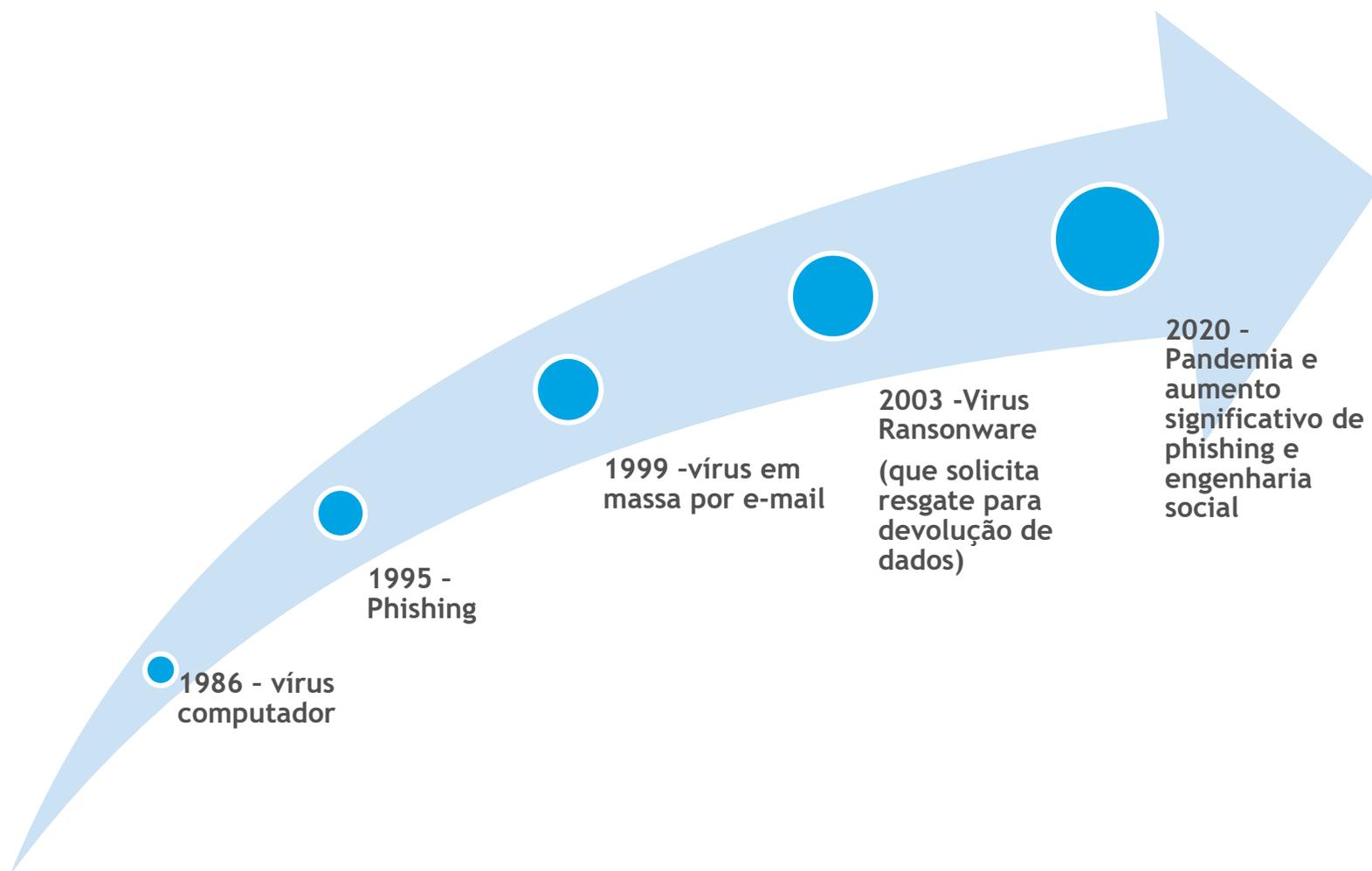


# SPEAR PHISHING E SERVIÇOS DE INVESTIGAÇÕES

PALESTRA REALIZADA NA CÂMARA DE COMÉRCIO E INDÚSTRIA JAPONESA DO BRASIL, EM 19/04/2023.

