UGB Centro Universitário Geraldo Di Biase

PROJETO DE REDES
www.projetoderedes.com.br

Auditoria e Análise de Segurança da Informação

Resposta a Incidentes de Segurança

Prof. José Maurício S. Pinheiro - UGB - 2009

Resposta a Incidentes de Segurança

Incidentes de Segurança

De acordo com CERT.br, um incidente de segurança pode ser definido como:

“Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores”.

Encaixam-se nessa definição todas as situações em que um sistema de informação está em risco (invasão de computadores, desfiguração do portal web, evasão de informações confidenciais e propagação de vírus).

Incidentes de Segurança

A gravidade de um incidente de segurança é medida de acordo com o impacto que ele causa no processo de negócio de uma empresa.

Todo incidente de segurança deve ser tratado através de uma metodologia previamente definida. Essa metodologia, conhecida como **Resposta a Incidentes de Segurança**, procura minimizar o impacto de um incidente e permitir o restabelecimento dos sistemas o mais rápido possível.

Incidentes de Segurança

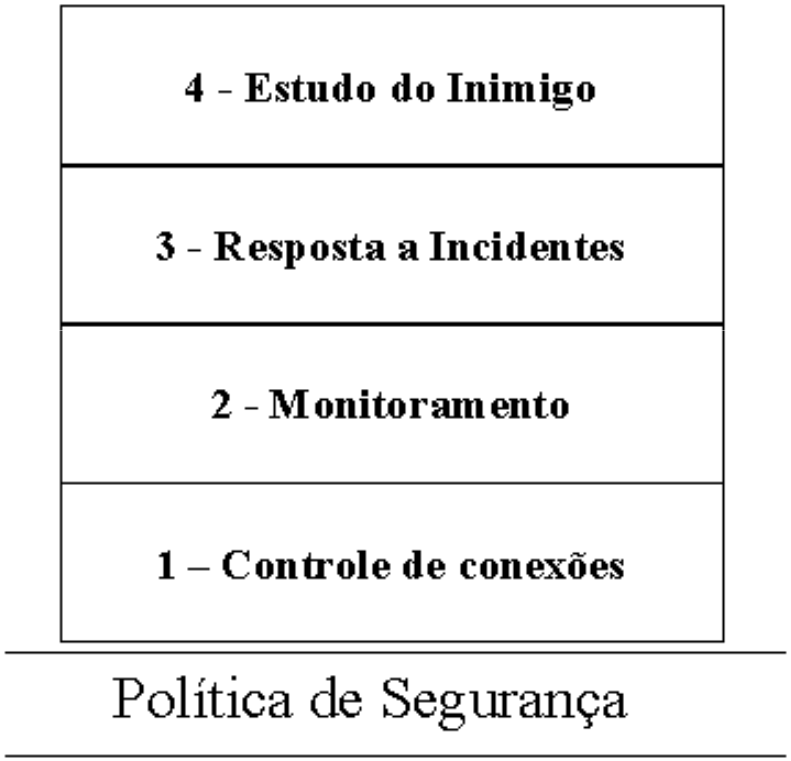
O CERT define Resposta a Incidentes de Segurança como:

“Uma metodologia organizada para gerir consequências de uma violação de segurança de informação”.

O processo de resposta a um incidente de segurança deve ser o resultado dos esforços de diferentes equipes organizacionais, agregando níveis gerenciais e técnicos.

