

# Resposta a Incidentes de SegInfo

Prof. Dr. Frederico Sauer  
[fred@sauersecurity.com.br](mailto:fred@sauersecurity.com.br)

# Objetivo



Discutir as fases para elaboração de um **Grupo** de Resposta a Incidentes de Segurança da Informação (GRIS) e de **Planos** de Resposta a Incidentes de SegInfo (PRI).

## Perguntas Iniciais a Responder...

- Quais são os requisitos básicos para se estabelecer um GRIS ?
- Que tipo de GRIS será necessário?
- Que tipos de serviços devem ser oferecidos?
- Qual deve ser o tamanho de um GRIS ?
- Onde o GRIS deve estar localizado na organização?
- Qual será o custo para implementar e manter um GRIS?
- Quais são os passos iniciais que devem ser seguidos para criar um GRIS ?

# Sumário

- Motivações
- Definições e Conceitos básicos
- Tipos de Incidentes
- Pré-Requisitos
- O processo de criação do Grupo de Resposta a Incidentes
- A Elaboração de um Plano de Resposta a Incidentes de SegInfo
- Trabalhos em Grupo
  - Trabalho de Estruturação de um GRIS
  - Trabalho de Plano de Resposta a Incidentes

# Motivações

- Uma boa Gestão de Riscos depende de dados estatísticos sobre incidentes e seus impactos
- Para isso são necessários dados sobre:
  - Incidentes de segurança ocorridos e seus efeitos
  - Percepção do grau de cultura corporativa de segurança
  - Tipos e comportamentos de novas ameaças
- Esta atitude possibilita às corporações:
  - Identificação da demanda de novas políticas para proteção das informações
  - Identificação de prioridades, treinamentos específicos, auditorias, etc.

# Motivações para o uso de uma Metodologia de Tratamento de Incidentes

- Padronização dos Procedimentos em caso de crise
  - Soluções *ad-hoc* nem sempre são as ideais
- Visão Geral dos Incidentes
  - Indicadores/Métricas
  - Lições Aprendidas
    - Ganho de desempenho em novas ocorrências
    - Mudança de postura para evitar novos incidentes
  - Melhor aplicação de Investimentos em SegInfo
  - São identificadas tendências de possíveis incidentes que nunca ocorreram
- Alguns ataques não são bloqueados por ferramentas automatizadas, como firewall ou proxies de aplicação
- Avanço das técnicas de invasão, cada vez mais *sthealth*

# Definições e Conceitos

- O que é um Evento de Segurança ?
  - Ocorrência em um sistema, serviço ou rede que indique um POSSÍVEL descumprimento de Política de Segurança ou falha nos controles, ou ainda uma situação previamente desconhecida que possa ser relevante para a SegInfo
- E um Incidente de Segurança ?
  - Um ou mais EVENTOS que tenham uma significativa probabilidade de comprometer o negócio e ameaçar a SegInfo
- Todo Incidente é composto de um ou mais eventos, então ambos devem ser foco do trabalho do GRIS e do PRI.

# Definições e Conceitos

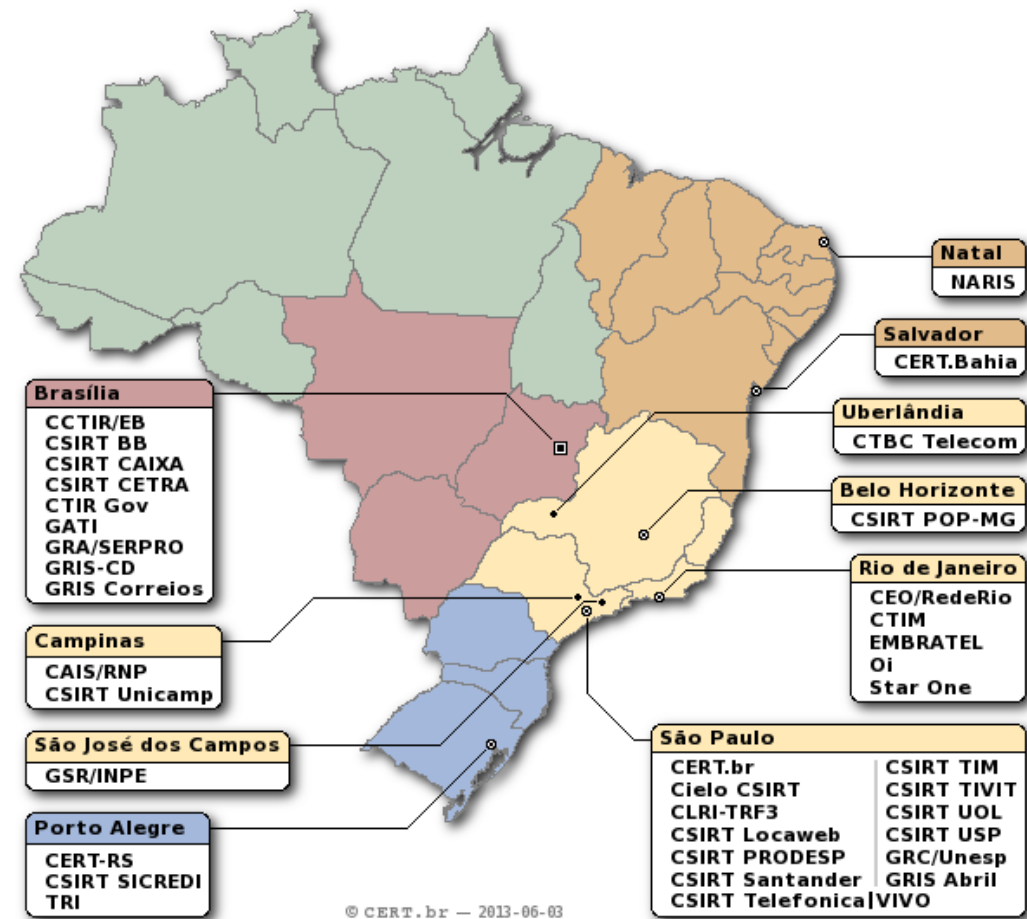
- GRIS (Grupo de Resposta a Incidentes de Segurança da Informação)
  - Responsável por serviços e suporte para um determinado público alvo, **para prevenção, tratamento e resposta a incidentes de segurança.**
  - Pode desempenhar **diversos papéis** e serviços dentro de uma organização
    - Tratamento de Incidentes, Auditoria, Monitoramento, Testes, Tratamento de Riscos, assessorar a criação de recomendações de SegInfo, Contato entre organizações afins (outros GRIS e CERT-BR, polícia especializada, provedores).