FID - (FRAUDES, INVESTIGAÇÕES E DISPUTAS)

# EVOLUÇÃO DAS FRAUDES TECNOLÓGICAS





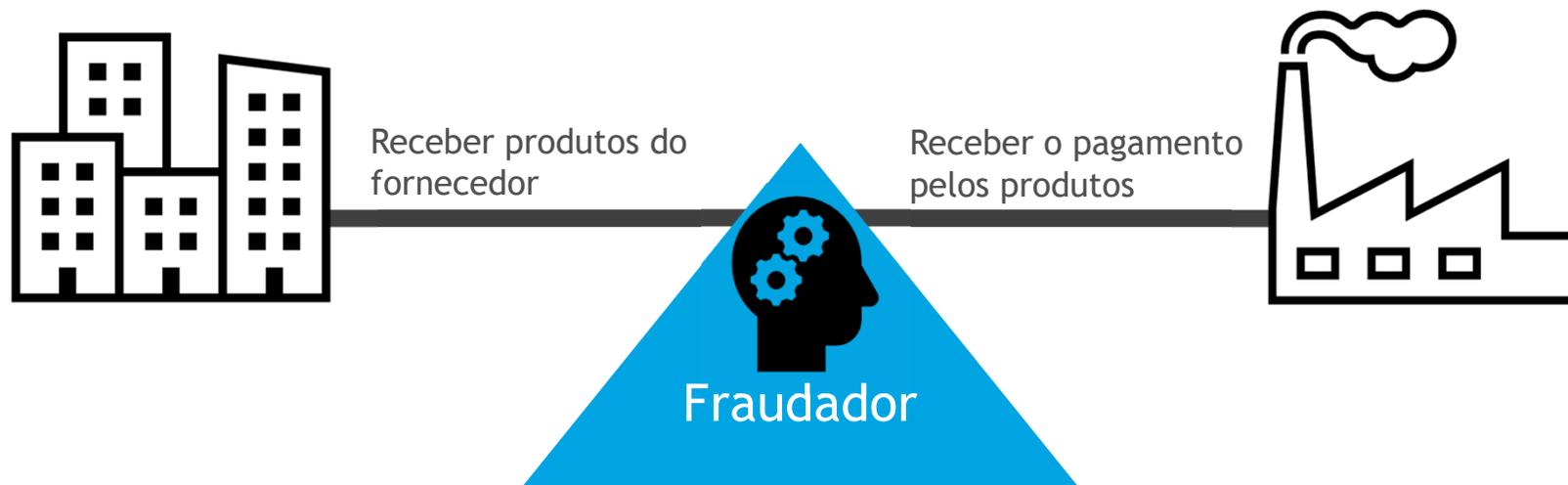
# SPEAR PHISHING

## O que é?

Diferente do Phishing, onde os fraudadores atuam de modo aleatório para obter informações, o Spear Phishing é mais elaborado.

No Spear Phishing o fraudador conhece o ambiente em que está se envolvendo e tenta personificar uma pessoa chave. Muitas vezes ele monitora as atividades de uma pessoa por dias até conseguir a oportunidade de agir.

## SPEAR PHISHING



- Criam um domínio de e-mail semelhante ao do fornecedor ou da empresa.
- Criam conta de Whatsapp com foto das pessoas envolvidas na negociação.

# SPEAR PHISHING

*Olá John!*

*Tivemos um problema no galpão onde os computadores seriam entregues. Estou lhe enviando outro endereço para realizar a entrega das máquinas.*

*Ressalto a urgência de recebermos esses computadores ainda hoje!*

*Ellen Smith*

*CFO, ABC Industries*

## **Exemplos de endereços alterados:**

- Endereço original: ellen\_smith@abcindustries.com
- Endereço falso: ellen\_smith@abcindustriies.com
- Endereço falso: ellen\_smith@abdindustries.com



# SPEAR PHISHING

## Curiosidades:

- O fraudador possui documentos reais da empresa (NF, fatura, pedido de compra etc.).
- Conhece a operação (quantidade de produtos, contexto de negociações, pessoas envolvidas etc.).

Como o fraudador obtêm os documentos e conhece o contexto?



# SPEAR PHISHING

## Possibilidades:

- Conta de e-mail está sendo monitorada ou o fraudador possui acesso a rede da empresa.
- Documentos estão na internet e todo conhecimento é obtido publicamente (LinkedIn, redes sociais, site da empresa etc.).
- Funcionários de dentro da empresa ou no fornecedor estão ajudando o fraudador (ou são os fraudadores).



# SPEAR PHISHING

## Possíveis controles:

- Controles e políticas de segurança da informação.
- Conscientização dos funcionários.
- Dupla autenticação em contas de e-mail e rede.
- Atualizações de softwares e antivírus.

# SPEAR PHISHING

## Possíveis controles:

- Utilização de sistemas de e-procurement para controlar as compras da empresa (tudo ocorre dentro da plataforma).
- Limitar a publicação de informações em redes sociais ou monitorar o que está online.
- Qualquer alteração de cadastro deve ser confirmada com um contato confiável do fornecedor.
- Alçada de aprovações para as alterações de cadastro.
- Garantir que os fornecedores da empresa tenham controles e políticas de segurança da informação.



