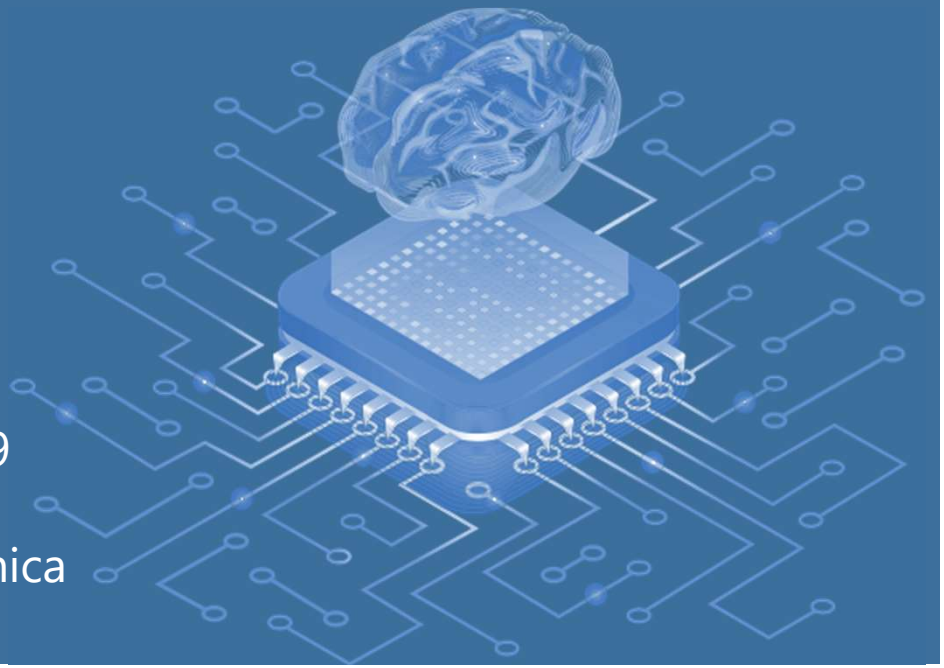
Investigações Internas e Negociação de Acordos
Aspectos Teóricos e Práticos

Tecnologia Forense
IBRAC - 22 de abril de 2021



Felipe Leitão Valadares Roquete
Coordenador-Geral de Análise Antitruste 09
Superintendência-Geral
Conselho Administrativo de Defesa Econômica

Disclaimer

O conteúdo da apresentação reflete a visão pessoal do autor e não representa, portanto,
o posicionamento oficial do Cade ou de qualquer outro órgão do Governo Federal.