# Definições e Conceitos

## ■ Tipos de GRIS

- Departamentos
- Empresas
- Países
- *Backbones*
- Órgãos Governamentais



## ■ Abordagens

### ■ Centralizada

- Recomendado para pequenas organizações, onde não existem unidades remotas

### ■ Distribuída

- Recomendado para grandes organizações. Possui diversos GRIS espalhados pelas várias unidades da empresa que deverão responder a um Centro Organizacional, que será responsável por todos os GRIS
  - Exemplo: Marinha do Brasil

### ■ Terceirizada

- Parcial: São terceirizados alguns Serviços especializados
- Total: Todo Serviço de Resposta é terceirizado

# Definições e Conceitos

- Dedicção
  - A organização deverá refletir sobre a sua situação quanto ao risco para definir a disponibilidade do GRIS, que poderá ser:
    - Dedicção Integral
    - Dedicção Compartilhada
- Nível de Autoridade
  - Total
  - Parcial
  - Nenhuma

# Definições e Conceitos

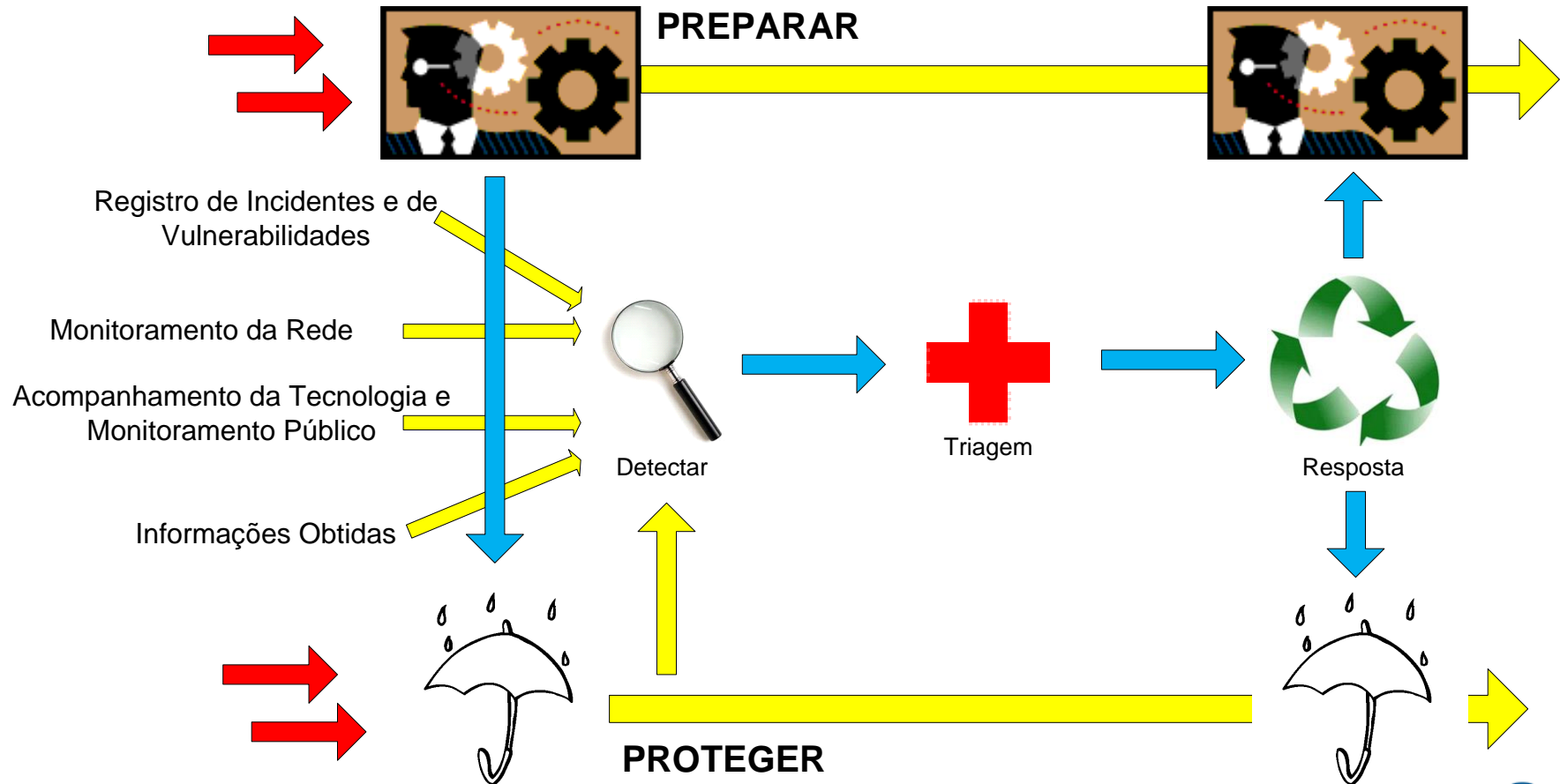
- Relação entre os termos Gerenciamento/Manipulação/Respostas:

Triagem	Análise
Detecção e Relato	<b>Resposta a Incidentes</b>



# Definições e Conceitos

## ■ Processo de Gerenciamento de Incidentes



## ■ Categorias de Serviços:

Serviços Reativos	Serviços Próativos	Gerenciamento da Qualidade da SegInfo
<ul style="list-style-type: none"><li>➤ Emissão de alertas e avisos (warnings)</li><li>➤ Manipulação de incidentes<ul style="list-style-type: none"><li>✓ Análise do incidente</li><li>✓ Resposta in-loco</li><li>✓ Suporte à resposta</li><li>✓ Coordenação da resposta</li></ul></li><li>➤ Manipulação de Vulnerabilidades<ul style="list-style-type: none"><li>✓ Análise de Vulnerabilidades</li><li>✓ Resposta às Vulnerabilidades</li><li>✓ Coordenação da Resposta às Vulnerabilidades</li></ul></li><li>➤ Manipulação de Artefatos<ul style="list-style-type: none"><li>✓ Análise de Artefatos</li><li>✓ Resposta à ação de Artefatos</li><li>✓ Coordenação da Resposta à ação de Artefatos</li></ul></li></ul>	<ul style="list-style-type: none"><li>➤ Emissão de anúncios (Announcements)</li><li>➤ Auditorias e Análises de Segurança</li><li>➤ Configuração e Manutenção de ferramentas de Segurança e da Infra necessária</li><li>➤ Desenvolvimento ou aquisição de ferramentas de segurança</li><li>➤ Detecção de Intrusos</li><li>➤ Disseminação de Informações sobre Segurança da Informação</li></ul>	<ul style="list-style-type: none"><li>➤ Análises de Risco</li><li>➤ Continuidade dos Negócios e DRP</li><li>➤ Consultoria de Segurança</li><li>➤ Criação da Cultura de Segurança corporativa</li><li>➤ Treinamento e Educação</li><li>➤ Avaliação e Certificação de produtos</li></ul>

