[SEGURANÇA]

Resposta a Incidentes de Segurança - (PARTE 1)

por: Verdade @bsoluta
http://www.absoluta.org

Data do Documento: 17/03/2002
Ultima atualização: 31/03/20002
Palavras Chave: segurança, incidentes, resposta a incidente, procedimentos de segurança , análise forense
Autor: Verdade @bsoluta
Tradutor:
Arquivo: seg_resposta_incidente_1.htm
Status: completo

Comentários e correções são sempre bem-vindos.

Observação :
O assunto tratado neste texto tem por objetivo principal ajudar os administradores de rede no processo de definição de procedimentos para a resposta a incidentes de segurança, com sua modesta abrangência, este trabalho pretende servir como motivação ao leitor para busca de novos conhecimentos no campo da segurança da informação. Não houve aqui a pretensão de esgotar o assunto, mas sim fornecer ao leitor um texto condensado, reunindo conceitos fundamentais ao entendimento dos termos relacionados.

Boa leitura!

.....

Índice

0 - Homenagem

Antes de abordar o tema principal deste artigo, será feita uma simples homenagem a alguns dos heróis brasileiros, pessoas que lutaram por um Brasil melhor e para a formação de uma consciência dos nossos reais interesses fugindo da mesmice apresentada por políticos fracos, são elas:

- Paulo Freire - Um dos principais educadores que o pais já teve;
- Irmãos Villas Boas - Pela defesa da Nação Indígena;
- Berta Ribeiro - Pela defesa da Nação Indígena;

A estes brasileiros meus agradecimentos pela luta e exemplos deixado!

1 - Introdução

Toda sociedade em qualquer tempo, apresenta um certo percentual de criminosos. Felizmente este percentual é pequeno. Como estas sociedades possuem certas "limitações" para o deslocamento de átomos, a ação dos criminosos de uma sociedade dificilmente afeta outras.

Ex. o batedor de carteira de SP "não incomoda" a população de BsB.

Já na Internet este pequeno percentual toma dimensões graves pois não temos a barreira do tempo e do átomo, são milhares de criminosos transportando bits 24x7.

O número de usuários da Internet está por volta de 100 milhões (???), se admitirmos que menos de 1% destas pessoas praticam alguma forma de crime eletrônico temos um exército de aproximadamente 1 milhão de *crackers*, espalhados por todo o mundo, e relativamente organizados.

- Drogas;
- Pedofilia;
- Espionagem;
- Roubo de informações;
- Vandalismo;
- Colarinho branco;

São apenas alguns dos crimes cometidos utilizando-se computadores e as redes.

Como podemos observar são crimes antigos que utilizam-se de tecnologia para sua efetivação. Muitos destes crimes são previstos em legislação.

Desta forma torna-se urgente a adoção de procedimentos com o objetivo de responder a estes incidentes de forma efetiva, estas ações devem ser tomadas antes da ocorrência do eventos.

Devemos notar também que nem todo incidente de segurança pode ser caracterizado como crime, pois sua origem pode ser uma falha elétrica. Além disso, no direito penal o crime é produto de uma conduta contrária à lei penal, sendo expressamente prevista por ela. Essa conduta criminal pode consistir numa **ação** (doloso), quando o sujeito faz

alguma coisa, ou numa **omissão** (culposo), quando o sujeito deixa de fazer alguma coisa [1].

2 - Maturidade em Segurança

É possível fazer uma analogia entre a estrutura de segurança das redes com as ações militares. A figura-1 apresenta esta analogia de forma esquemática:

Fig. 1 - Maturidade em Segurança
http://www.absoluta.org

De forma genérica a base do sistema militar em situações de conflito é a estratégia de combate no qual são definidas as ações, recursos a utilizar, entre outros. Já nos sistemas de segurança de redes, a base deve ser a definição de uma política de segurança, que irá reger as estratégias a serem adotadas, os procedimentos, os níveis hierárquicos, a classificação de ativos, a classificação da informação, etc.

Em seguida, no sistema militar, temos as barreiras que têm por objetivo "conter" o avanço das tropas inimigas; paralelamente, nos sistemas de informação, temos os elementos de controle de conexão, tais como estruturas de *firewalls* (ACL em roteadores, programas para controle de conexão *statefull*, remoção de serviços desnecessários dos servidores). A tecnologia de*firewall* envolve vários conceitos e elementos e não iremos nos aprofundar em tal tema visto que existe literatura diversificada sobre o assunto.

