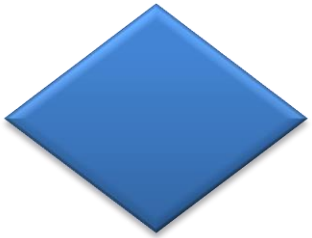
Diretrizes para a coleta e preservação de evidências digitais – NC nº 21

Colóquio do CTIR Gov – 2015

Auditório do Anexo I – Palácio do Planalto

Brasília/DF

Polícia Federal



SRCC/DICOR/DPF

Polícia Federal

Atribuições (em resumo)

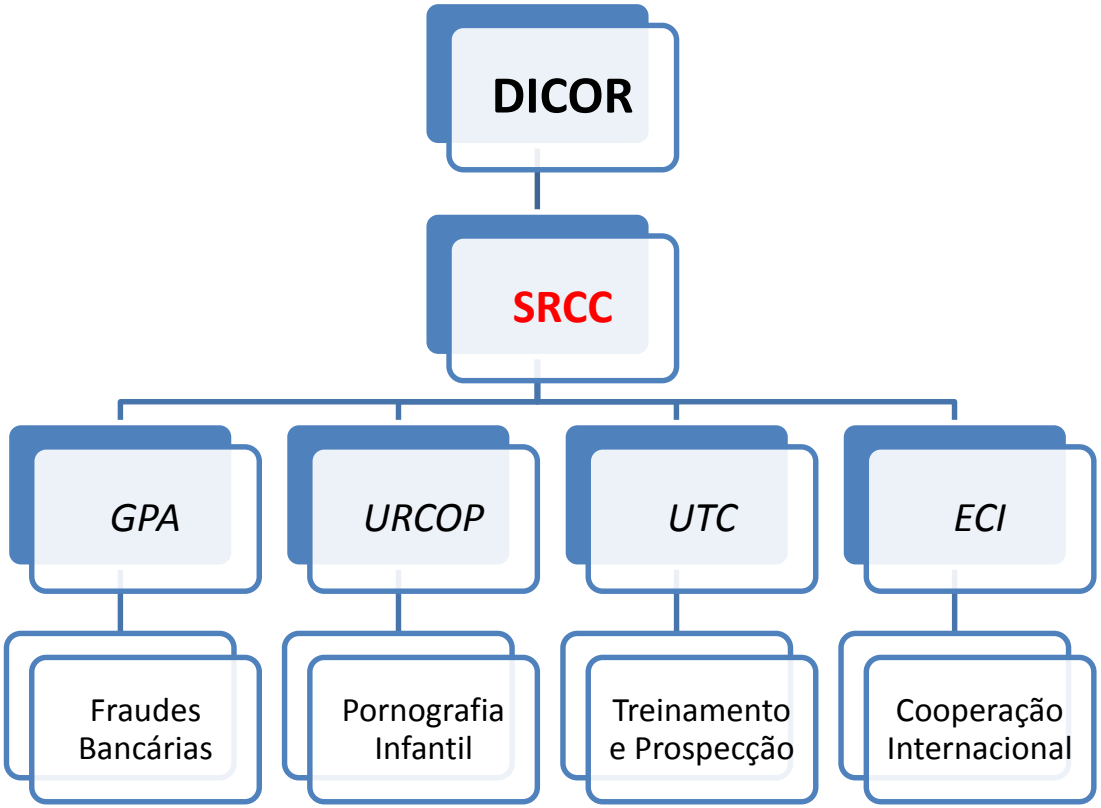
- Polícia judiciária da União
- Infrações de repercussão interestadual e internacional que exigem repressão uniforme
  - Requer autorização do MJ em alguns casos (Internet)
- Tráfico de drogas, contrabando e descaminho
- Polícia marítima, aeroportuária e de fronteiras
- Conflitos agrários

Histórico

- Criada em 2003 para coordenar as ações de:
  - **Combate às fraudes eletrônicas (GPA – Grupo Permanente de Análise)**
    - **Internet banking**
    - **Clonagem de cartões de crédito/débito**
  - Combate a venda de medicamentos na Internet
  - **Combate aos crimes de Alta Tecnologia**
  - **Combate à pornografia infantil (2014 - URCOP)**

SRCC/DICOR/DPF

Estrutura



SRCC/DICOR/DPF

Estrutura

- **GRCC's** constituídos
  - 15 **GRCC's** operacionais
  - Responsável designado nos estados sem GRCC
    - Atuação em 100% do território nacional.