## ■ Categorias de Serviços:

Serviços Reativos	Serviços Próativos	Gerenciamento da Qualidade da SegInfo
<ul style="list-style-type: none"><li>➤ Emissão de alertas e avisos (warnings)</li><li>➤ Manipulação de incidentes<ul style="list-style-type: none"><li>✓ Análise do incidente</li><li>✓ Resposta in-loco</li><li>✓ Suporte à resposta</li><li>✓ Coordenação da resposta</li></ul></li><li>➤ Manipulação de Vulnerabilidades<ul style="list-style-type: none"><li>✓ Análise de Vulnerabilidades</li><li>✓ Resposta às Vulnerabilidades</li><li>✓ Coordenação da Resposta às Vulnerabilidades</li></ul></li><li>➤ Manipulação de Artefatos<ul style="list-style-type: none"><li>✓ Análise de Artefatos</li><li>✓ Resposta à ação de Artefatos</li><li>✓ Coordenação da Resposta à ação de Artefatos</li></ul></li></ul>	<ul style="list-style-type: none"><li>➤ Emissão de anúncios (Announcements)</li><li>➤ Auditorias e Análises de Segurança</li><li>➤ Configuração e Manutenção de ferramentas de Segurança e da Infra necessária</li><li>➤ Desenvolvimento ou aquisição de ferramentas de segurança</li><li>➤ Detecção de Intrusos</li><li>➤ Disseminação de Informações sobre Segurança da Informação</li></ul>	<ul style="list-style-type: none"><li>➤ Análises de Risco</li><li>➤ Continuidade dos Negócios e DRP</li><li>➤ Consultoria de Segurança</li><li>➤ Criação da Cultura de Segurança corporativa</li><li>➤ Treinamento e Educação</li><li>➤ Avaliação e Certificação de produtos</li></ul>

## ■ Categorias de Serviços:

Serviços Reativos	Serviços Próativos	Gerenciamento da Qualidade da SegInfo
<ul style="list-style-type: none"><li>➤ Emissão de alertas e avisos (warnings)</li><li>➤ Manipulação de incidentes<ul style="list-style-type: none"><li>✓ Análise do incidente</li><li>✓ Resposta in-loco</li><li>✓ Suporte à resposta</li><li>✓ Coordenação da resposta</li></ul></li><li>➤ Manipulação de Vulnerabilidades<ul style="list-style-type: none"><li>✓ Análise de Vulnerabilidades</li><li>✓ Resposta às Vulnerabilidades</li><li>✓ Coordenação da Resposta às Vulnerabilidades</li></ul></li><li>➤ Manipulação de Artefatos<ul style="list-style-type: none"><li>✓ Análise de Artefatos</li><li>✓ Resposta à ação de Artefatos</li><li>✓ Coordenação da Resposta à ação de Artefatos</li></ul></li></ul>	<ul style="list-style-type: none"><li>➤ Emissão de anúncios (Announcements)</li><li>➤ Auditorias e Análises de Segurança</li><li>➤ Configuração e Manutenção de ferramentas de Segurança e da Infra necessária</li><li>➤ Desenvolvimento ou aquisição de ferramentas de segurança</li><li>➤ Detecção de Intrusos</li><li>➤ Disseminação de Informações sobre Segurança da Informação</li></ul>	<ul style="list-style-type: none"><li>➤ Análises de Risco</li><li>➤ Continuidade dos Negócios e DRP</li><li>➤ Consultoria de Segurança</li><li>➤ Criação da Cultura de Segurança corporativa</li><li>➤ Treinamento e Educação</li><li>➤ Avaliação e Certificação de produtos</li></ul>



## ■ Categorias de Serviços:

Serviços Reativos	Serviços Próativos	Gerenciamento da Qualidade da SegInfo
<ul style="list-style-type: none"><li>➤ Emissão de alertas e avisos (warnings)</li><li>➤ Manipulação de incidentes<ul style="list-style-type: none"><li>✓ Análise do incidente</li><li>✓ Resposta in-loco</li><li>✓ Suporte à resposta</li><li>✓ Coordenação da resposta</li></ul></li><li>➤ Manipulação de Vulnerabilidades<ul style="list-style-type: none"><li>✓ Análise de Vulnerabilidades</li><li>✓ Resposta às Vulnerabilidades</li><li>✓ Coordenação da Resposta às Vulnerabilidades</li></ul></li><li>➤ Manipulação de Artefatos<ul style="list-style-type: none"><li>✓ Análise de Artefatos</li><li>✓ Resposta à ação de Artefatos</li><li>✓ Coordenação da Resposta à ação de Artefatos</li></ul></li></ul>	<ul style="list-style-type: none"><li>➤ Emissão de anúncios (Announcements)</li><li>➤ Auditorias e Análises de Segurança</li><li>➤ Configuração e Manutenção de ferramentas de Segurança e da Infra necessária</li><li>➤ <b>Desenvolvimento ou aquisição de ferramentas de segurança</b></li><li>➤ <b>Deteção de Intrusos</b></li><li>➤ <b>Disseminação de Informações sobre Segurança da Informação</b></li></ul>	<ul style="list-style-type: none"><li>➤ Análises de Risco</li><li>➤ Continuidade dos Negócios e DRP</li><li>➤ Consultoria de Segurança</li><li>➤ Criação da Cultura de Segurança corporativa</li><li>➤ Treinamento e Educação</li><li>➤ Avaliação e Certificação de produtos</li></ul>