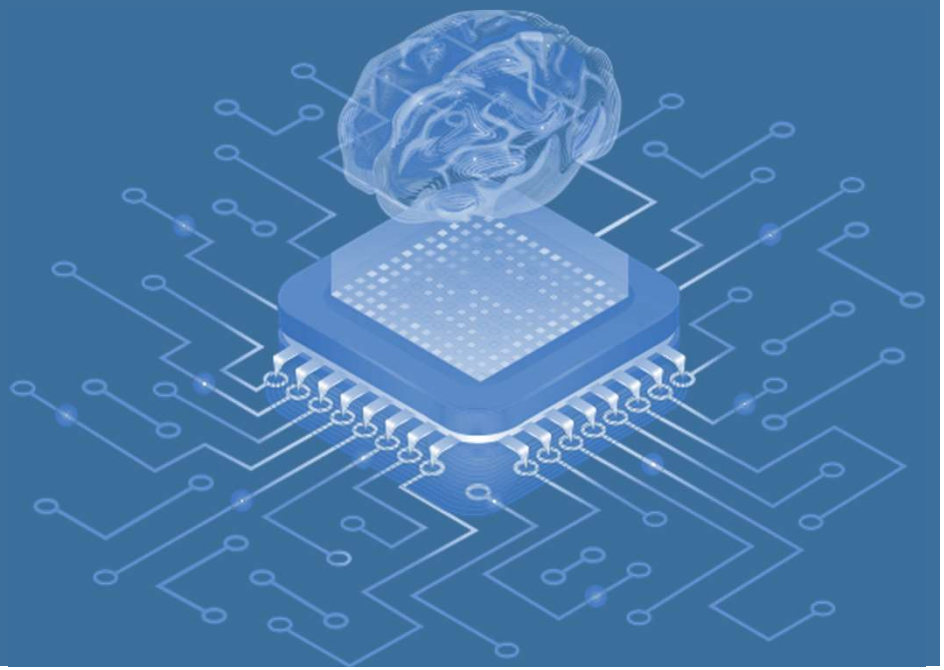
Sumário

O que não será abordado

Detalhes técnicos de ferramentas forenses

Casos concretos

Contexto



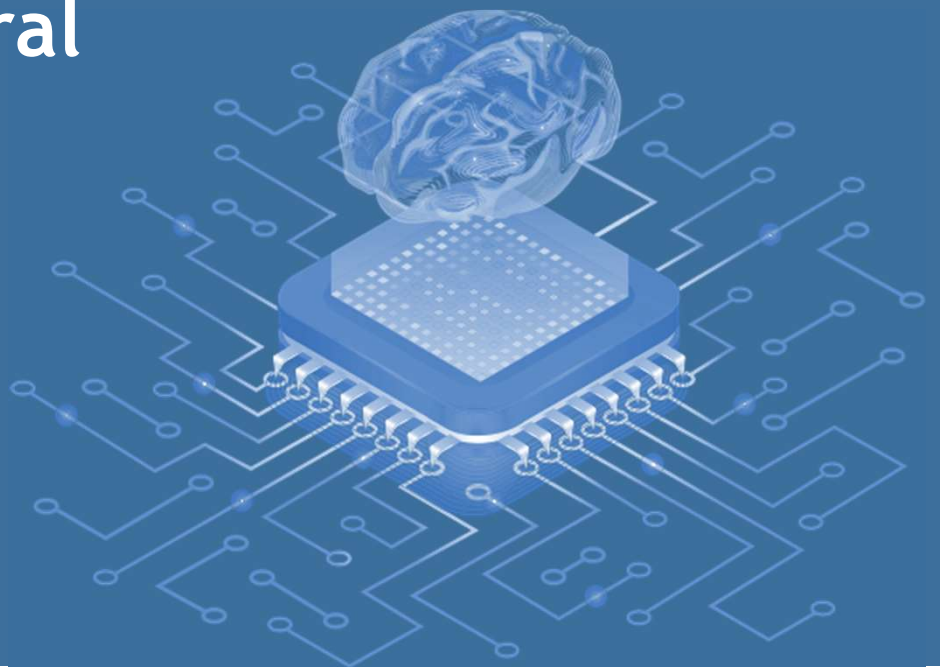
Contexto

Documentos eletrônicos

Pervasivos
Adaptabilidade
. Tecnologia
. Novos arranjos corporativos

Ponto de interseção
. Confiança, credibilidade, custo

Atuação da Superintendência-Geral

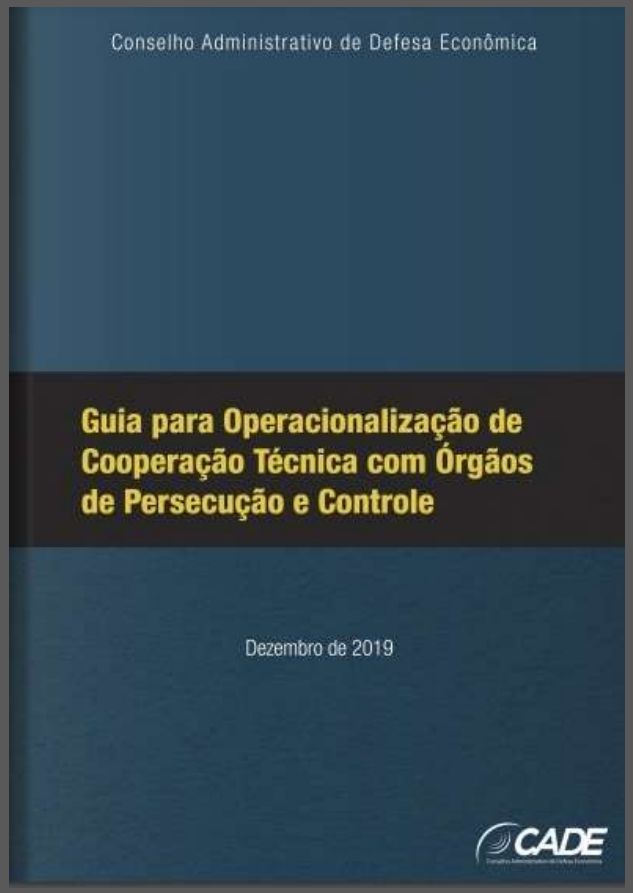


Atuação da Superintendência-Geral

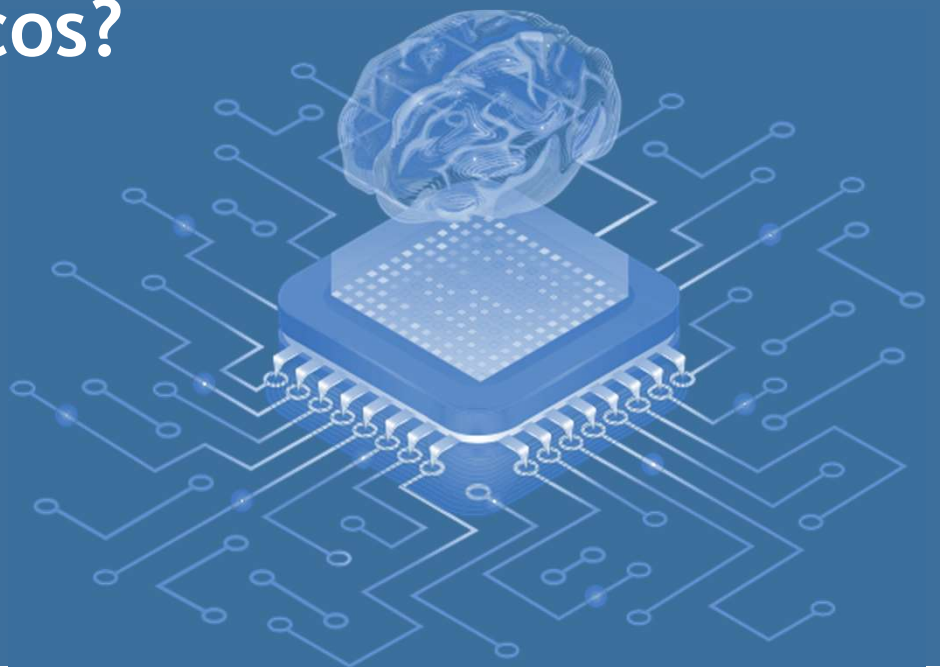
Princípios

Preservação da cadeia de custódia
Procedimentos técnicos
. ABNT NBR ISO/IEC 27037:2013: *Diretrizes para identificação, coleta, aquisição e preservação de evidência digital*
.*United Nations Office on Drugs and Crime (UNODC)*
Transparência
Problem-driven
Garantia do pleno exercício do direito de defesa

Atuação da Superintendência-Geral



Como lidamos com os documentos eletrônicos?



Como lidamos com os documentos eletrônicos?

Diligência criminal

Autorização judicial

Apoio técnico

Prova emprestada

Cadeia de custódia criminal

Como lidamos com os documentos eletrônicos?