SRCC/DICOR/DPF

Missão

Coordenação

- Combate às fraudes eletrônicas
- Segurança cibernética
- Crimes de alta tecnologia
- Pornografia infantil
- Apoio aos crimes cibernéticos impróprios

Capacitação e Treinamento

- Cursos a distância para difusão do conhecimento básico
- Cursos presencias para aperfeiçoamento e especialização

Desenvolvimento de Tecnologia de Investigação

- Ferramentas específicas para busca de informações e de investigação / inteligência policial

Cooperação Internacional

- Cooperação na área de crimes cibernéticos com outros países e forças policiais

Operações

- Operações 2014/2015 – Fraude Bancária
  - **COURRIEU** (Nov/2014-SP)
    - Desarticular quadrilha responsável pelo desvio de cartões bancários.
    - Aproximadamente R$ 20.000.000,00 em fraudes
  - **IB2K** (Set/2014-DF)
    - Desarticular organização criminosa voltada ao furto de valores de contas de clientes via internet, bem como à lavagem de dinheiro.
  - **TENTÁCULOS III** (Mar/2014-SP)
    - Desarticular organização criminosa especializada em fraude com retenção de cartões bancários nos Estados de São Paulo e Minas Gerais.
    - Aproximadamente R$ 720.000,00 em fraudes
  - **SHEIK** (Mar/2015-GO)
    - Preso o maior fraudador Internet Banking da CEF

SRCC/DICOR/DPF

Projetos

- Tentáculos
  - Base de fraudes bancárias (convênio Caixa e Febraban)
  - Elaboração de relatórios de análise pelo GPA
  - Investigação de quadrilhas
    - Otimização de recursos
    - Redução de inquéritos
- Gênesis
  - Base de denúncias de pornografia infantil
  - Parceiros internacionais
  - Correlação de informações
- Oráculo
  - Coleta de informações em fontes abertas (OSINT)
  - Coleta de informações de análise de malware
  - Coleta de informações de incidentes em ETIR
- Hórus
  - Tramitação de dados telemáticos entre empresas de conteúdo/acesso e a PF

HÓRUS

Crimes Cibernéticos

Normatização Atual

- Legislação atual sobre Crimes Cibernéticos
  - Invasão de dispositivo informático
  - Produção de dispositivo ou software ilícito
  - Obtenção de informações qualificadas e controle remoto
  - Interrupção de serviço
  - Falsificação de cartão de crédito ou débito

- Norma Complementar 21/IN01/DSIC/GSIPR
  - http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf
  - Diretrizes para:
    - Registro de eventos
    - Coleta e preservação de evidências
    - Comunicação às autoridades competentes

Norma Complementar 21

Referencial

- Norma Complementar nº 08/IN01/DSIC/GSIPR
- ABNT NBR ISO/IEC 27037:2013
- RFC 3227

Conceitos Básicos

- Evidência digital:
  - informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento.

