

**Ibmec Business School**  
**Especialização em Segurança da Informação**  
**IBMEC - Petrobras**

**Disciplina: Tratamento de Incidentes de  
Segurança**

**Professor**

Frederico Sauer, D.Sc.

[fred@sauersecurity.com.br](mailto:fred@sauersecurity.com.br)

**ESTUDO DE CASO**

**ESTRUTURAÇÃO DE UM**

**PLANO DE RESPOSTA A INCIDENTES DE DoS**

**PRIMEIRA VERSÃO**

**Empresa Gerbet Produtos Radiológicos**

## 1. Definições

### Incidentes de Segurança

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 [CERT.br a]. Em geral, toda situação onde uma entidade de informação está sob risco de ser impactada é considerada um incidente de segurança.

### Grupo de Resposta a Incidentes de Segurança (GRIS)

Equipe responsável por serviços e suporte para um determinado público alvo (comunidade), para prevenção, tratamento e/ou resposta a incidentes de segurança, podendo desempenhar diversos papéis e serviços dentro de uma organização tais como tratamento de Incidentes, Auditoria, Monitoramento e etc.

### Plano de Resposta a Incidentes (PRI)

Resposta a incidentes de segurança é uma metodologia organizada para gerir as consequências de uma violação de segurança da informação [CERT.br]. O principal objetivo do processo de resposta a incidentes de segurança é minimizar o impacto de um incidente e permitir o restabelecimento dos sistemas o mais rápido possível.

### Plano de Comunicação

Consiste basicamente no estabelecimento de relacionamentos com os públicos estratégicos afetos ao incidente em questão, buscando estabelecer um padrão uniforme de comunicação, com isso fortalecendo a imagem da empresa.

### Plano de Contingência

Descreve as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação.

### Negação de Serviço (Denial of Service - DoS)

Nos ataques de negação de serviço (DoS -- Denial of Service) o atacante utiliza um computador para tirar de operação um serviço ou computador.

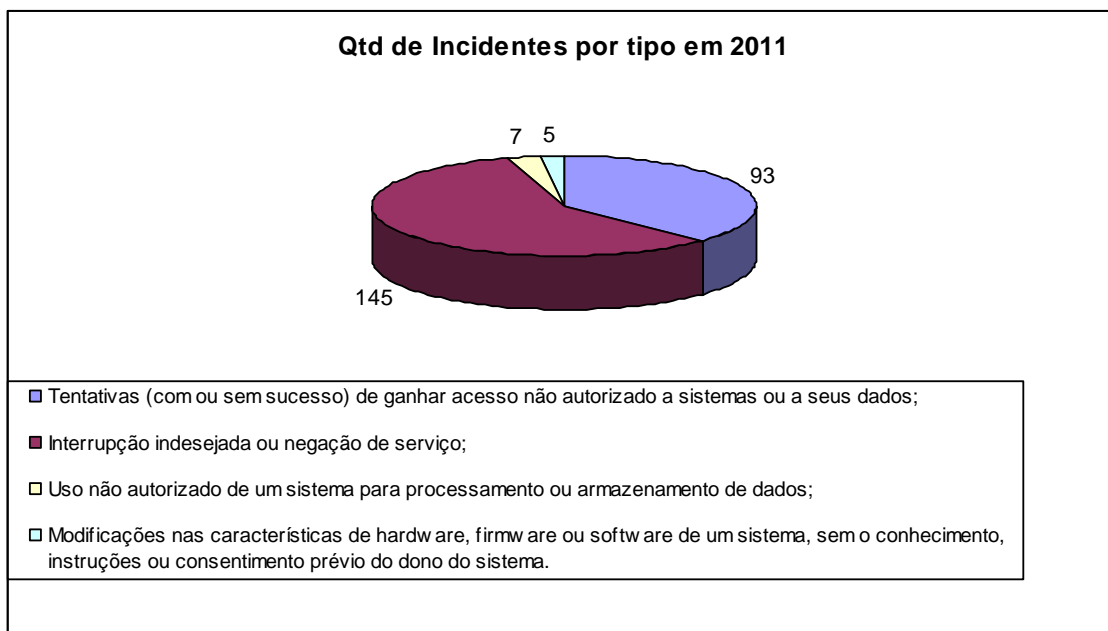
### Negação de Serviço Distribuída (Distributed Denial of Service - DDoS)

DDoS (Distributed Denial of Service) constitui um ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores.

## 2. Motivações para a criação do Plano

Com o crescimento do número de incidentes de segurança ao longo dos anos e o impacto financeiro decorrente, percebe-se que há necessidade de criar uma equipe específica para resposta, independente do Help Desk, e a adoção de metodologias específicas para determinados tipos de ataques.