A proxima camada é a observação do inimigo, movimentação das tropas, ações entre outros. Em nosso sistema de informação temos os sistemas de detecção de tentativas de intrusão, os IDS - *Intrusion Detection System*, estes sistemas "monitoram" o tráfego da rede e *hosts* com o objetivo de identificar padrões de ataque e tomar algumas ações de contra-resposta..

Na quarta camada dos sistemas militares temos as contra-medidas que são executadas em função das ações adotadas pelo inimigo. Nos sistemas de informação temos a resposta a incidente de segurança que envolve vários procedimentos, tais como: identificação do incidente, notificação das pessoas responsáveis, coleta e preservação de evidencias, rastreamento da origem, ações de contra-resposta. Estes e outros procedimentos serão abordados neste artigo.

Finamente temos o último estágio que nos sitemas militares corresponde à análise do inimigo, sendo representado pela espionagem, onde busca-se descobrir as técnicas e táticas que serão adotadas. Nos sistemas de informação o correspondente é o estudo do inimigo, que significa a implementação de *honeypots* para o estudo das ações e comportamento dos invasores com a finalidade de compreender sua mentalidade a fim de melhor proteger os sistemas críticos.

Como podemos observar, em nossa analogia, cada nível necessita dos serviços da camada anterior e provê serviços para a camada superior, como na pilha TCP/IP.

Desta forma, esta é uma das formas de mensurar a maturidade em segurança de uma instituição, ainda que não se trate de uma verdade absoluta e outras metodologias existam com abordagens relativamente diferentes e/ou complementares.

Podemos notar que um dos pontos básicos são as estratégias, nesta matéria podemos obter ajuda em literatura disponível, tais como:

- Sun Tzu (356-320 a.C.) - A Arte da Guerra;
- Nicolau Maquiavel (1469-1527);
- Napoleão Bonaparte (1793- 1815);
- Estratégias de xadrez;

Enfim sistemas que permitam o exercício da elaboração de ações planejadas.

3 - Definição de Incidente de Segurança

Inicialmente temos que ter em mente que a questão não é: "SE, mas QUANDO", ou seja, em algum momento teremos um incidente de segurança em nossa rede com um maior ou menor nível de gravidade, desta forma, faz-se necessário definirmos claramente o que é um incidente de segurança. Esta definição DEVE estar contida em nossa política de segurança, mas de forma genérica podemos classificar como incidente de segurança:

"*Invasões de computador, ataques de negação de serviços, furto de informações por pessoal interno e/ou terceiros, atividades em rede não autorizadas ou ilegais* " [4]

Desta forma, além de termos claramente definido o que é um incidente de segurança devemos estabelecer medidas de pré e pós incidente, ou seja, devemos estar preparados para a ocorrência de um incidente.

Entre as medidas **pré** incidentes podemos incluir:

- Classificação dos recursos a serem protegidos;
- Implementação de mecanismos de segurança;
- Definição de equipe multidisciplinar para atuar em caso de incidentes;
- Classificação dos incidentes quanto ao nível de gravidade;
- Elaboração da estrutura administrativa de escalonamento do incidente (do operador, passando pelos gerentes até o presidente);
- Montagem de *kit* de ferramentas para atuar em incidentes em plataforma diversas;
- Definição de procedimentos a serem adotados;

Entre as medidas **pós** incidentes podemos incluir:

- Procedimentos de coleta e preservação de evidências;
- Procedimentos de recuperação dos sistemas afetados;
- Procedimentos de rastreamento da origem;
- Elaboração de processo legal contra o causador do incidente;

Estes são alguns dos procedimentos/ações a serem adotados. O importante a observar é que a resposta a um incidente inicia antes da ocorrência do mesmo com a adoção de certos procedimentos.

4 - Detecção e Resposta Inicial

A detecção do incidente pode ser feita com os sistemas descritos nas camadas 1 e/ou 2 dafigura-1 , ou seja, através dos mecanismos de controle de conexão como, roteadores, sistemas de *firewalls* e/ou ferramentas de IDS, além destes mecanismos podemos ser alertados por usuários e/ou parceiros quanto ao mau funcionamento de determinadas aplicações e/ou suspeita de má utilização dos recursos.

Diversas são as formas de detecção de incidentes e o momento de ocorrência de um pode em alguns casos até ser prevista, por exemplo, após a notificação de uma vulnerabilidade em determinada aplicação anunciada pelo CERT [7], podemos ser alvo de tentativas de intrusão.