Tratamento de Incidentes

Visão geral

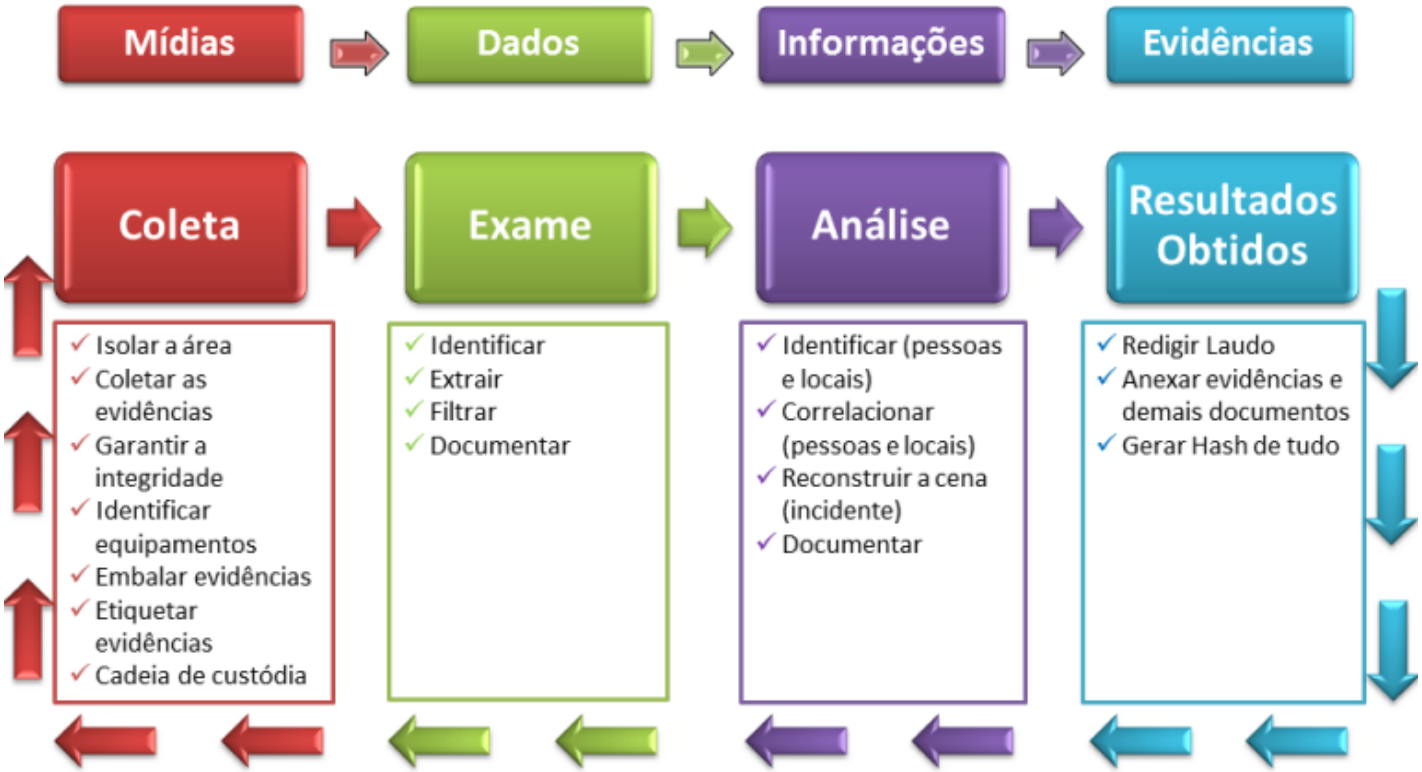
Incidente de Segurança

Tratamento do Incidente

Tratamento das Evidências Digitais

Tratamento de Incidentes

Visão geral



Fonte: http://fdtk.com.br/wiki/tiki-index.php

Tratamento das Evidências

Visão geral

PREPARAÇÃO

- Formalização da ETIR
- Treinamento
- Aquisição de Ferramentas

COLETA

- Definir Metodologia
- Aquisição das Evidências

PRESERVAÇÃO

- Gerar hash
- Gravar em mídia
- Identificar /
- Embalar /
- Etiquetar /
- Transportar e/ou
- Armazenar de forma segura

COMUNICAÇÃO

- Redigir relatório (correlacionar evento/pessoas/local
- Elaborar o termo de custódia
- Anexar evidências coletadas
- Proteger o sigilo/privacidade
- Formalizar a entrega

Tratamento das Evidências

Considerações iniciais

- Fragilidade da evidência digital
- Volatilidade da evidência digital
- Criticidade do ativo afetado

Tratamento das Evidências

Considerações iniciais

- Minimizar o manuseio
- Documentar todas as ações tomadas e modificações resultantes.
- Recursos humanos (ETIR) capacitados

Evidência Digital

Princípios

- Pertinência:
  - a evidência prova ou refuta um elemento do caso.
- Confiabilidade:
  - a **evidência "é o que diz ser".**
- Suficiência:
  - deve-se coletar vestígios suficientes para permitir o exame ou investigação adequados.