## ■ Categorias de Serviços:

Serviços Reativos	Serviços Próativos	Gerenciamento da Qualidade da SegInfo
<ul style="list-style-type: none"><li>➤ Emissão de alertas e avisos (warnings)</li><li>➤ Manipulação de incidentes<ul style="list-style-type: none"><li>✓ Análise do incidente</li><li>✓ Resposta in-loco</li><li>✓ Suporte à resposta</li><li>✓ Coordenação da resposta</li></ul></li><li>➤ Manipulação de Vulnerabilidades<ul style="list-style-type: none"><li>✓ Análise de Vulnerabilidades</li><li>✓ Resposta às Vulnerabilidades</li><li>✓ Coordenação da Resposta às Vulnerabilidades</li></ul></li><li>➤ Manipulação de Artefatos<ul style="list-style-type: none"><li>✓ Análise de Artefatos</li><li>✓ Resposta à ação de Artefatos</li><li>✓ Coordenação da Resposta à ação de Artefatos</li></ul></li></ul>	<ul style="list-style-type: none"><li>➤ Emissão de anúncios (Announcements)</li><li>➤ Auditorias e Análises de Segurança</li><li>➤ Configuração e Manutenção de ferramentas de Segurança e da Infra necessária</li><li>➤ Desenvolvimento ou aquisição de ferramentas de segurança</li><li>➤ Detecção de Intrusos</li><li>➤ Disseminação de Informações sobre Segurança da Informação</li></ul>	<ul style="list-style-type: none"><li>➤ <b>Análises de Risco</b></li><li>➤ <b>Continuidade dos Negócios e DRP</b></li><li>➤ <b>Consultoria de Segurança</b><ul style="list-style-type: none"><li>➤ Criação da Cultura de Segurança corporativa</li><li>➤ Treinamento e Educação</li><li>➤ Avaliação e Certificação de produtos</li></ul></li></ul>

## ■ Categorias de Serviços:

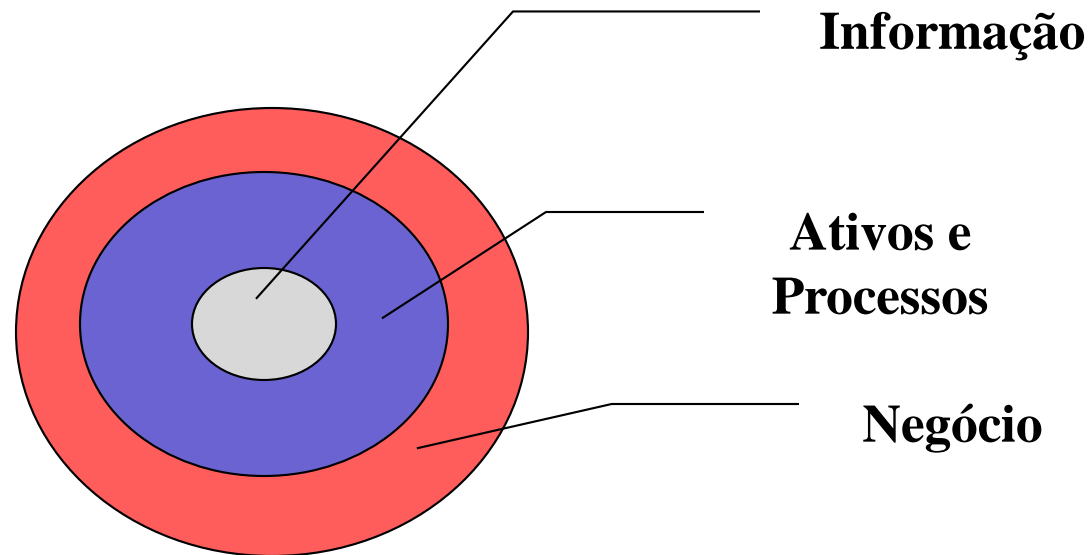
Serviços Reativos	Serviços Próativos	Gerenciamento da Qualidade da SegInfo
<ul style="list-style-type: none"><li>➤ Emissão de alertas e avisos (warnings)</li><li>➤ Manipulação de incidentes<ul style="list-style-type: none"><li>✓ Análise do incidente</li><li>✓ Resposta in-loco</li><li>✓ Suporte à resposta</li><li>✓ Coordenação da resposta</li></ul></li><li>➤ Manipulação de Vulnerabilidades<ul style="list-style-type: none"><li>✓ Análise de Vulnerabilidades</li><li>✓ Resposta às Vulnerabilidades</li><li>✓ Coordenação da Resposta às Vulnerabilidades</li></ul></li><li>➤ Manipulação de Artefatos<ul style="list-style-type: none"><li>✓ Análise de Artefatos</li><li>✓ Resposta à ação de Artefatos</li><li>✓ Coordenação da Resposta à ação de Artefatos</li></ul></li></ul>	<ul style="list-style-type: none"><li>➤ Emissão de anúncios (Announcements)</li><li>➤ Auditorias e Análises de Segurança</li><li>➤ Configuração e Manutenção de ferramentas de Segurança e da Infra necessária</li><li>➤ Desenvolvimento ou aquisição de ferramentas de segurança</li><li>➤ Detecção de Intrusos</li><li>➤ Disseminação de Informações sobre Segurança da Informação</li></ul>	<ul style="list-style-type: none"><li>➤ Análises de Risco</li><li>➤ Continuidade dos Negócios e DRP</li><li>➤ Consultoria de Segurança</li><li>➤ <b>Criação da Cultura de Segurança corporativa</b></li><li>➤ <b>Treinamento e Educação</b></li><li>➤ <b>Avaliação e Certificação de produtos</b></li></ul>

# Definições e Conceitos

- Outros Termos Importantes:
  - IRT = Incident Response Team
  - IRC = Incident Response Capability
  - IHT = Incident Handling Team
  - IMT = Incident Managing / Management Team
  - CSIRT = Computer/Cyber Security Incident Response Team
  - CIRT = Computer Incident Response Team
  - CIRC = Computer Incident Response Capability or Center
  - SIRT = Security Incident Response Team
  - SERT = Security Emergency Response Team

# Definições e Conceitos

- O GRIS deve definir suas ações em função dos ativos de TI ?



## ■ Quanto ao Tipo:

### ■ **Negação de Serviço (Indisponibilidade)**

- Utilização indevida dos recursos da rede e de sistemas, levando à impossibilidade de atender solicitações legítimas

### ■ **Código Malicioso (Integridade)**

- Vírus, *Worms*, *Trojan horse*, *exploits*, etc.

