# Guia Prático: Investigação de Ilícitos Cibernéticos (PIILC-PJ)

## Preparação e Adequação Técnica

### Sincronização por Hora Legal Brasileira

Todos os ativos devem seguir o horário oficial do Observatório Nacional.


### Registro Detalhado de Eventos

Logs devem identificar usuários, IPs, portas de origem e a natureza do evento.

### Dados Essenciais no Registro de Auditoria

**Identificação do Usuário**
Nome ou ID único de quem acessou o recurso.

**Natureza do Evento**
Sucesso/falha de autenticação ou troca de senha.

**Dados de Conexão**
Endereço IP e porta de origem da conexão.


### Armazenamento Mínimo de 6 Meses

Registros de ativos críticos devem ser armazenados remotamente por este periodo.

## Resposta e Coleta de Evidências

### Prática Forense Digital

A coleta deve garantir a confidencialidade, integridade e autenticidade das informações.


### Relatório de Incidente de Segurança

Documento obrigatório contendo tratamento, melhorias e lições aprendidas sobre o caso.

**Ministério Público**

**Polícia**

### Acionamento de Órgãos Competentes

Fatos penalmente relevantes precisam ser comunicados ao Ministério Público e à polícia.