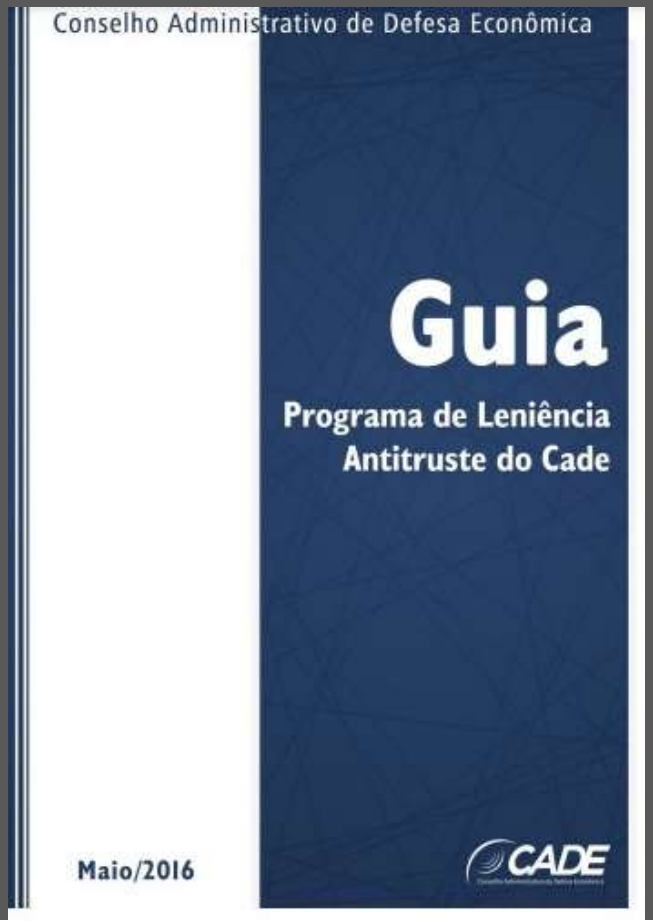
Diligência cível

Benchmarking

Procedimento operacional padrão: parcimônia e celeridade

Abordagem procedimental

Como lidamos com os documentos eletrônicos?



FR1

49. Quais os cuidados que o proponente do Acordo de Leniência deve ter na coleta dos documentos eletrônicos e físicos?

Slide 13

FR1 É importante que os proponentes do Acordo de Leniência tomem cuidados técnicos durante a coleta das evidências. Via de regra, o proponente deve registrar a cadeia de custódia dos documentos eletrônicos e físicos que serão submetidos ao Cade, ou seja, a história cronológica da evidência, apresentando informações específicas dos responsáveis pela coleta. Além disso, para documentos eletrônicos, o proponente do Acordo de Leniência deve, via de regra, ser capaz de descrever o método de extração das evidências, ou seja: a) identificar os dispositivos (CPU, Servidor de e-mails, notebook e pendrive) de onde foram obtidas as evidências e quem eram os proprietários/custodiantes/usuários dos equipamentos e/ou dos arquivos extraídos; b) identificar os procedimentos adotados e equipamentos/softwares utilizados na extração da evidência. Descrever, por exemplo, se foi realizada uma imagem forense do HD, detalhando qual tipo de imagem (AD1, E01, DD); se foi utilizado bloqueador de escrita, detalhando qual modelo; qual hash obtido da imagem (MD5, SHA1); e qual a data da coleta e o local; c) identificar os tipos de arquivos extraídos e softwares compatíveis para abrilos com as versões (por exemplo, arquivos de e-mail, Lotus Notes, Outlook, arquivo de banco de dados); d) informar outros dados relevantes para o caso. Ademais, via de regra, o proponente 35 do Acordo de Leniência deve ser capaz de descrever o método de análise/perícia das evidências eletrônicas, explicitando qual(is) software(s) foi(ram) utilizado(s) e quem realizou a análise. Em se tratando de e-mails, além das informações acima, devem ser apresentadas as informações de metadados do cabeçalho (Header) de cada e-mail, tais como: From, To, Cc, Bcc, Subject, Date, Delivery Date, Received, Return-Path, Envelop-to, Message-id, Mime-version, Content-type, etc. Ressalte-se que o proponente do Acordo de Leniência deve preservar, sempre que possível, os discos rígidos ou equipamentos originais (de onde foram extraídas as evidências) e/ou sua imagem forense autenticada preservada sem alterações; bem como extrair números hash dos documentos originais, pois podem ser solicitados pela Superintendência-Geral do Cade durante as investigações. É possível apresentar ao Cade os discos rígidos ou equipamentos originais, sempre que isso for factível. Em regra, quando os documentos apresentados não forem os originais, deve ser fornecida, comprovação de que os originais existem ou, então, a justificativa de sua inexistência. A SG/Cade avaliará, caso a caso, os cuidados tomados para garantir a autenticidade dos documentos ao original. Ressalta-se, de todo modo, que eventual impossibilidade no prosseguimento de alguns dos procedimentos mencionados não invalida a possibilidade de utilização dos documentos apresentados.