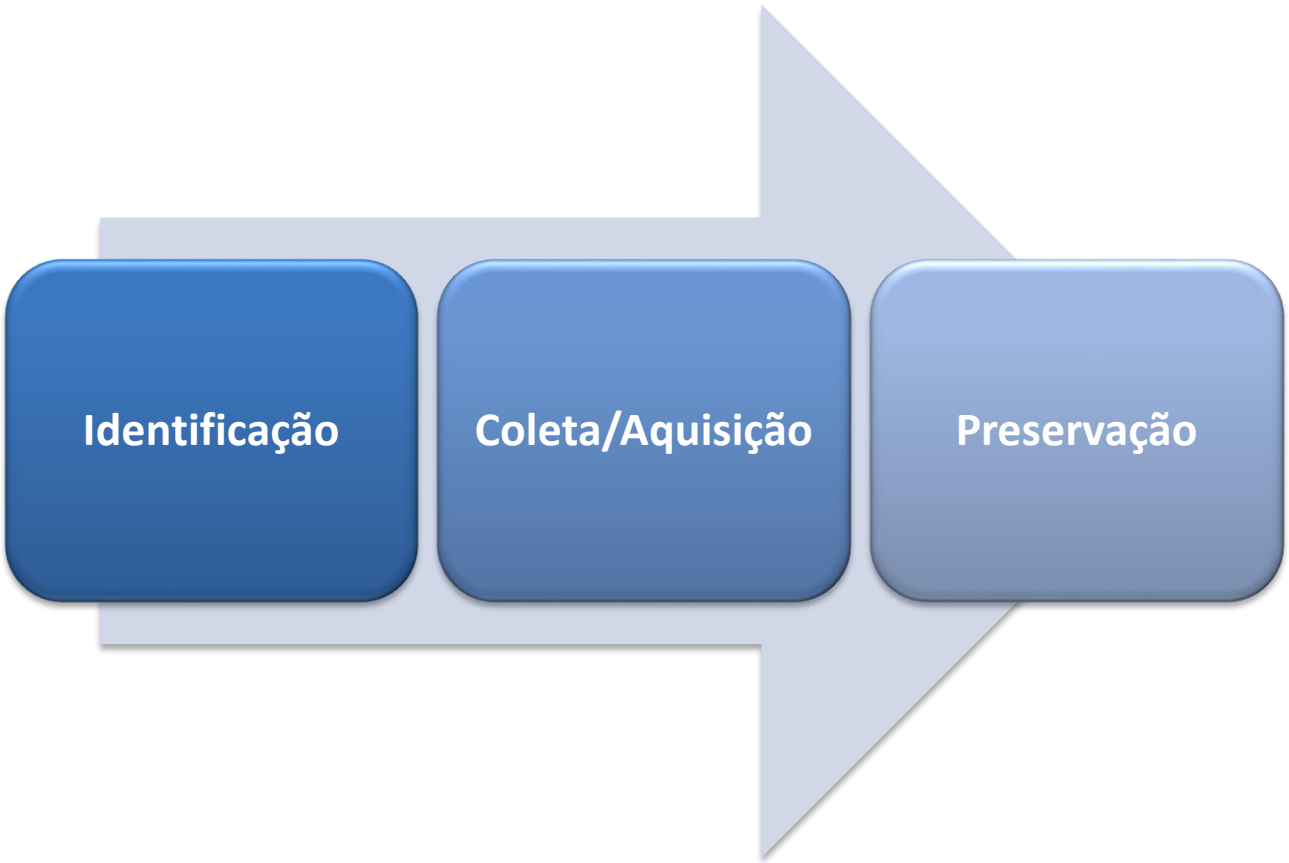
Evidências Digitais

Pontos-chave

- Auditabilidade
- Repetibilidade / Reprodutibilidade
- Justificabilidade

Evidências Digitais

Tratamento



Tratamento das Evidências

Identificação

- Envolve a busca, reconhecimento e documentação
- Priorização com base na importância do ativo e na volatilidade da evidência digital
- Possibilidade de evidências ou ativos ocultos (pendrives, partições criptografadas, etc)

