Guia de Tratamento de Incidentes – SI

(baseado na NIST 800-61/Rev.2)

- Objetivos
  - Ajudar as organizações a lidar e mitigar os riscos de incidentes de segurança;
  - Fornecer orientações práticas sobre como responder a incidentes de forma eficaz e eficiente;
  - Incluir diretrizes sobre o estabelecimento de um programa eficaz de resposta a incidentes;
  - Organizar uma capacidade de resposta a incidentes de segurança de computador (CSIRC) eficaz.

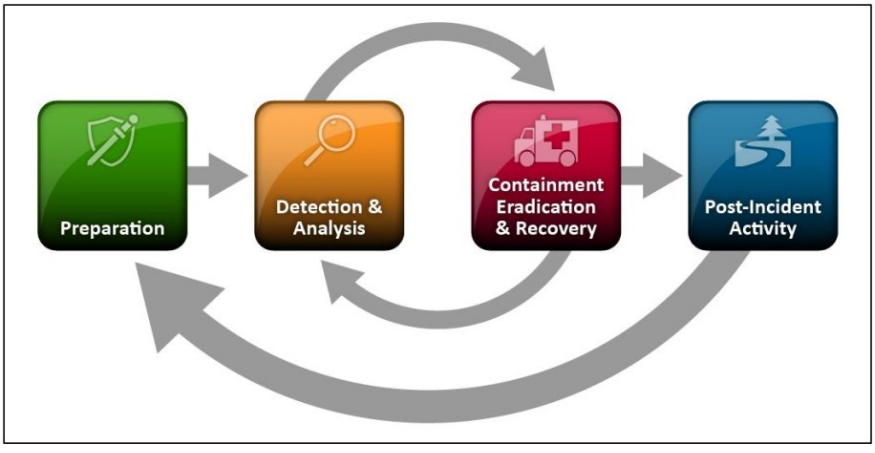
- Estrutura do Time de Resposta a Incidentes (CSIRT):
  - Centralizado → demanda geral em toda a organização;
  - Distribuído → descentralizado, por times em cada segmento/setor;
  - Ainda podem ser formados:
    - Internamente pelos funcionários normais de segurança da informação;
    - Parcialmente terceirizado;
    - Totalmente terceirizado.

- Atribuições do CSIRT:
  - Detecção de Intrusão;
  - Avisos sobre novas tendências de ataques, comunicação, treinamento e conscientização;
  - Compartilhamento de informações com grupos externos e entidades de segurança (ex.: OWASP).

- Dependências dentro da Organização que deverão atuar em conjunto:
  - Gerência → coordenando e atuando na sinergia entre todos os membros;
  - Equipe de TI/Suporte;
  - Equipe Financeira/Seguros/ Compliance/RH/Infraestrutura, etc.;
  - Relações Públicas/Mídia;
  - Departamento Legal da Empresa;
  - Plano de Continuidade de Negócios, etc.

- Principais Recomendações para o tratamento de incidentes:
  - Estabelecer formalmente a capacidade de resposta a incidentes;
  - Criar uma política de resposta a incidentes e desenvolver um plano para executá-lo;
  - Desenvolver procedimentos passo-a-passo para executar a política;
  - Criar políticas/proc. relativos ao compartilhamento de inf. relacionadas a incidentes (mídia, lei, etc.);
  - Considerar o contexto organizacional para adotar o melhor tipo de estrutura de times;
  - Identificar outros grupos na organização que podem precisar participar no tratamento de incidentes;
  - Determinar quais ações e serviços o time irá fornecer, delimitando um escopo de atuação.

- Lidando com o Incidente – Fases:
  - Preparação → estabelecer e treinar uma equipe de resposta e adquirir as ferramentas e recursos necessários;
  - Detecção e Análise → estabeler os principais vetores de ataque e os tipos, logo, como lidar com eles;
  - Contenção, Erradicação e Recuperação → contenha o ataque e depois erradique a ameaça e retorne ao normal;
  - Pós-Incidente → onde deverão ser revistos os procedimentos para melhorar e aprender com os resultados.