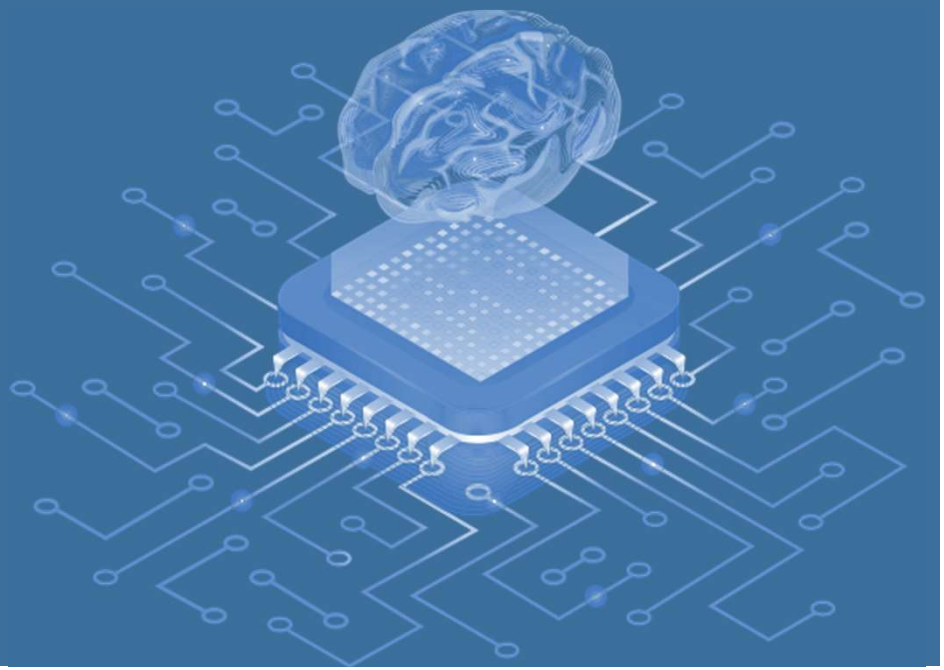
Felipe Roquete; 04/04/2021

Como lidamos com os documentos eletrônicos?

V.9 Orientações para elaboração de Relatório de certificação eletrônica

Solicitações gerais 1. Esse modelo é meramente sugestivo. Situações especiais poderão ser discutidas, a depender do tipo e formato de evidência a ser apresentada. Este modelo não é um questionário, mas sim um documento a ser apresentado e assinado pelos Compromissários.

Conclusões



Conclusões

Benchmarking

Princípios

Abordagem procedimental

Problem-driven

Muito obrigado!