### ■ **Acesso não autorizado (Confidencialidade)**

- Pessoas sem permissão ganham acesso físico ou lógico à rede, sistemas, aplicativos, ambientes, outros recursos/locais

### ■ **Uso indevido de recursos (CID)**

- Violação da Política de Segurança por pessoas direta ou indiretamente envolvidas

### ■ **Diversos**

- Combinação de 2 ou mais tipos de incidentes

## ■ Quanto a Severidade:

- Alerta 1
  - Falso Positivo
- Alerta 2
  - Ocorrência de evento (sem consequências)
- Alerta 3
  - Ocorrência do evento com consequências suportáveis, dentro dos critérios de aceitação (ex. propagação de vírus controlada)
- Alerta 4
  - Ocorrência do evento com consequências próximas dos critérios de aceitação (ex. servidor com *malware* instalado, porém aparentemente sem danos à CID)
- Alerta 5
  - Ocorrência do evento com consequências Altas (ex. Servidor de Banco de Dados fora do ar)

**Obs.: A classificação dos Incidentes poderá mudar de acordo com o cenário de cada empresa e deverá levar em consideração o histórico dos incidentes da organização!**

NP-1

# Pré-Requisitos

- Todos os GRIS devem possuir as mesmas Características, Estrutura e Formação?



Comunicação relacionada à Incidentes com parceiros externos



# Pré-Requisitos

- Então o que levar em consideração na criação do GRIS ?
  - Missão, Visão e Objetivos do GRIS
  - Tipo/Natureza e Escopo dos serviços prestados pelo GRIS
  - Experiência/conhecimentos necessários para formação da Equipe
  - Tamanho e abrangência da organização → tamanho do GRIS
  - Classificação dos Incidentes por Níveis de Criticidade
  - Patrocinadores/*Stakeholders*
  - Natureza do Negócio
  - Leis, Normas e Regulamentos

# O Processo de criação do GRIS

## ■ Tópicos para Reflexão!

- Qual o verdadeiro papel do GRIS ?
  - Tratamento do Incidente?
  - Apenas como identificador do incidente?
  - Apenas como Controlador/Mantenedor da SegInfo ?
- Qual deve ser o tamanho e *expertise* da Equipe?
- Qual a previsão de custo para implementação e manutenção
  - Manter equipe capacitada em TI e Negócio
- Em que posição deve estar localizado na hierarquia da organização?
- Quem apoiará o processo? Quem são as partes interessadas ?
- De que forma o GRIS irá contribuir para o negócio da organização ?

# O Processo de Criação do GRIS

## ■ As Macro Etapas:

- Fase 1: Identificar e obter o apoio e a aprovação dos *Stakeholders* / Patrocinadores
- Fase 2: Levantamento de Informações
- Fase 3: Planejamento Estratégico do GRIS
- Fase 4: Implantação
- Fase 5: Campanha de divulgação do GRIS
- Fase 6: Avaliações e Métricas

## ■ Fase 1: Identificar e obter o apoio e a aprovação dos *Stakeholders*/patrocinadores

- Carta de compromisso da Alta Direção
- Termo de Compromisso dos Envolvidos no Processo
- Identificar claramente as forças envolvidas (Positivas e Negativas)
- Possíveis *Stakeholders* (Partes Interessadas)
  - Diretores/Gerentes de negócios
  - Gerentes/Coordenador de TI
  - Gerente/Coordenador de RH
  - Representante(s) do departamento jurídico
  - Representantes da Organização
  - Equipe de Auditoria
  - Equipe de Segurança
  - Representantes das áreas que serão atendidas pelo GRIS

## ■ Fase 2: Levantamento de Informações

- Obter histórico de incidentes
- Mapear os Serviços e Estrutura da Organização
- Quantificar, e possivelmente identificar os profissionais que tenham o perfil para participar do Projeto
- Realizar reuniões com os envolvidos para discutir ideias, alinhar as expectativas e responsabilidades. Sempre que possível envolver as partes interessadas
- Recursos relevantes:
  - Organogramas da empresa e das áreas de negócio
  - Infraestrutura de TI (topologia da rede, sistemas, provedores, etc.)
  - Inventários dos sistemas e recursos, classificados de acordo com a criticidade
  - Planos de DRP/continuidade dos negócios existentes
  - Normas para comunicar violações de segurança física e Lógica já existentes
  - Informação sobre eventuais GRIS já existentes
  - Leis, Normas e Regulamentos aos quais a organização esteja sujeita
  - Políticas, Normas e Procedimentos de SegInfo existentes

## ■ Fase 3: Planejamento Estratégico do GRIS

- Conceber a Missão, a Visão e os Objetivos
- Desenvolvimento do Projeto com *milestones* para a Equipe
- Questões administrativas e processuais de Gerência do Projeto ou de TI
- Planejar a equipe e os envolvidos (direta e/ou indiretamente)
  - Ter sempre substitutos definidos para cada responsável por uma função relevante
- Canais de Comunicação / Divulgação
  - Determinar a melhor forma de obter apoio da organização
  - Facilitar a interação entre departamentos
- Definir o armazenamento das informações
  - Dependerá da estrutura adotada

## ■ Fase 3: Planejamento Estratégico do GRIS (cont.)

- Alinhar as expectativas com as partes envolvidas e com os clientes (usuários internos, externos, terceiros, etc.)
- Comunicar com antecedência a Visão, Missão e os Objetivos
  - Pode ajudar a identificar problemas no processo
  - Permite um *feedback* antes da operacionalização do processo
  - Inicia o marketing do Grupo
- O que levar em consideração na criação da Visão:
  - Identificar a comunidade a ser atendida. A quem o GRIS presta serviços e suporte ?
  - Definir a missão e os objetivos do GRIS. O que o GRIS faz para a comunidade a qual ele atende ?
  - Como o GRIS dará suporte à sua missão ?
  - Determinar o modelo organizacional. Como o GRIS é estruturado e organizado ?
  - Identificar os recursos necessários. Que pessoal, equipamentos e infraestrutura são necessários para operar o GRIS ?
  - Determinar o modelo de financiamento do GRIS na fase de implantação e durante as fases de crescimento e manutenção a longo prazo?

