquisa que busca as publicações que possui relação com as palavras-chave cefetmg.br, hacked e defaced.

- https://twitter.com/search?f=tweets&q=.cefetmg.br%20hacked%20OR%20defaced&src=typd.

Endereço de pesquisa para acompanhamento das publicações relacionadas a um dos principais grupos de Hackers do mundo.

- https://twitter.com/search?q=%23anonymous%20OR%20%23tangodown&src=typd

Endereço de pesquisa para acompanhamento das publicações relacionadas a um dos principais grupos de Hackers do mundo e sua relação com o domínio Cefetmg.br.

- https://twitter.com/search?f=tweets&q=cefetmg.br%20%23anonymous%20OR%20%23tangodown&src=typd

Endereço de pesquisa para acompanhamento das publicações relacionadas ao domínio Cefetmg.br.

- https://twitter.com/search?q=cefetmg.br&src=typd

Endereço de pesquisa para acompanhamento das publicações relacionadas ao domínio Cefetmg.br e alguns dos principais termos e perfis de hackers.

- https://twitter.com/search?f=tweets&q=.cefetmg.br%20%23anonymous%20OR%20%23antisec%20OR%20%23OpHacking%20OR%20%23tangodown%20OR%20%23down%20OR%20%23tango%20OR%20%23hacked%20OR%20%23deface%20OR%20%23ProtestoBH%20OR%20%23ProtestoBR%20OR%20%23PrimaveraBrasileira%20OR%20%23sambahack%20OR%20%23ChangeBrazil%20OR%20%40youranonnews%20OR%20%40theanonirc%20OR%20%40anon_central%20OR%20%40havittaja%20OR%20%40mindsector%20OR%20%40AnonHfg%20OR%20%40AnonRio%20OR%20%40AnonymousIRC%20OR%20%40YourAnonNews%20OR%20%40HADESUnsekurity%20OR%20%40TheAnonyBay%20OR%20%40HighTech%20OR%20%40LulzSecBrazil%20OR%20%40anonymousOIC&src=typd

## 8.4 APÊNDICE D

Modelo de um Plano Estratégico para Criação de um CSIRT.

### 8.4.1 Plano Estratégico

#### *8.4.1.1 Introdução*

Nome do Projeto: Implementação de um CSIRT no CEFET-MG

Este documento define o plano estratégico para o projeto Implementação de um CSIRT no DECOM/CEFET-MG, no qual são documentadas estratégias para montagem, implementação e monitoramento dos incidentes no DECOM/CEFET-MG.

#### *8.4.1.2 Justificativa do projeto*

Com o intuito de identificar, controlar e monitorar os incidentes nos sistemas e rede de computadores do DECOM/CEFET-MG, busca-se, na implementação de um CSIRT a obtenção de dados e informações necessárias para resolver os incidentes de forma rápida e eficiente e dessa forma, contribuir para uma maior segurança da comunidade no uso dos sistemas e rede de computadores.

#### *8.4.1.3 Estratégia do projeto*

Desenvolver uma metodologia baseada nas melhores práticas, recomendações e padrões para implantação e monitoramento de incidentes de segurança da informação, de forma que possa identificar, monitorar e demonstrar a situação atual do DECOM/CEFET-MG.

#### *8.4.1.4 Plano de gerenciamento integrado do projeto*

##### *8.4.1.4.1 Objetivo*

O projeto tem por objetivo estabelecer métodos e ferramentas para identificar, solucionar e monitorar os incidentes de segurança da informação do DECOM/CEFET-MG.

*8.4.1.4.2 Escopo*

Serão produtos deste projeto: diretrizes para a implementação de um CSIRT, relatório com identificação, ocorrências e monitoramento de dados dos incidentes de segurança da informação, diretrizes para monitoramento dos incidentes, equipe para tratamento de incidente de segurança.

As diretrizes para a implementação de um CSIRT deverão conter orientações para coletar as informações dos incidentes, comportamento da equipe, o que fazer com os incidentes, como efetuar o monitoramento dos incidentes (monitoramento interno e externo ao DECOM), definição de perfis para equipe para tratamento de incidente de segurança.

O relatório com identificação, ocorrências e monitoramento de dados dos incidentes de segurança da informação deverá conter informações físicas do incidente (data e hora de criação, tempo de resolução, existência de indisponibilidade etc.), quantidades de ocorrências em um determinado tempo e informações que possam ser consideradas relevantes para análise.

8.4.1.4.2.1 Comunidade

O projeto visa a atender acomunidade do CEFET-MG que é formada por professores, funcionários técnico-administrativos e alunos, além de toda a comunidade mineira que necessite de usufruir dos serviços oferecidos.

8.4.1.4.2.2 Missão

A missão do CSIRT é desenvolver processos para que o tratamento dos incidentes de segurança da informação para que possam ser resolvidos com maior agilidade e eficiência, garantindo assim uma melhor qualidade e segurança no uso dos sistemas administrados pelo DECOM.