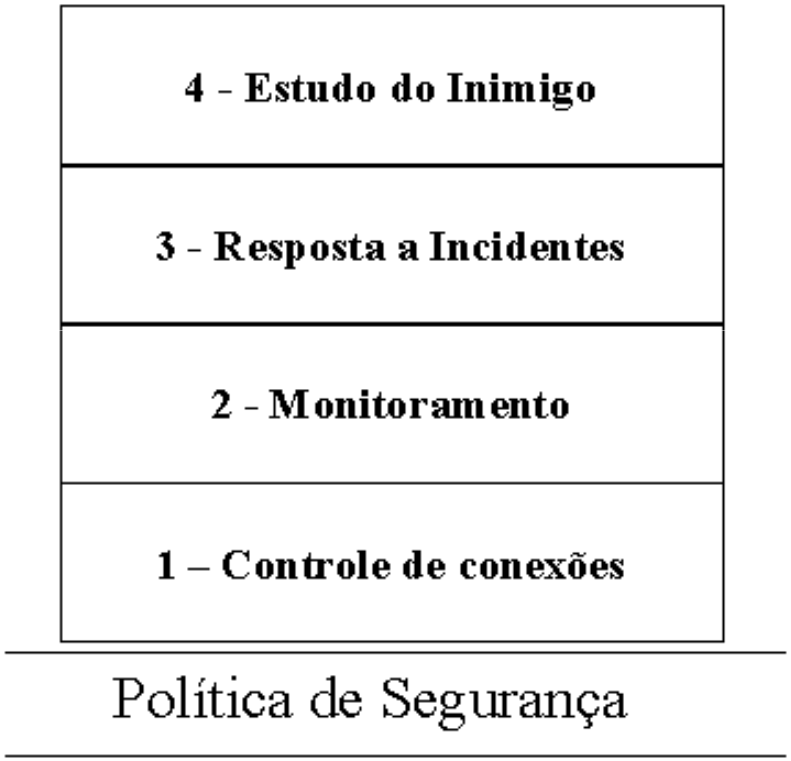
Monitoramento de Segurança em Camadas

Um sistema de gestão integrada de segurança é a base para se obter uma resposta eficiente a incidentes e está apoiado na definição de uma política de segurança em camadas, que irá reger as estratégias a serem adotadas, procedimentos, níveis hierárquicos, classificação das informações, etc.



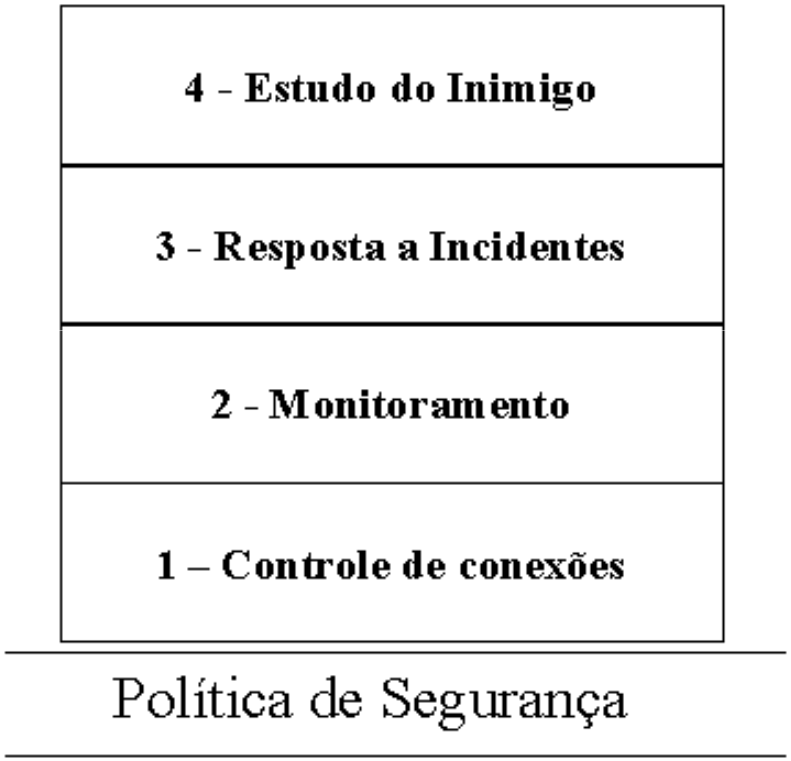
Monitoramento de Segurança em Camadas

Na camada **Controle de Conexões**, são inseridas barreiras com o intuito de conter as ameaças que podem ocasionar um incidente. Para tal, utilizam-se estruturas como firewalls, ACL em roteadores, programas de estado de conexão, anti-vírus, etc.