# Fase 4: Implantação

## ■ Fase 4: Implantação

- Com base no Planejamento, executar:
  - Contratar e/ou capacitar a equipe responsável
  - Comprar equipamentos e software
  - Montar a infraestrutura necessária para dar suporte ao grupo, como Notebook, salas, telefones, câmeras para monitoramento, etc.
  - Desenvolver as políticas e procedimentos para o GRIS, de maneira a dar suporte aos serviços
  - Definir as especificações para os Plano de Gerenciamento de Incidentes e implementá-los
  - Desenvolver recomendações e formulários para o acompanhamento/tratamento dos incidentes
  - Executar as demais tarefas pré-estabelecidas no Planejamento Estratégico.



# O Processo de Criação do GRIS

## ■ Fase 5: Campanha de divulgação do GRIS

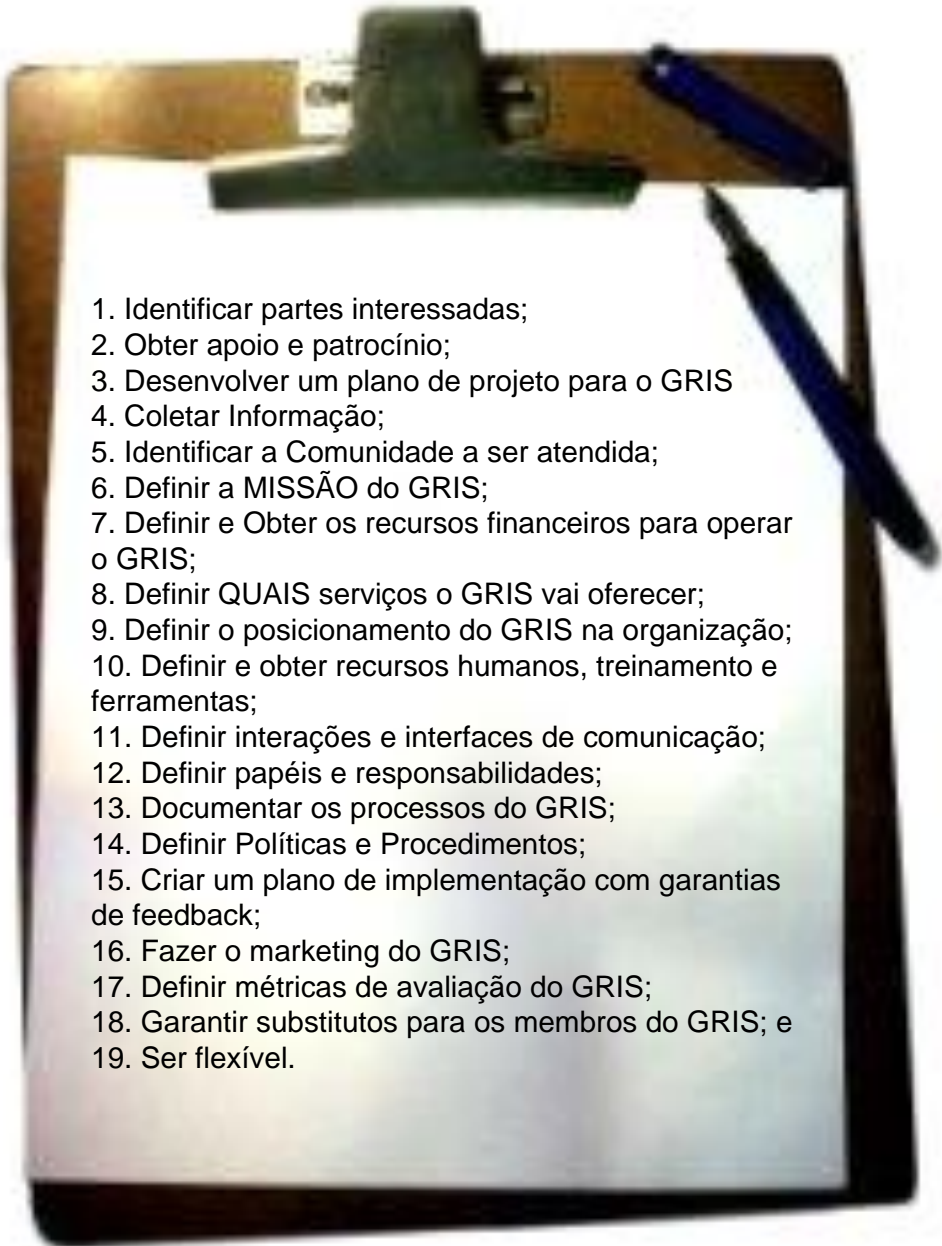
- Envolver RH e Marketing
  - Folhetos, Brindes, GRIS *Day*, Palestras, etc.
- Comunicar a Missão, Visão e Princípios à Organização e às Partes interessadas
- Divulgar Carta de Compromisso da Alta Direção
- Uso da Intranet para divulgar elementos de contato no GRIS, telefones para reportar incidentes, Disque-denúncia anônimo, etc.

# O Processo de Criação do GRIS

## ■ Fase 6: Avaliação e Métricas

- Benchmarking entre o seu e outros GRIS
- Criar padrões de Qualidade e Controle
- Questionário de Qualidade de Atendimento periódico
- Criar um critério para avaliar a evolução da equipe
- Métricas básicas
  - % de incidentes reportados
  - % de incidentes resolvidos com sucesso
  - % de incidentes não resolvidos
  - tempo médio de resposta
  - % de capacitação da equipe

# Checklist

- 
1. Identificar partes interessadas;
  2. Obter apoio e patrocínio;
  3. Desenvolver um plano de projeto para o GRIS
  4. Coletar Informação;
  5. Identificar a Comunidade a ser atendida;
  6. Definir a MISSÃO do GRIS;
  7. Definir e Obter os recursos financeiros para operar o GRIS;
  8. Definir QUAIS serviços o GRIS vai oferecer;
  9. Definir o posicionamento do GRIS na organização;
  10. Definir e obter recursos humanos, treinamento e ferramentas;
  11. Definir interações e interfaces de comunicação;
  12. Definir papéis e responsabilidades;
  13. Documentar os processos do GRIS;
  14. Definir Políticas e Procedimentos;
  15. Criar um plano de implementação com garantias de feedback;
  16. Fazer o marketing do GRIS;
  17. Definir métricas de avaliação do GRIS;
  18. Garantir substitutos para os membros do GRIS; e
  19. Ser flexível.