8.4.1.4.2.3 Serviços

Os serviços que podem ser prestados pelo CSIRT podem ser categorizados em 3 tipos, segundo o CERT/CC (Figura 3):

- Reativos - Os serviços reativos são concebidos para responder a pedidos de assistência, as notificações de incidentes na comunidade utilizadora CSIRT e a quaisquer ameaças ou ataques contra os sistemas CSIRT. Alguns serviços podem ser desencadeados por notificação de terceiros ou por monitorização e visualização ou por registos e alertas dos IDS (sistemas de detecção de intrusões).
- Proativos - Os serviços proativos são concebidos para melhorar a infraestrutura e os processos de segurança da comunidade de utilizadores antes de se registar ou de ser detectado qualquer incidente ou ocorrência. Os seus principais objetivos consistem em evitar incidentes e reduzir o seu impacto e extensão quando se registam.
- Gerenciais - Os serviços que se inserem nesta categoria não se esgotam na gestão de incidentes ou nas CSIRT. Trata-se de serviços bem conhecidos e estabelecidos, que visam melhorar a segurança geral de uma organização. Graças à experiência adquirida com a prestação dos serviços reativos e proativos acima descritos, uma CSIRT pode trazer a estes serviços de gestão da qualidade perspectivas únicas que de outro modo não estariam disponíveis. Estes serviços visam a tomada em consideração do feedback e dos ensinamentos adquiridos com a resposta a incidentes, vulnerabilidades e ataques. A integração destas experiências nos serviços tradicionais existentes (adiante descritos), no quadro de um processo de gestão da qualidade da segurança, pode melhorar os esforços de segurança a longo prazo numa organização. Consoante as estruturas e responsabilidades organizacionais, uma CSIRT pode prestar estes serviços ou participar num esforço organizacional de equipa mais vasto.

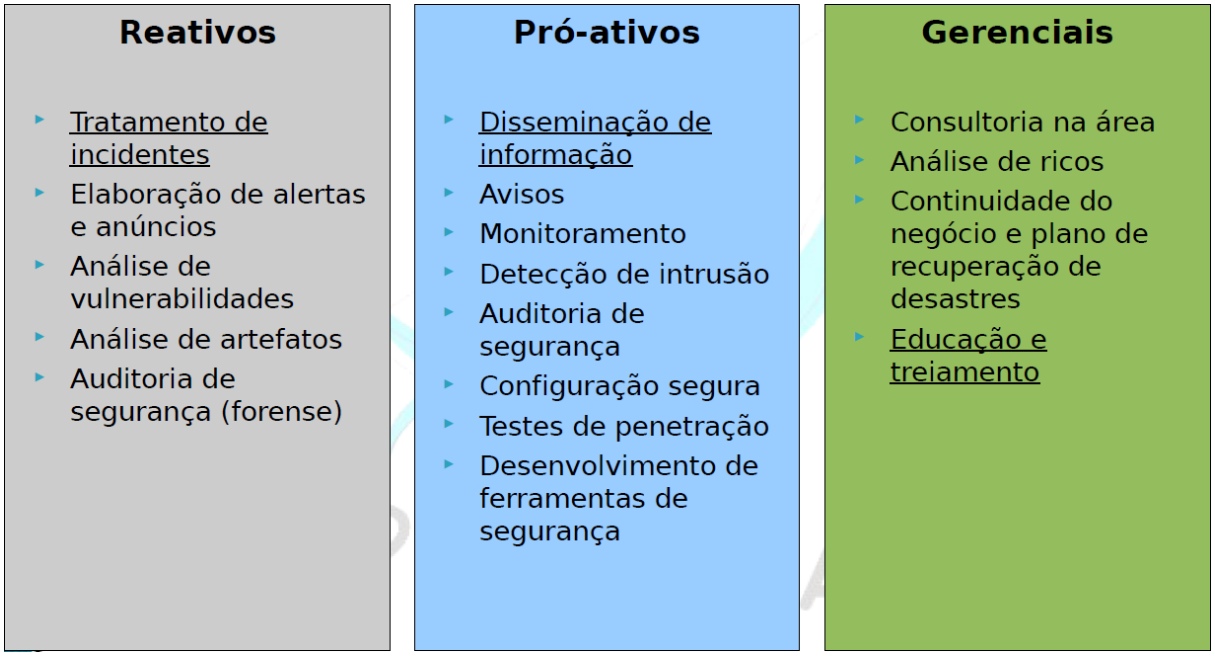


*Figura 3 - Tipos de serviços de um CSIRT*

Alguns serviços serão empregados a partir do momento que houver a maturidade e estabilidade do CSIRT na Instituição.

#### 8.4.1.4.2.4 Modelo organizacional

Um modelo proposto para o CSIRT/CEFET-MG é o de estrutura interna e centralizada, pois focará em prover suporte aos incidentes relativos aos serviços prestados pelo DECOM/CEFET-MG.

Este modelo permite um revezamento entre funcionários e servirá como ponto de contato da organização com os incidentes.

A posição hierárquica do CSIRT será a de unidade do DECOM, a princípio. À medida que o CSIRT obtiver maturidade, estuda-se a necessidade de mudanças.

#### 8.4.1.4.2.5 Recursos necessários

Os equipamentos a serem utilizados para operar o CSIRT serão do setor administrativo do DECOM.

Para operá-los, serão selecionados alunos do curso tecnológico de Redes do CEFET-MG e funcionários do DECOM.

Assim que for definida a equipe fixa, poderão ser oferecidos cursos de aperfeiçoamento sobre redes e segurança, visandoà melhoria na qualidade dos serviços prestados.

8.4.1.4.2.6 Modelo de financiamento

Os recursos do CSIRT serão financiados pelo DECOM/CEFET-MG em sua fase de implantação. À medida que houver maturidade e o CSIRT começar a expandir, deverá ser revisto o modelo de financiamento, bem como a sua estrutura para suportar os serviços em longo prazo.