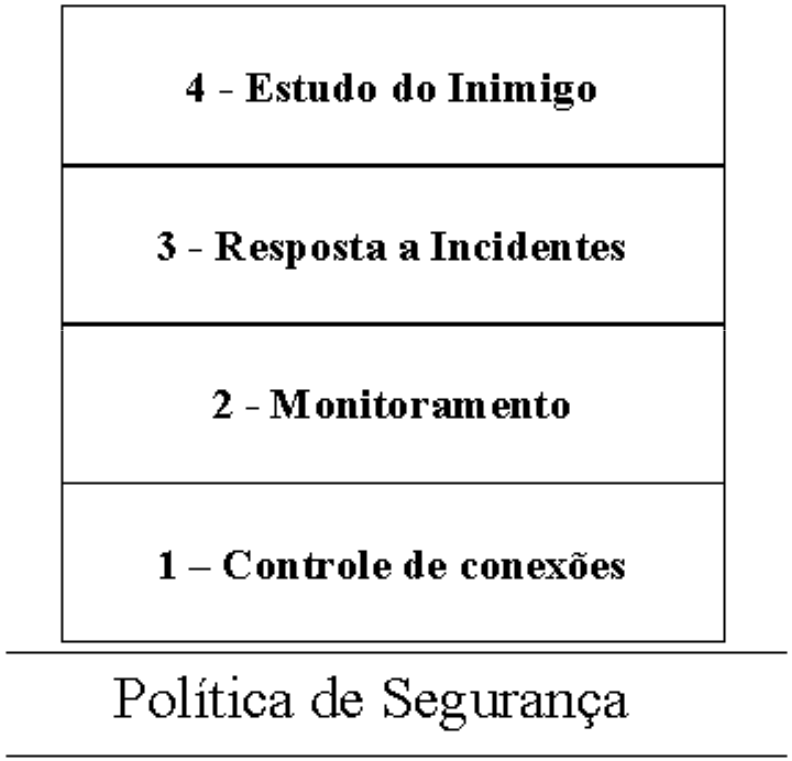
Monitoramento de Segurança em Camadas

Na camada **Monitoramento** ocorre a observação e detecção de tentativas de intrusão, os IDS - Intrusion Detection System, sistemas que monitoram o tráfego da rede e hosts com o objetivo de identificar padrões de ataque e tomar algumas ações de contra-resposta.



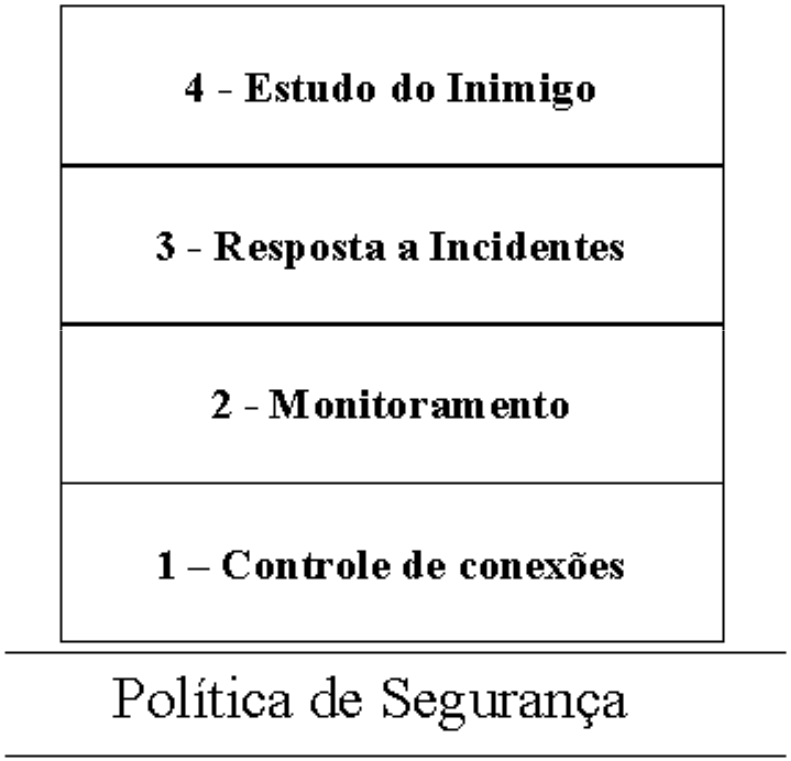
Monitoramento de Segurança em Camadas

A camada **Resposta a Incidentes** envolve vários procedimentos, tais como: identificação do incidente, notificação das pessoas responsáveis, coleta e preservação de evidencias, rastreamento da origem, ações de contra-resposta.