Após a identificação de um possível incidente devemos:

1. Confirmar a ocorrência do mesmo, de forma a evitar esforço desnecessário, ou seja, distingir entre falso-positivo e incidente real;
2. Registrar todas as ações tomadas;
3. Definir o nível de criticidade do incidente;
4. Identificar sistemas atingidos direta ou indiretamente;
5. Observar se o incidente continua em curso;
6. Acionar os especialistas necessários para a resposta ao incidente;
7. Notificar a gerência quanto ao estado do sistema, tempo estimado de recuperação e ações de contra-resposta;
8. Isolar os sistemas atingidos até a recuperação do mesmo e coleta das

evidências;

Devemos notar que ações de contra-resposta não significa bombardear a origem do ataque, caso tenhamos identificado a mesma, mas sim os procedimentos de preservação das evidências, recuperação do sistema. Esta questão é fundamental, pois realizar uma ação de "ataque" contra o agressor não é uma medida muito inteligente visto que:

1. Seu tempo será gasto com uma ação que poderá complicá-lo;
2. Você mostra ao agressor que o mesmo foi descoberto;
3. Estará utilizando os recursos de sua instituição de forma incorreta;
4. Estará contribuindo para a elevação do nível de lixo na Internet como um todo;

Os procedimentos mais recomendados são a discrição e ações para identificação da técnica utilizada para comprometer o sistema. Somente as pessoas certas devem ser notificadas, com informações claras do que ocorreu, as ações que estão sendo tomadas e os tempos estimados para normalização do sistema. Tratando-se de uma instituição comercial os gerentes estarão mais preocupados com a normalização dos negócios do que que com a identificação das origens, lembre-se no capitalismos tempo é dinheiro. Mas como um perito em crime eletrônico, você sabe que a normalização é apenas uma das fases do processo de resposta e, provavelmente, uma das mais simples e rápidas.

Todas as informações coletadas na fase inicial servirão de base para a elaboração da estratégia de acompanhamento e investigação do incidente. Esta estratégia deve contemplar aspectos técnicos e comerciais, a mesma deve ter a aprovação da direção da instituição, pois conforme o nível de gravidade do incidente não é justificável sua investigação. Algumas vezes, para o desespero dos especialista em crime eletrônico, a instituição decide simplesmente não continuar um processo de investigação com receio de manchar a imagem da instituição, esta visão deve ser mudada, todas as redes estão sujeitas a intrusão, e esconder a ocorrência de uma não ajuda a comunidade em nada. Lógico que não significa que a mesma deva ser tornada pública, mas sim que deve ser analisada com seriedade antes de tomar uma decisão quanto ao abandono das investigações.

5 - Medidas Pré Incidente

Como pudemos observar no item anterior a detecção de um incidente de segurança pode ser realizada de várias formas, mas uma das principais é através da monitoração contínua dos sistemas e conexões da redes à procura de desvio no padrão de funcionamento e/ou ações maliciosas.

Neste item iremos abordar alguns procedimentos fundamentais que irão facilitar e tornar mais ágil o processo de resposta. Para tanto é fundamental que tenhamos uma visão clara dos impactos que uma intrusão pode causar à continuidade dos negócios de nossa instituição, seja ela financeira, comercial, governamental ou educacional.

Cada instituição possui diferentes níveis de requisitos. Ademais ações classificadas como graves para uma instituição financeira podem ter menor impacto em uma

instituição acadêmica.

Por exemplo, um servidor WWW que disponibilize informações sobre o resultado do vestibular. Antes da apuração dos resultados, a indisponibilidade deste servidor pode até não ser percebida pela comunidade, mas na semana de divulgação dos resultados, torna-se crítica a indisponibilidade do mesmo. Já para uma instituição financeira a qualquer momento a indisponibilização dos servidores de Internet *Bank* torna-se crítico.

De modo a auxiliar no processo de mapeamento e pontuação do grau de criticidade dos recursos, segue alguns pontos que devem ser observados:

- Identificação dos ativos a serem protegidos:
  - Dados - Quanto à confidencialidade, integridade e disponibilidade;
  - Recursos - Quanto à má utilização, indisponibilidade, outros;
  - Reputação - Imagem, credibilidade, outros;

- Identificação dos possíveis atacantes:
  - Concorrentes;
  - Funcionários;
  - Ex-funcionários;
  - Pessoal terceirizado;
  - Visitantes;
  - Vândalos;
  - Espiões;

- Identificação dos tipos de ataque:
  - DoS;
  - Roubo de Informação;
  - Erros;
  - Acidentes;

- Classificação dos ativos quanto ao grau de impacto para o negócio, caso seja comprometido;

- Elaboração da documentação da rede e arquitetura atual, a documentação deve conter dados como:
  - Sistemas operacionais utilizados;
  - Versão do sistema operacional;
  - Fornecedor;
  - Serviços habilitados;
  - Responsáveis pelo sistema;
  - Outros dados.