Tratamento das Evidências

Identificação

Tratamento das Evidências

Ordem de volatilidade

1. Registradores, memória cache

2. Tabela de rotas, cache ARP, tabela de processos, RAM

3. Disco rígido

Tratamento das Evidências

Coleta/Aquisição

Tratamento das Evidências

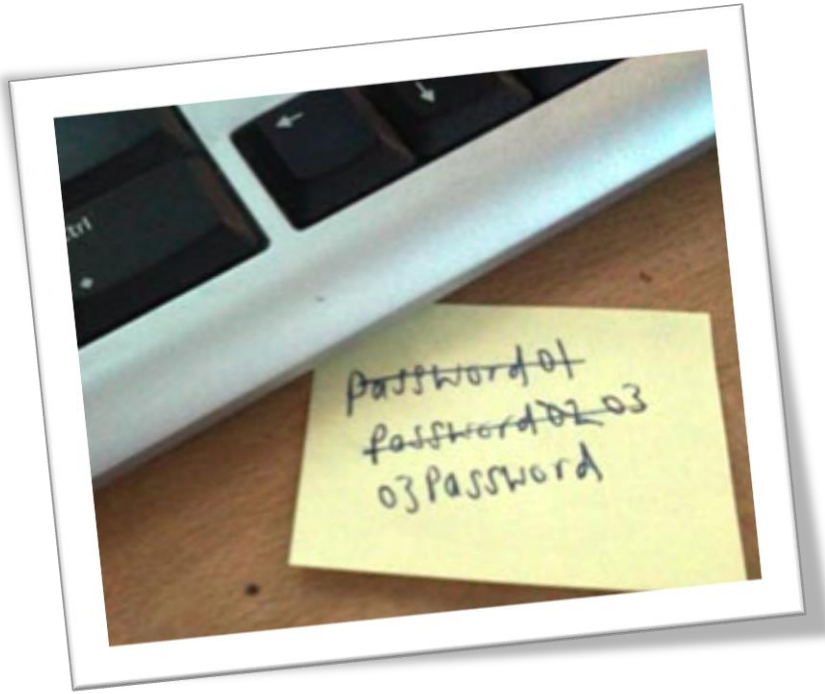
Coleta/Aquisição

- Obtenção dos dispositivos computacionais envolvidos e geração de cópia da evidência digital
- Disco rígido inteiro, partição ou arquivos selecionados
- De acordo com o caso, acondicionar apropriadamente o dispositivo para futura aquisição

Tratamento das Evidências

Coleta/Aquisição

- Evitar sempre que possível métodos que alterem a evidência digital
- Documentar o processo
- Outros materiais (papéis com senhas, cabos de alimentação, etc)