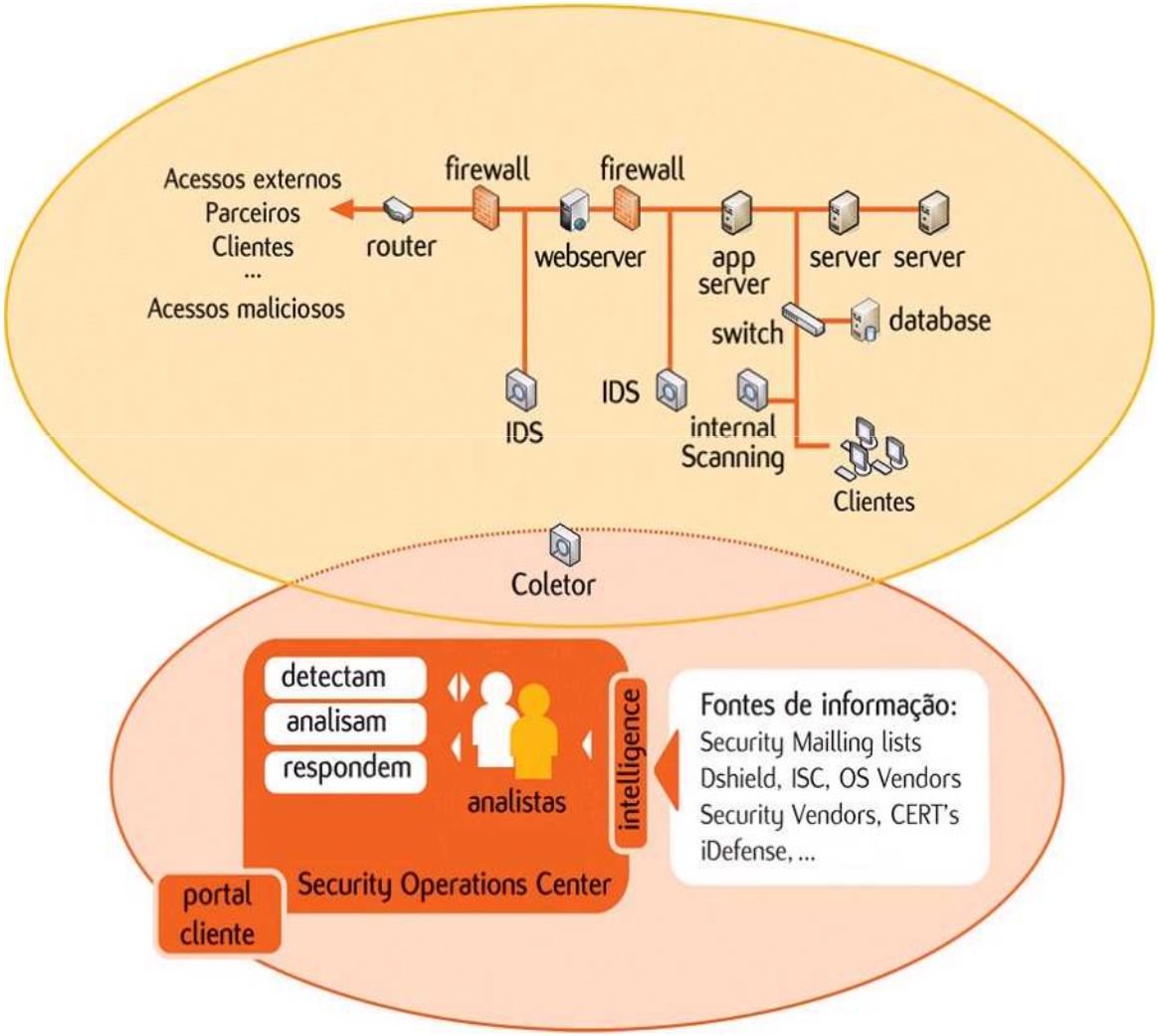


Monitoramento de Segurança em Camadas

Na camada **Estudo do Inimigo** temos o estágio em que se procura analisar o inimigo, buscando-se descobrir as técnicas e táticas que serão utilizadas. Utilizam-se *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.



Monitoramento de Segurança em Camadas



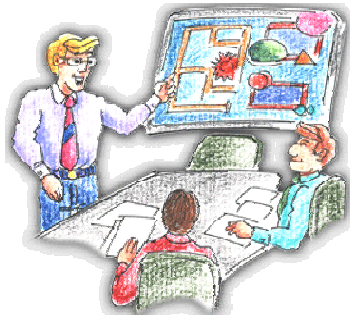
Um sistema de gestão de eventos de segurança realiza uma correlação integrada de eventos gerados de várias fontes, permitindo a análise no que realmente constitui uma ameaça efetiva.

Resposta a Incidentes de Segurança

Durante a preparação e planejamento da resposta a incidentes, não se deve perguntar SE um incidente ocorrerá, mas sim, QUANDO ele irá ocorrer, ou seja, sempre há a possibilidade de incidentes de segurança ocorrerem, com maior ou menor grau de gravidade.