- Definição dos ativos mais importante para a instituição;

- Existe plano de contigência para o caso da ocorrência de um incidente de segurança?;

- Definição de diretivas quanto ao monitoramento da rede e sistemas (e-

mail, sites acessados, programas utilizados);

- Definição de diretivas referentes à propriedade intelectual;

- Identificar instituições federais, internacionais e os profissionais especializados, bem como estabelecer acordo de cooperação.

Este é um procedimento importante para ações coordenadas, pois durante uma situação de crise o tempo de resposta é um fator crucial e se você já tiver os contatos estabelecidos com outras instituições sabe a quem procurar e principalmente em quem confiar. Abaixo estão algumas instituições que possuem equipes de resposta a incidente:

- Contato com órgãos federais:
  - FAPESP
  - RNP
  - DPF

- Contato com empresas privadas de BackBone:
  - EMBRATEL
  - Telecom em geral

- Contato com profissionais de segurança:
  - Eu
  - Mim
  - Frank Ned
  - ... :)

- Instituições Internacionais:
  - CERT
  - FIRST
  - I-4 (só Estados Unidos)

Mas não limite seus contados a estas instituições, procure administradores de outras redes, de provedores, enfim, monte uma relação de confiança com várias instituições, definindo chaves PGP, canais seguro de comunicação, telefone de emergência entre outros.

Os pontos relacionados acima auxiliam na identificação e classificação dos ativos quanto ao grau de importância para o negócio, bem como a identificação de possíveis grupos atacantes. Os fatores que levam a uma ação de intrusão são vários e os mesmos devem ser analisados de acordo com a realidade do negócio.

Devemos também definir uma estratégia de proteção dos ativos conforme o grau de criticidade do mesmo para a instituição, uma regra universal para definição dos investimentos é "o valor investido na proteção do ativo não deve ser maior que o valor do mesmo", na definição dos valores devemos levar em consideração fatores, tais como: tempo de recuperação, impacto ao negócio entre outros.

Nossa estratégia de proteção deve contemplar pontos como:

- Camadas de proteção:
  - Nível de rede;
  - Nível de *host*;
- Definição de níveis de privilégios
- Rastreamento / Identificação e Eliminação de pontos vulneráveis;
- Definir participação dos usuários:
  - Voluntária;
  - Obrigatória;

Outra característica da estratégia de proteção diz respeito à forma de implementação:

- Diversidade de soluções;
- Simplicidade da solução;

Cada abordagem possui pontos positivos e pontos negativos, sempre devemos ter em mente o grau de especialização de nossa equipe, os investimentos em qualificação, BONS salários para a equipe técnica de preferência compatíveis com os salários dos gerentes...:)).

Montar uma equipe de resposta a incidente não é tarefa fácil, desta forma devemos identificar dentro da instituição profissionais com diferentes perfis e acioná-los no caso de intrusão, estes profissionais devem antes passar por treinamento para familiarização dos procedimentos de resposta a incidentes e entendimentos das ações e hierarquias a serem respeitadas, ou seja, podemos ter uma equipe relativamente pequena de profissionais altamente especializados em resposta a incidentes, sendo que esta equipe sabe que pode acionar outros interlocutores internos ou até mesmo externo para o processo de resposta a um incidente de segurança, nossa equipe deve contar com profissionais multi-disciplinares e/ou com especialidade tais como:

- Criptografia;
- Banco de dados;
- TCP/IP;
- Firewall;
- IDS;
- Elementos de conectividade;
- Plataformas variadas;
- Estenografia;
- Estrutura de arquivos;
- Outras especializações;

Em conjunto com outros setores a equipe de resposta a incidente deve classificar os mesmos quanto:

- Gravidade;
- Prioridade;
- Valor do ativo;
- Técnica utilizada;
- Outros;

Esta equipe também é responsável entre outras funções pela elaboração de matrizes de valores que devem conter dados como:

- Histórico de eventos;
- Estatísticas:
  - Por hora;
  - Por dia;
  - Por tipo de evento;
  - Por número de ocorrência;
  - Por origem - destino;

Também é importante lembrar que uma equipe de resposta a incidente deve ter direito de acesso a setores, recursos e dados de forma a poder executar seu trabalho.