Tratamento das Evidências

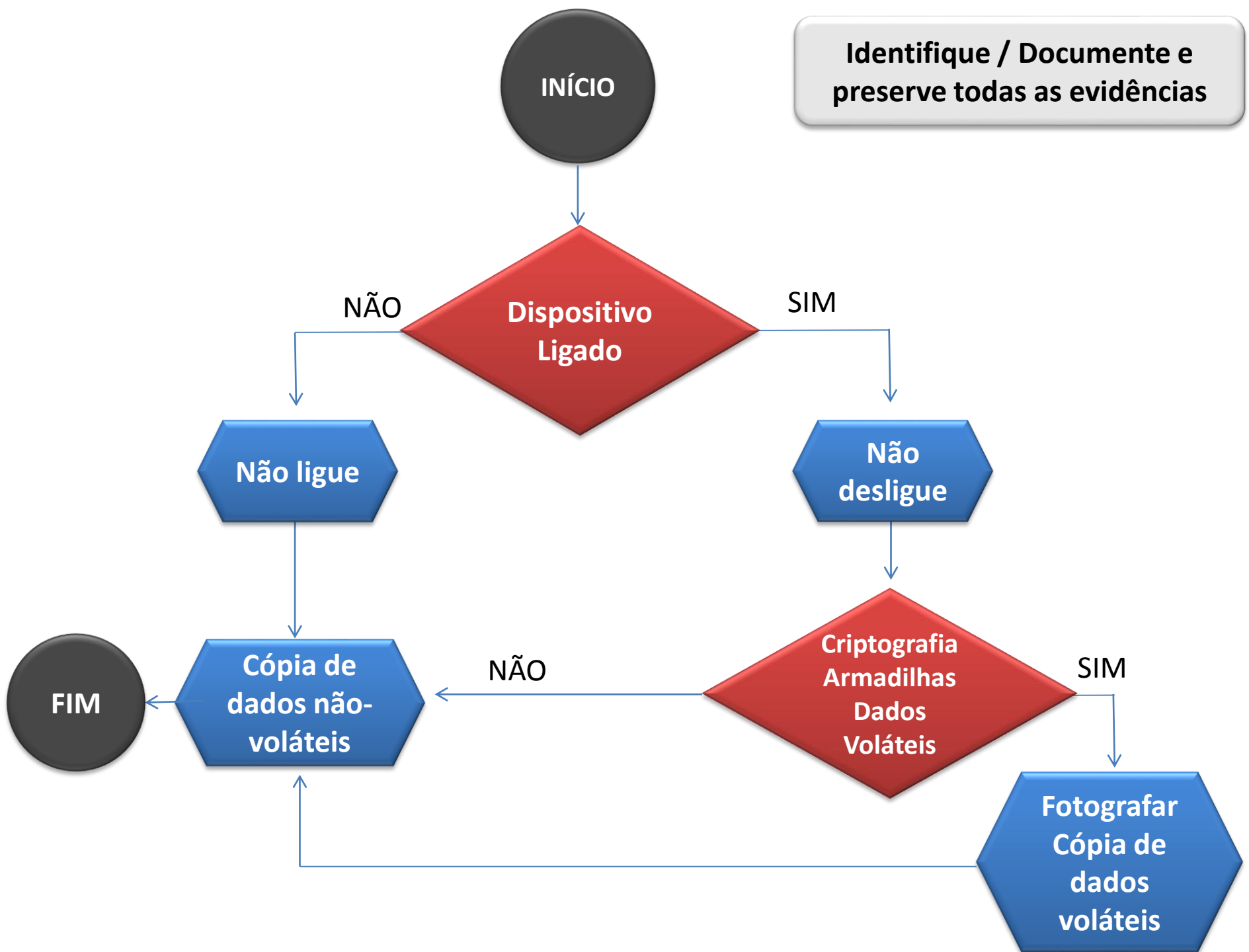
Coleta/Aquisição

- Impossibilidade de cópia da mídia completa:
  - Ex.: disco muito grande, storage, serviço crítico, etc
- Solução:
  - Aquisição lógica (partições, diretórios ou arquivos relacionados ao incidente)

Tratamento das Evidências

Coleta/Aquisição

- Duas situações:
  - dispositivo ligado
  - dispositivo desligado


Identifique / Documente e preserve todas as evidências
INÍCIO
Dispositivo Ligado
NÃO
SIM
Não ligue
Não desligue
Criptografia Armadilhas Dados Voláteis
NÃO
SIM
Cópia de dados não-voláteis
FIM
Fotografar Cópia de dados voláteis

Tratamento das Evidências

Preservação

- Manutenção da integridade e (se for o caso) do sigilo dos dados coletados
- Uso de funções de verificação:
  - resumo criptográfico (*hash*)
- Acondicionamento apropriado:
  - Proteção contra choque, calor, umidade e magnetismo

Norma Complementar 21

Requisitos Importantes

- Fonte de tempo confiável (NTP / HLB / ON)
- Registro de eventos dos ativos de informação
- Registros de eventos (logs) armazenados por no mínimo 6 (seis) meses
- Registro de auditoria armazenados remotamente

Norma Complementar 21

Coleta e Preservação

- Responsabilidade da ETIR
- Mídias de armazenamento
  - Copia dos arquivos caso seja inviável
- Todos os registros de eventos
- Hashes dos arquivos
- Hash do arquivo de hashes
- Material lacrado + termo de custódia

Norma Complementar 21

Comunicação

- Comunicação às autoridades competentes
  - Relatório de comunicação de incidente de segurança
  - Envelope lacrado e rubricado
  - Encaminhamento à autoridade responsável
  - Autoridade responsável encaminha formalmente para a autoridade competente
  - Preocupação com a privacidade e sigilo dos dados custodiados

Norma Complementar 21

Conclusão

- Nova abordagem no tratamento de incidentes
- Foco na comunicação para investigação
  - Não apenas reestabelecimento do serviço
- Importância da coleta, preservação, sigilo e custódia de evidências
- Relação ETIR x Autoridades Competentes (PF)

Exemplos de cursos

- Escola Superior de Redes – ESR/RNP:
  - Análise forense (http://esr.rnp.br/seg3)
- CERT.br:
  - FIH e AIH (http://www.cert.br/cursos/)