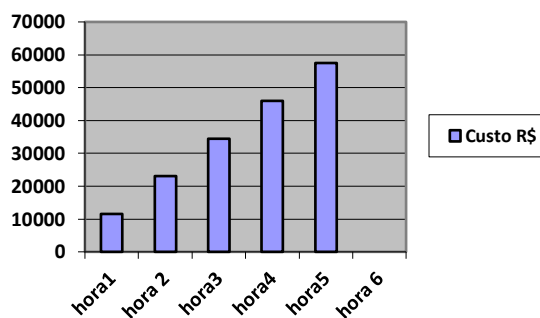
Foi feita também uma análise dos tipos de incidentes mais frequentes no ano anterior, com o objetivo de verificar quais ataques são mais comuns na organização. Como pode-se observar no gráfico a seguir, **a interrupção indesejada ou negação de serviço, como, por exemplo, os ataques DDoS, foi o tipo de incidente de maior ocorrência no ano de 2011** e que, portanto, merece uma atenção maior por parte do GRIS.



A empresa tem como maior produto a fabricação de meios de contraste para auxílio de diagnóstico. No processo de fabricação deste contraste o produto tem um tempo de quarentena de 14 dias.

Devido a esse fato, qualquer incidente que implique em parada de produção, irá acarretar em atraso na entrega do produto, perda de matéria prima de alto custo e consequentemente prejuízos financeiros inaceitáveis.

Segue abaixo gráfico que demonstra como incidentes no ambiente de produção da empresa causam impactos significativos às finanças da empresa.



### 3. Planejamento Estratégico do GRIS

#### Missão

Atuar de forma proativa no diagnóstico e solução de incidentes de segurança, minimizando os impactos e apoiando a melhoria do plano de continuidade dos serviços da organização.

#### Visão

Ser capaz de identificar as principais ameaças de segurança da informação, agindo de forma proativa e respondendo tempestivamente aos eventos e incidentes que possam interferir nas atividades da organização.

#### Objetivos

- Identificar as principais ameaças de segurança;
- Definir um Plano de Resposta a Incidentes;
- Tratar os Incidentes de Segurança, minimizando seus impactos e garantindo a continuidade dos serviços afetados;
- Estabelecer e gerar indicadores e métricas sobre os Incidentes de Segurança;
- Compilar informações e estatísticas, gerando pareceres que possam ser úteis para a gerencia no processo de tomada de decisão;

#### Membros Associados

Membro associado	Descrição da função
Contato de TI	Responsável pela coordenação da comunicação entre o líder de incidentes do GRIS e o restante do grupo de TI, sendo basicamente responsável pela localização das pessoas no grupo de TI que devem tratar eventos de segurança em especial.
Representante legal	<p>Advogado muito familiarizado com as diretrizes estabelecidas de resposta a incidentes. O representante legal determina como proceder durante um incidente com responsabilidade legal mínima e autorização máxima para processar transgressores.</p> <p>Antes que haja um incidente, o representante legal deve ter informações sobre as diretrizes de monitoramento e resposta para assegurar que a organização não esteja correndo riscos legais durante uma operação de limpeza ou de retenção. É muito importante levar em consideração as implicações legais do desligamento de um sistema e da possibilidade de violação dos contratos de nível de serviço ou de associação firmados com seus clientes ou do não desligamento de um sistema com e responsável por danos causados por ataques iniciados a partir deste sistema.</p> <p>Toda a comunicação externa com autoridades competentes ou órgãos investigativos externos deve ser coordenada com o representante legal.</p>
Diretor de relações públicas	Este membro faz parte do departamento de relações públicas, sendo responsável por resguardar e promover a imagem da organização, sendo responsável pela elaboração da mensagem (o conteúdo e o objetivo desta

	mensagem costumam ser de responsabilidade da gerência). Todas as solicitações de imprensa devem ser direcionadas ao Departamento de Relações Públicas.
Gerência	<p>Dependendo do incidente em especial, serão envolvidos apenas os gerentes do departamento ou todos os gerentes de toda a organização. A pessoa responsável pela gerência apropriada varia de acordo com o impacto, o local, a gravidade e o tipo de incidente.</p> <p>A Gerência é responsável pela aprovação e orientação da diretiva de segurança, sendo responsável pela determinação do impacto total (em termos financeiros ou não) do incidente na organização. A Gerência orientará o Diretor de Relações Públicas a respeito das informações a serem divulgadas à imprensa e determina o nível de interação entre o Representante legal e as autoridades competentes.</p>

### Definição de Responsabilidades durante o processo de resposta ao incidente

Atividade	Função				
	Líder de incidentes do GRIS	Contato de TI	Representante legal	Diretor de Relações Públicas	Gerência
Avaliação inicial	Proprietário	Avisa	Nenhuma	Nenhuma	Nenhuma
Resposta inicial	Proprietário	Implementa	Atualiza	Atualiza	Atualiza
Obtém evidências forenses	Implementa	Avisa	Proprietário	Nenhuma	Nenhuma
Implementa correção temporária	Proprietário	Implementa	Atualiza	Atualiza	Avisa
Envia a comunicação	Avisa	Avisa	Avisa	Implementa	Proprietário
Consultar as autoridades competentes locais	Atualiza	Atualiza	Implementa	Atualiza	Proprietário
Implementa correção permanente	Proprietário	Implementa	Atualiza	Atualiza	Atualiza
Determina o impacto financeiro nos negócios	Atualiza	Atualiza	Avisa	Atualiza	Proprietário