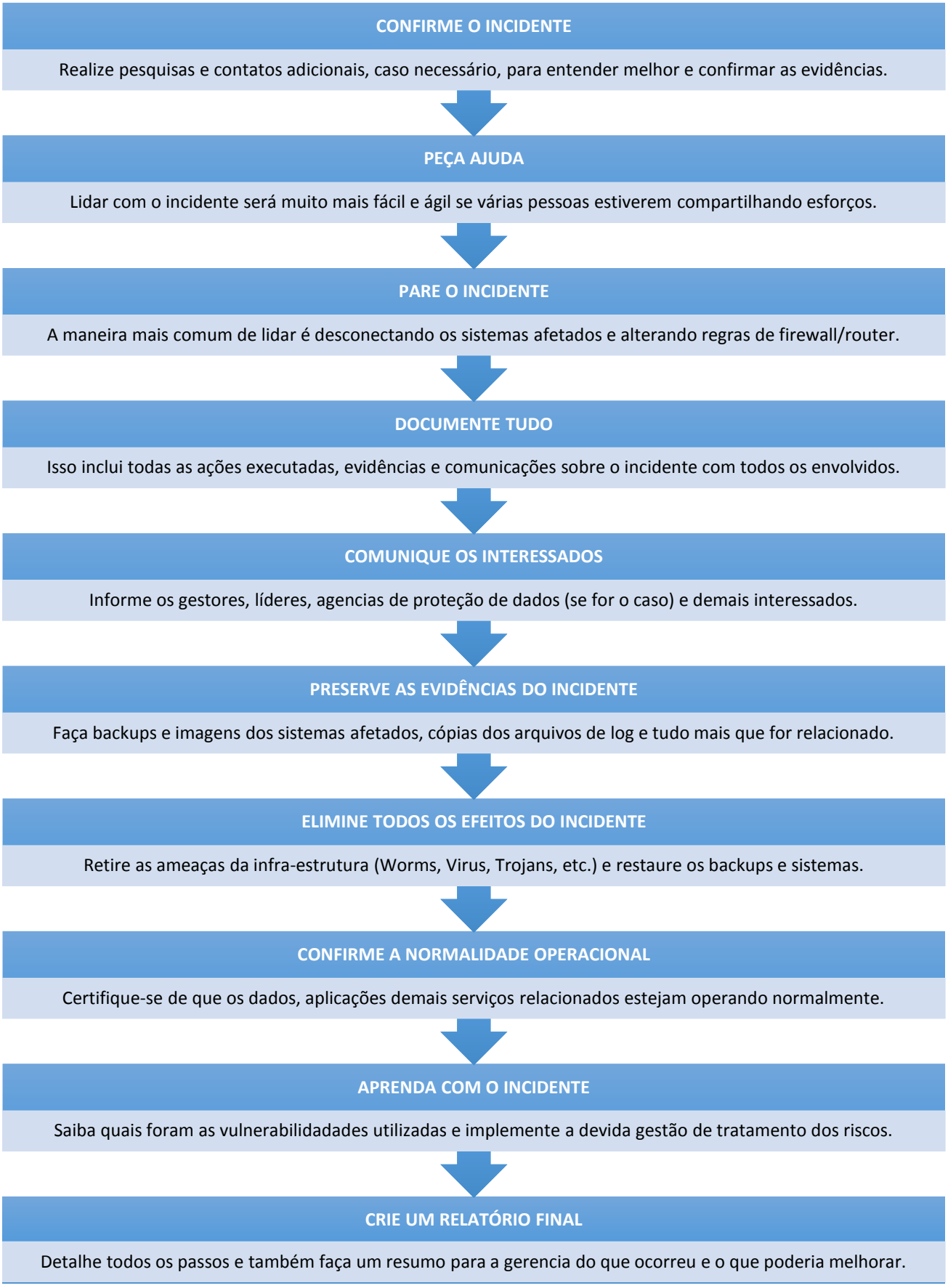


- **<u>Cenário avaliativo para lidar com Incidentes:</u>**

As questões listadas abaixo são aplicáveis a quase todos os cenários. As organizações são fortemente encorajadas a adaptar essas questões e cenários para uso em seus próprios exercícios de resposta a incidentes.

1. Preparação
1.1. A organização consideraria esta atividade um incidente? Em caso afirmativo, quais políticas são violadas?
1.2. Que medidas existem para tentar evitar que este tipo de incidente ocorra ou para limitar seu impacto?
2. Detecção e Análise
2.1 Qual é a origem/evento precursor do incidente? Poderia ser detectado antes de ocorrer?
2.2 Que indicadores do incidente a organização pode detectar? Existe resposta de ação para cada um?
2.3 Quais ferramentas adicionais podem ser necessárias para detectar este incidente específico?
2.4 Como a equipe de resposta a incidentes analisaria e validaria esse incidente? Que pessoal estaria envolvido?
2.5 Para quais pessoas e grupos dentro da organização a equipe relataria o incidente?
2.6 Como o time deveria lidar com a priorização deste incidente?
3. Contenção, Erradicação e Recuperação
3.1 Qual estratégia a organização deve adotar para conter o incidente e qual o motivo desta escolha?
3.2 O que poderia ocorrer se o incidente em questão não fosse tratado?
3.3 Quais ferramentas adicionais podem ser necessárias para responder a este incidente específico?
3.4 Quem (pessoa/função/papel) estaria envolvido nos processos de contenção, erradicação e recuperação?
3.5 Havendo evidências, como elas seriam adquiridas, armazenadas e retidas na organização?
4. Atividades Pós Incidente
4.1 Quem participaria da reunião de lições aprendidas sobre este incidente?
4.2 O que poderia ser feito para evitar que incidentes semelhantes ocorram no futuro?
4.3 O que poderia ser feito para melhorar a detecção de incidentes semelhantes?
Questões de âmbito geral
Quantos membros da equipe de resposta a incidentes participariam no tratamento deste incidente?
Além da equipe de resposta a incidentes, quais grupos (int./ext.) estariam envolvidos no tratamento deste incidente?
Para quais partes externas a equipe relataria o incidente e em que prazo cada reportagem ocorreria?
Como seria criado cada relatório? Quais informações seriam relatadas e por quê?
Que outras comunicações com partes externas poderiam ocorrer?
Quais ferramentas e recursos a equipe usaria para lidar com esse incidente?
Quais seriam os resultados se o incidente ocorresse em um horário de produção/alta demanda ou fora deste?
Que aspectos do tratamento teriam sido diferentes se o incidente tivesse ocorrido em um local físico diferente?

- **<u>Resumo para lidar com incidentes</u>** (*podem ocorrer em paralelo!*)



Dúvidas? Contate o DPO:
https://www.linkedin.com/in/adriano-dpo
https://www.gid.net.br