## Estudo de Caso 1 - GRIS

- Empresa multinacional de Produtos Radiológicos
- Altíssima criticidade de processos cuja falha pode comprometer milhares de vidas humanas
- Máquinas e equipamentos controlados por CLP e computadores convencionais, ligados em rede
- Há regulamentações internacionais, como a GAMP, com foco em ações decorrentes do nível de risco
- O case anexo é a primeira versão do documento, elaborado em 2012.

## Trabalho 1

- Elaboração, em grupo, do documento de planejamento do GRIS para a empresa de comércio virtual detalhada em anexo.
- Todas as demandas necessárias para a tomada de decisões devem ser compatíveis com as características típicas de uma empresa deste tipo, e tudo que não estiver explicitamente definido pode ser livremente arbitrado.

# Plano de Resposta a Incidentes de Segurança da Informação

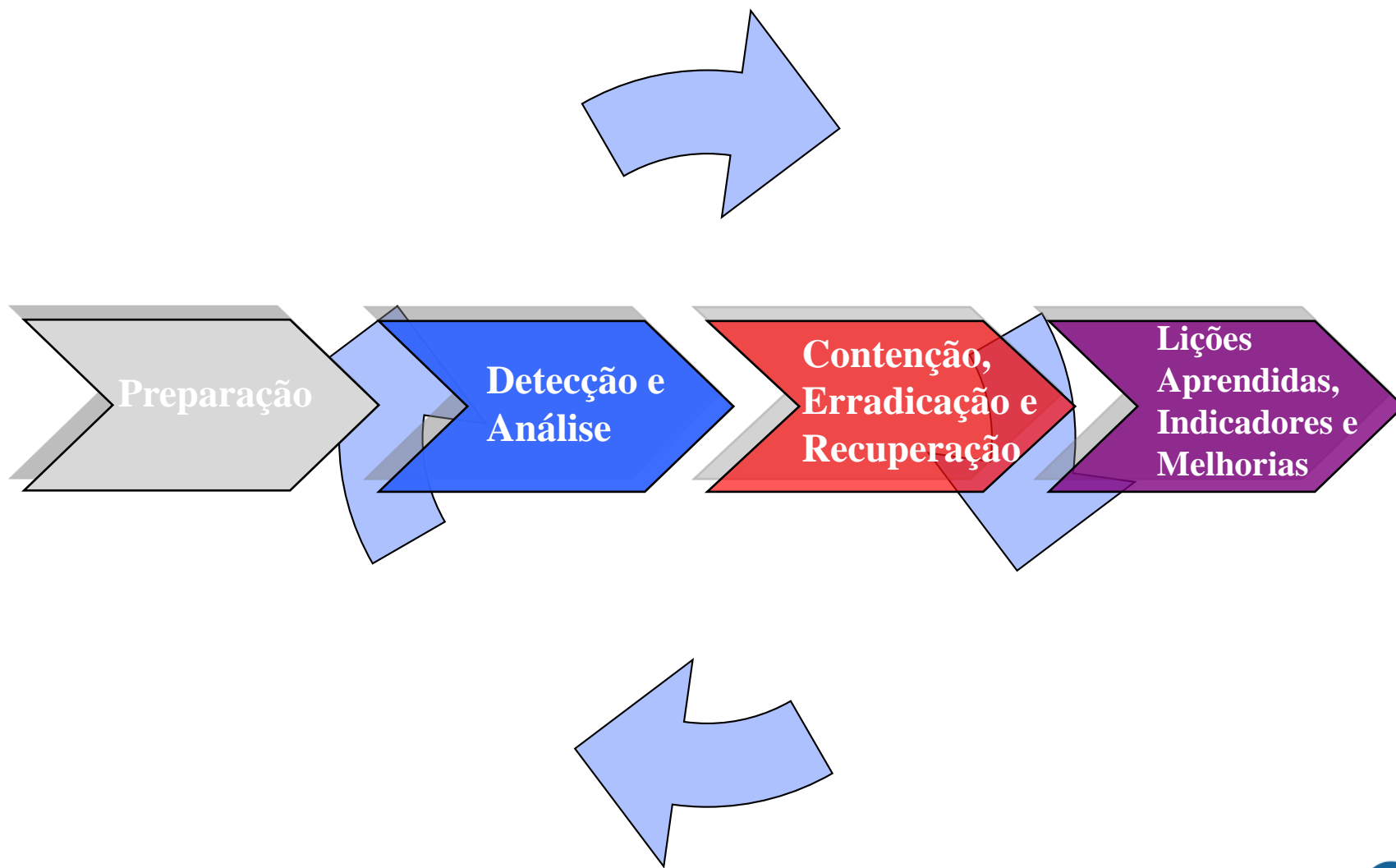
## Definição - PRI

Processo de resposta a incidentes de Segurança da Informação que pode envolver uma parte ou toda a organização, empresas parceiras e clientes

O objetivo final de um PRI é restabelecer o ambiente anterior ao incidente com as devidas medidas de segurança implantadas e monitoradas

Adicionalmente, deve prover condições para as lições aprendidas, buscando evitar que o incidente volte a ocorrer