### Plano de Comunicação

Este plano tem como objetivo cientificar os diretores do conselho das informações descritas abaixo:

**Fase 1 - Uma vez ocorrido um incidente de DDOS**

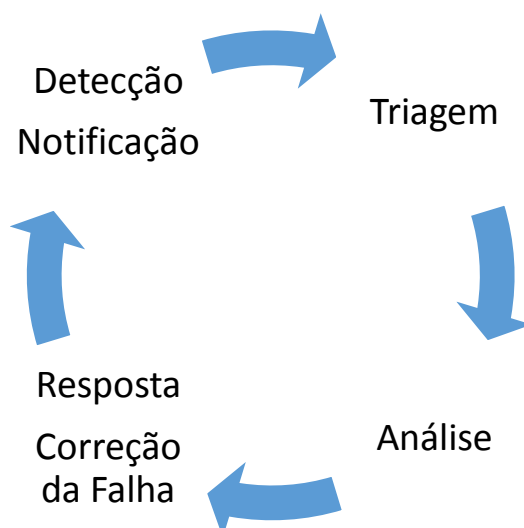
Informação	Obs.
O que aconteceu?	(Foco nos fatos ou nas acusações.)
Quanto?	(Danos, dinheiro envolvido.)
Quem foi afetado?	(Vítimas, acusados etc.)

**Fase 2 - Após um incidente de DDOS**

Informação	Obs.
Qual foi a causa?	-
Obedece a um padrão?	Ex: Atacantes do mesmo país
Quem pagará os danos?	Necessidade de acionar meios legais ?
Qual é o prejuízo potencial para a reputação da empresa?	Perda de contratos? credibilidade e etc.
Que impacto terá no preço da ação?	Como se refletirá em seus planos? Realinhamento de estratégias?

**Instrução de trabalho**

O plano de resposta a incidentes de DDOS segue o fluxo tradicional da resposta a incidentes.



A Equipe do GRIS da empresa é proativa e dispõe de ferramentas de detecção de tráfego anormal.

### Etapa 1 – Detecção

Através do monitoramento proativo através da ferramenta The Dude as portas dos *switchs* onde estão ligados os servidores, roteadores e equipamentos de borda são monitorados quanto ao tráfego.

### São 3 os estágios do enlace:

**Normal** – Operando dentro dos padrões de normalidade para o protocolo, octetos in e out, erros, descarte de pacotes.

**Instável** – O tráfego de rede está atingindo 70% do limite máximo, houve descarte de pacotes, houve latência acima do normal.

**Off-line** – O tráfego da rede atingiu o limite máximo, os descartes de pacotes estão em taxas altas que não permitem a retransmissão, a latência está provocando a queda da conexão por *timeout*.

O sistema de monitoramento emite alerta visual, alterando a cor do enlace e do ativo conectado, entre verde (normal), amarelo (instável) a vermelho (off-line).

O sistema emite email à equipe responsável por receber a notificação a cada alteração de estágio.

### Etapa 2 – Triagem

De posse do email, a equipe de triagem verifica o alvo, ou seja quais os ativos foram afetados e, se for visível, a origem do ataque.

### Etapa 3 – Análise

A equipe de triagem abre um ticket no sistema de help-desk descrevendo o problema e avisa imediatamente a equipe de análise.

A equipe de análise analisa o tráfego para descobrir a origem, a porta e protocolos anormais.

A primeira ação é bloquear o tráfego *in* das portas e endereços detectados.

Caso a ação não tenha efeito para cessar o ataque, a porta de origem do ataque é desabilitada, isolando a rede da origem do ataque.

A porta de contingência do roteador é ativada, possibilitando o tráfego *out* através de um NAT, e o tráfego *in* só é permitido por endereço e porta específico.

O tráfego capturado é analisado, e é elaborado um plano de correção da falha.

O plano de comunicação é acionado em sua fase 1, informando aos diretores a situação atual e demais informações relevantes.

### **Etapa 4 – Implementação da correção.**

Uma máquina virtual com a imagem dos servidores atacados e com as correções aplicadas é colocada no ar como um *honey pot* a fim de testar se as correções foram efetivas.

O tráfego é monitorado para verificar se os ataques cessaram. Após 12 horas no ar se os ataques não continuarem as correções são aplicadas nos servidores de produção.

Os parâmetros de detecção do The Dude são alterados para a detecção precoce de novos ataques.

É elaborado um relatório de investigação forense com a documentação do caso e das correções aplicadas.

O ticket de help-desk é fechado e a causa raiz é documentada e publicada na base de casos.

O plano de comunicação é acionado em sua fase 2, informando aos diretores a situação atual e informações relevantes.