Resposta a Incidentes de Segurança

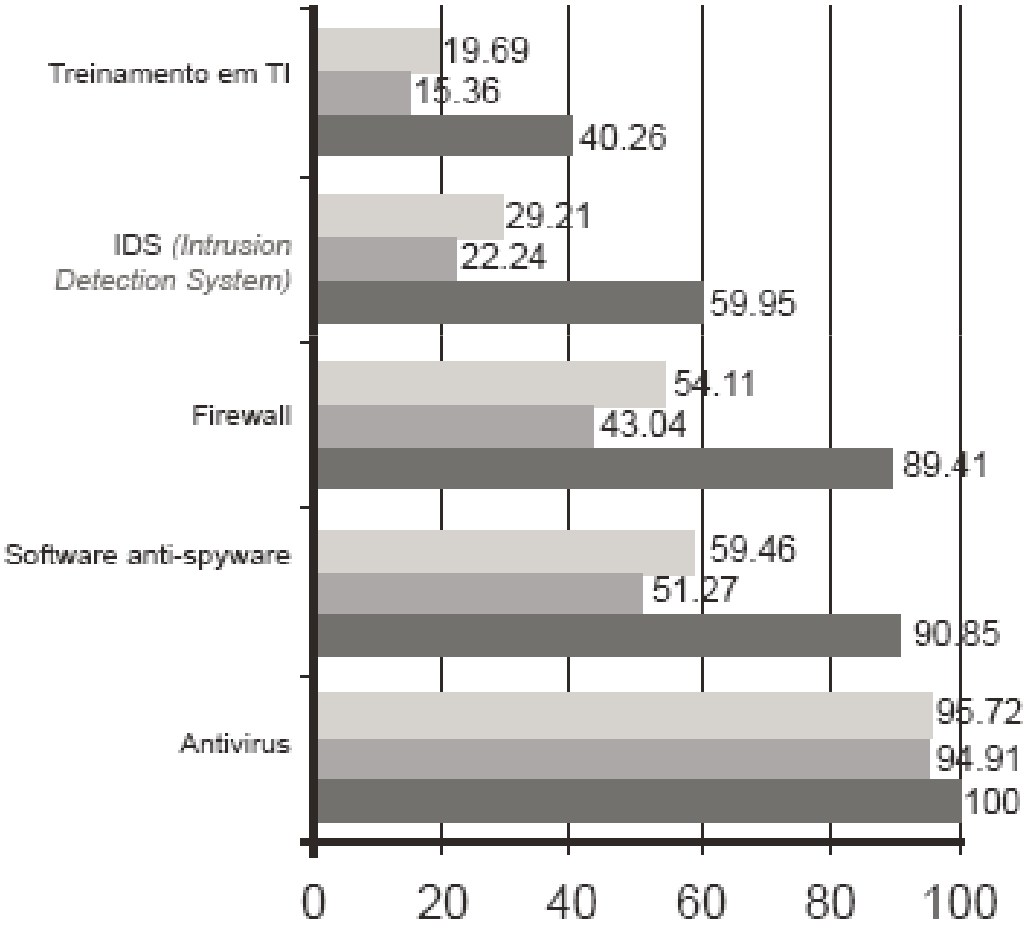
Medidas pré incidentes:



- 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;

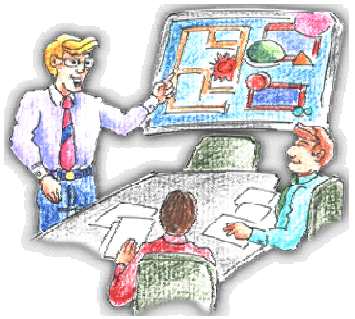
Resposta a Incidentes de Segurança

Medidas de Segurança adotadas por empresas com acesso à Internet



Fonte: CGI.br - 2005

Resposta a Incidentes de Segurança



Medidas pós incidentes:

- 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;

Resposta a Incidentes de Segurança

Após a detecção de um possível incidente de segurança recomenda-se:

- ✓ Confirmar a ocorrência do mesmo, de forma a evitar esforço desnecessário, ou seja, distinguir entre falso-positivo e incidente real;
- ✓ Registrar todas as ações tomadas;
- ✓ Definir o nível de criticidade do incidente;
- ✓ Identificar sistemas atingidos direta ou indiretamente;

Resposta a Incidentes de Segurança

Após a detecção de um possível incidente de segurança recomenda-se: (continuação)

✓Observar se o incidente continua em curso;
✓ Acionar os especialistas necessários para a resposta ao incidente;
✓ Notificar aos responsáveis quanto ao estado do sistema, tempo estimado de recuperação e ações de contra-resposta;
✓ Isolar os sistemas atingidos até a recuperação do mesmo e coleta das evidências.

Gerenciamento de Incidentes

Cada incidente fornece novas informações para uma análise contínua da segurança no modelo de resposta a incidentes

Registro de Incidentes

À medida que novos incidentes ocorrem, o Time de Resposta à Incidentes (TR) analisa se eles representam um risco novo ou alterado à empresa e cria ou renova diretivas e procedimentos baseados em seus achados.

Toda correção às diretivas de segurança deve acatar os padrões de gerenciamento de alterações da empresa.

O registro dos incidentes possibilita a identificação de padrões e, possivelmente, a prevenção de ataques futuros.

Obrigado!