# Fases do Plano de Resposta



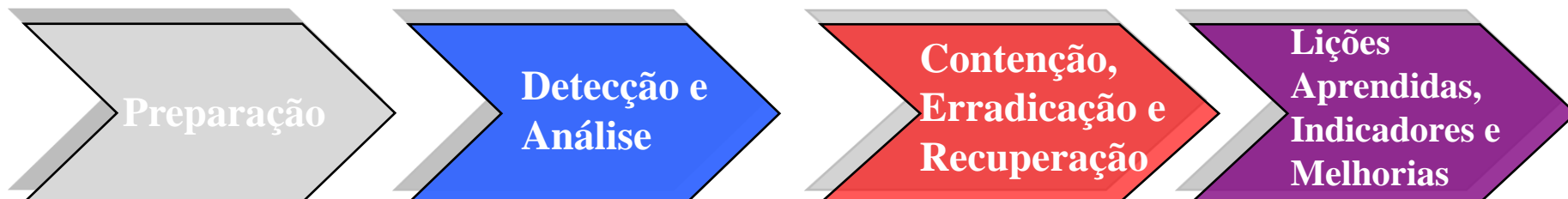


# Fases do Plano de Resposta



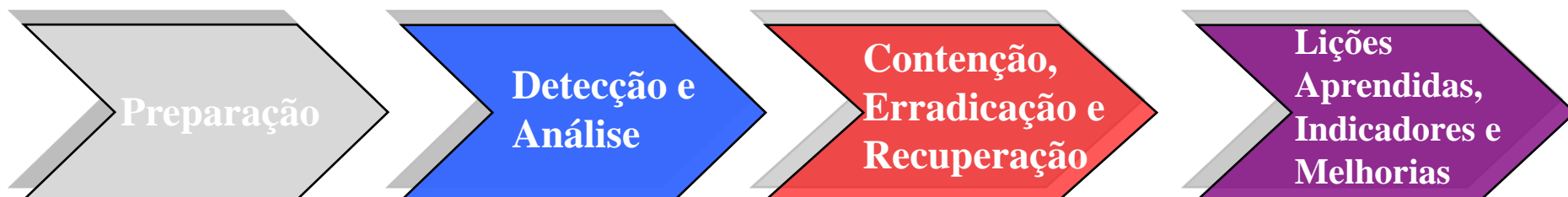
- Garantir que os Processos, Recursos e Tecnologia identificados durante a fase de estruturação do GRIS estão disponíveis e funcionais
  - Equipamentos adequados (TAP, notebooks, duplicadores de imagem, mídias para gravação de dados, máquina fotográfica, gravadores de som, etc.)
  - Responsáveis mapeados/disponíveis
  - Informações da organização mapeadas e atualizadas
  - Possuir um local de reunião seguro quanto à CID das informações coletadas
  - Testes periódicos

# Fases do Plano de Resposta



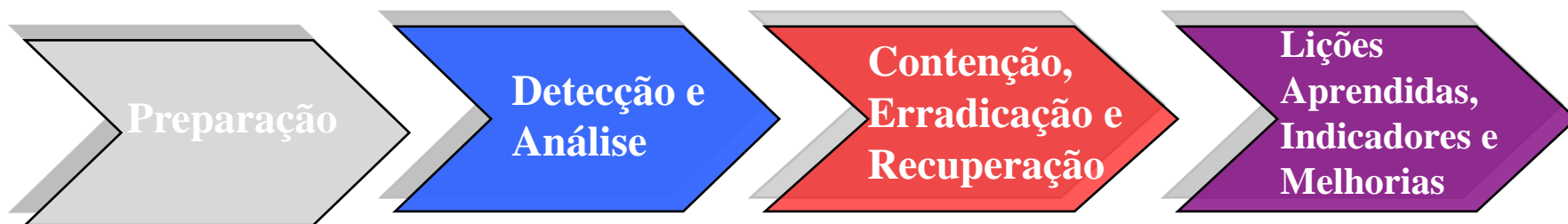
- Possuir sistemas de monitoramento eficazes (IDS, SYSLOG, etc.)
- Identificar a estrutura do ambiente do incidente (Processos, Tecnologia e Pessoas)
- Buscar possíveis correlações com outros sintomas
- Validar o incidente quanto à sua real ocorrência
- Classificar o Incidente
  - Categoria e Relevância
  - Identificar os Procedimentos a serem seguidos
- Garantir que os técnicos alocados possuam capacitação para a análise
- Evitar o caos, notificando apenas as áreas/pessoas efetivamente necessárias
- Não divulgar o ocorrido até que as investigações tenham sido finalizadas.

# Fases do Plano de Resposta



- Tomar decisões APENAS com base em evidência
- Preservar as evidências para casos futuros e eventual ação policial
  - Data, local, nomes, telefones, logs, fotos, etc.
- Criar uma estratégia adequada para cada tipo/nível de Incidente
- Determinar o nível de abrangência do incidente (outras partes afetadas)
- Estimar o tempo de contenção e recuperação para cada tipo/nível de Incidente
- Backup Funcional
  - Garantir que a cópia a ser usada está protegida e integra
- Garantir que as medidas de segurança necessárias foram implantadas de forma correta
- Manter-se alerta durante um período de tempo após o tratamento do incidente

# Fases do Plano de Resposta



- Criar um **Mecanismo** para disseminar a experiência adquirida
  - Palestras, Reuniões, Cartilhas, Intranet, etc.
- Documentar todas as ações Positivas e Negativas
- Melhoria Contínua (Obter estatísticas para *Benchmarks*)
- Evidenciar os Fatores Críticos de Sucesso
- Atualizar Políticas, Normas, PCN, etc.
- Criar Indicadores para Avaliar o Processo
- Criar uma forma de registro duradouro das atividades para disseminação do conhecimento e controle da evolução

## ■ O que não pode faltar em um PRI

- Classificação do Documento
- Pontos de Contato/Comunicação (Departamentos/Áreas e Responsáveis)
  - Plano de Comunicação do Incidente
- Detalhes do Incidente (Classificação, Data, local, Tecnologia, Pessoas e Processos envolvidos, etc.)
- Contextualização do Incidente (possíveis interações com outros incidentes ou localidades)
- Evidências coletadas
- Medidas e Contra Medidas adotadas
- Fechamento e Conclusão do caso
- Padronização na execução
  - Criar uma ficha para cada etapa do Processo de forma a atender a estrutura da organização
- Plano de contingência para o negócio

## Estudo de Caso 2 - PRI

- Empresa multinacional de Produtos Radiológicos
- Altíssima criticidade de processos cuja falha pode comprometer milhares de vidas humanas
- Máquinas e equipamentos controlados por CLP e computadores convencionais, ligados em rede
- Há regulamentações internacionais, como a GAMP, com foco em ações decorrentes do nível de risco
- O case anexo é a primeira versão do documento, elaborado em 2012.

## Trabalho 2

- Elaboração, em grupo, do documento de planejamento de um PRI para a empresa de comércio virtual detalhada em anexo.
- Todas as demandas necessárias para a tomada de decisões devem ser compatíveis com as características típicas de uma empresa deste tipo, e tudo que não estiver explicitamente definido pode ser livremente arbitrado.

- Qual é a utilidade de um GRIS para o negócio de uma corporação ?
- Como devem ser escolhidos os serviços a serem oferecidos ?
- Quais são os fatores críticos de sucesso para um GRIS ?
- Quais são as abordagens de implementação ?
- O que é Forense Computacional ?
- Qual é a utilidade de PRIs para o negócio de uma corporação ?
- Quais são as etapas de um PRI ?
- Qual é a utilidade das “lições aprendidas” de um incidente ?