Deve estar claro a todos os envolvidos no processo a hierarquia de escalonamento, no caso da ocorrência de um incidente de segurança, ou seja, deve-se ter um interlocutor entre a equipe de resposta e a direção da instituição, em nenhum momento membros da equipe devem comentar as ações com outras pessoas, sobre o risco de comprometer a continuidade dos trabalhos, pois o incidente pode ter origem interna. Uma estrutura hipotética seria:

- Operador;
- Técnico de setor;
- Especialista;
- Gerente de área;
- Gerente de setor;
- Diretor de negócios;
- Presidente;

Lógico que cada instituição possui uma estrutura própria e o grau de escalonamento deve ser definido de acordo com a gravidade do incidente, pois não iremos notificar o presidente da instituição sobre *port scan* a todo momento que ocorrer um.

O objetivo neste ponto é deixar claro que o processo de resposta a incidente de segurança envolve várias pessoas, lógico que após a constatação de um incidente a equipe de resposta toma a frente das ações e o número de pessoas envolvidas reduz, o que é classificado como, isolamento de área, a partir deste momento somente pessoas autorizadas terão acesso as informações. Neste meio tempo nosso relações publica já deve estar passado para a direção de outros níveis o estado dos acontecimentos e elaborando memorandos internos e externos de esclarecimento, se for o caso.

Uma equipe de resposta a incidente deve possuir um conjunto de ferramentas e equipamento específicos para o tratamento de eventos, vamos supor que após o isolamento da área, seja encontrado no local do crime um disquete de 5 1/4, opa, você possui um *drive* de leitura para este disquetes...?

Até este ponto tratamos de medidas basicamente procedimentais, mas faz-se necessário um conjunto de medidas física, tais como:

- Elaboração de uma arquitetura de rede segura;

- Elevação do nível de segurança dos *hosts*;
- Monitoração contínua do tráfego da rede e dos serviços;
- Definição de testes periódicos à procura de vulnerabilidades;
- Definição de políticas de *backup* ;

Uma arquitetura possível é a apresentada na figura 2:

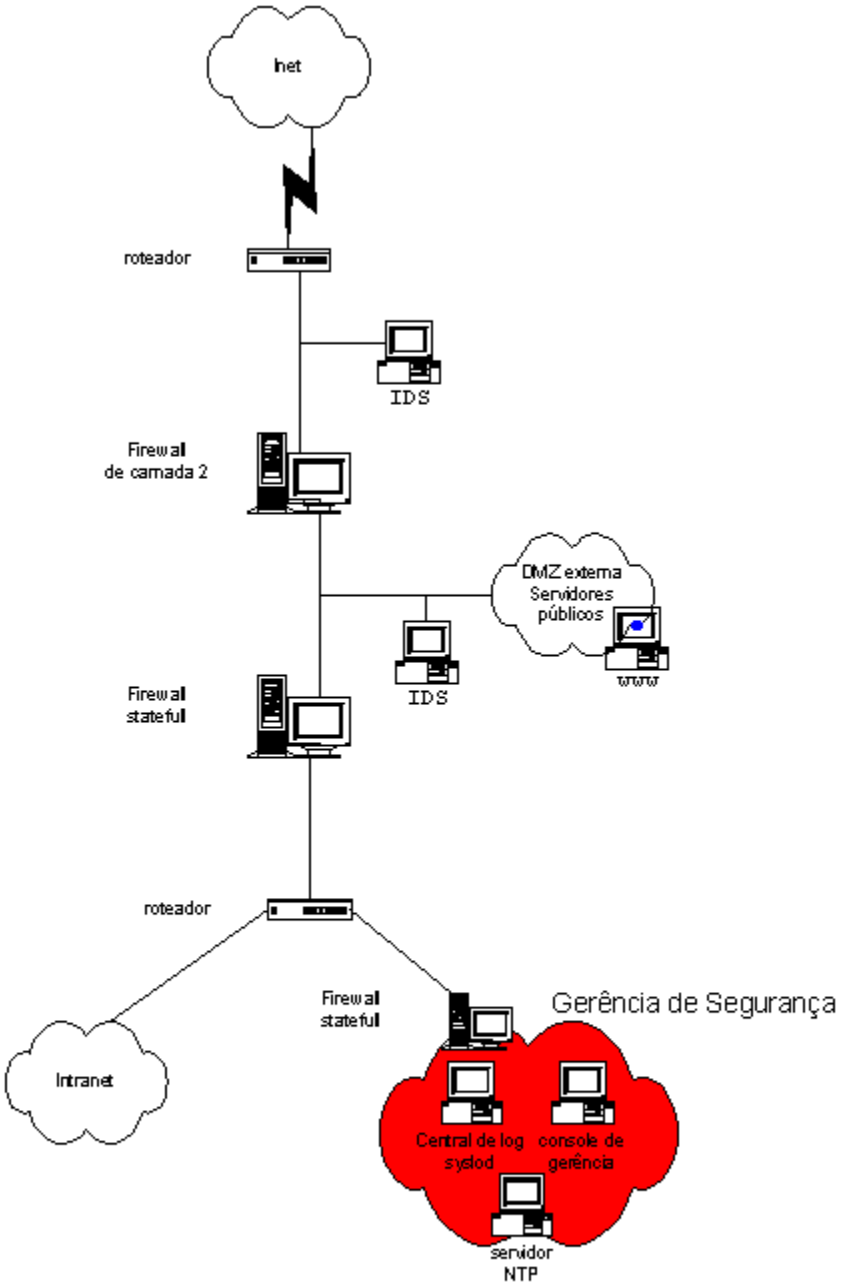

Figura 2 - Arquitetura de Rede Segura
http://www.absoluta.org

Na arquitetura apresentada os roteadores possuem ACLs - Lista de controle de acesso, sendo que os logs são enviados através de um canal seguro para o servidor de log localizado na rede de gerência da segurança. O *firewall* externo é um sistema de camada dois (*firewall bridigie*) desta forma é possível a implementação de filtros e o sistema

fica invisível na rede já que não possui IPs. Já o *firewall* interno é um sistema *stateful* que permite análise de todas as camadas do modelo OSI. Além disso, são colocados IDSs em segmentos estratégicos de forma a monitorar o tráfego na rede e seus eventos também são enviados para a rede de gerência. Nos servidores críticos são colocados IDS de *host* além de ser executado um *ckeck list* de segurança neste elementos removendo-se os serviços desnecessários, aplicando as correções de segurança, gerando MD5 dos arquivos principais do sistema, gerando cópia de segurança do sistema no estado inicial entre outros procedimentos. Implementamos também um servidor de tempo, NTP - *Network Time Protocol* de forma a manter sincronizado o horário de todos os ativos. E finalmente somente a partir da console de gerência pode-se acessar os recursos da rede para alterações de configuração, procedimentos de manutenção, etc.

Dependendo dos recursos disponíveis pode-se implementar o balanceamento de carga entre os sistemas de *firewall* de forma a prover redundância e melhor utilização dos recursos, para isso pode-se utilizar protocolos específicos como o VRRP (RFC-2338). Outros elementos de conectividade podem ser utilizados para elevar o nível de segurança da rede como *switchs* de camada 7, implementação de canais de VPN (IPSec), etc.

Não é o propósito deste artigo tratar sobre a implementação de redes seguras, mas este é um dos procedimentos recomendáveis, pois auxilia no processo de resposta a incidentes.

Nesta seção tratamos de aspectos referentes à elaboração da política de segurança, implementação de controles e sistemas de monitoração. Na questão política de segurança é bom lembrar que a mesma deve ser elaborada em conjunto com o departamento jurídico e o departamento de pessoal da instituição, se possível outros setores de decisão devem ser envolvidos.

A partir da próxima seção iremos focar na resposta a incidentes que corresponde ao nível 3 da figura-1 .

6 - O Processo de Resposta em Fases

A parte dois deste artigo será apresentada no mês de maio de 2002.

7 - Referencias

- **Livros / Revistas**
- [1] - Direito e Legislação - ISBN 8502-02054-4
- [2] - The Counter-Terrorism Handbook: Tactics, Procedures, and Techiniques - ISBN
- [3] - Forensic Pathology - ISBN
- [4] - Incident Response: Investigating Computer Crime - ISBN 0-07-213182-9
- [5] - Investigating Computer Crime - ISBN 0-8493-8158-4
- **Links**
- [5] - http://www.net.ohio-state.edu/security/talks.shtml - Forensic Computer Investigations

- [6]- http://www.aic.gov.au - Australian Institute of Criminology
- [7] - http://www.cert.org