## SPEAR PHISHING

### O que se pode fazer quando ocorre um Spear Phishing?

Pontos de Investigação que podem trazer evidências:

- Imagens ou fotos enviadas podem conter metadados importantes.
- Documentos enviados e contexto explorado pelo fraudador podem delimitar as suspeitas internas.
- Logs de acesso aos e-mails da empresa podem demonstrar anormalidades.
- Registros de telefonia podem demonstrar possíveis contatos internos com o fraudador.



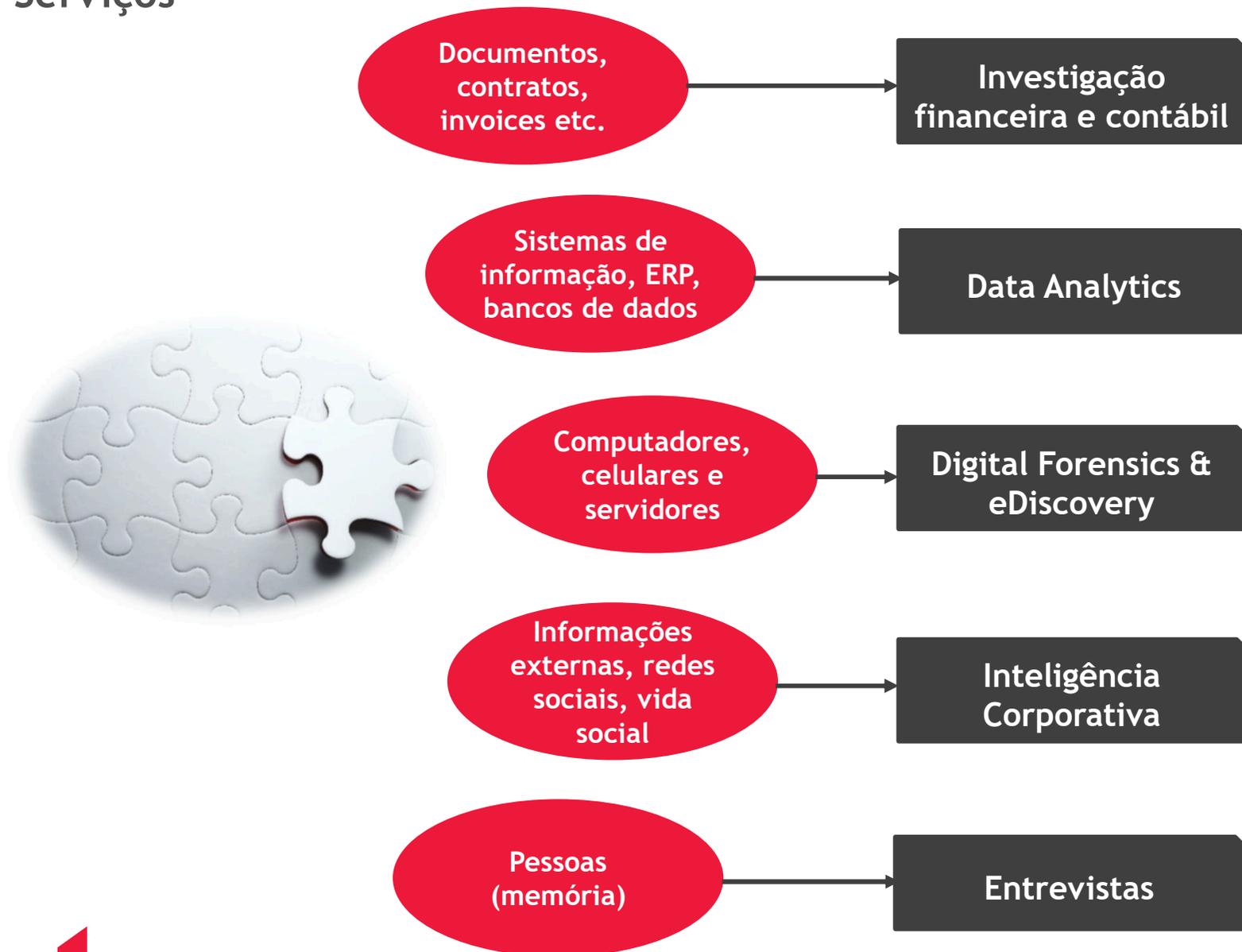
# SPEAR PHISHING

Serviços de investigação



# FID - FRAUDES, INVESTIGAÇÕES E DISPUTAS

## Serviços



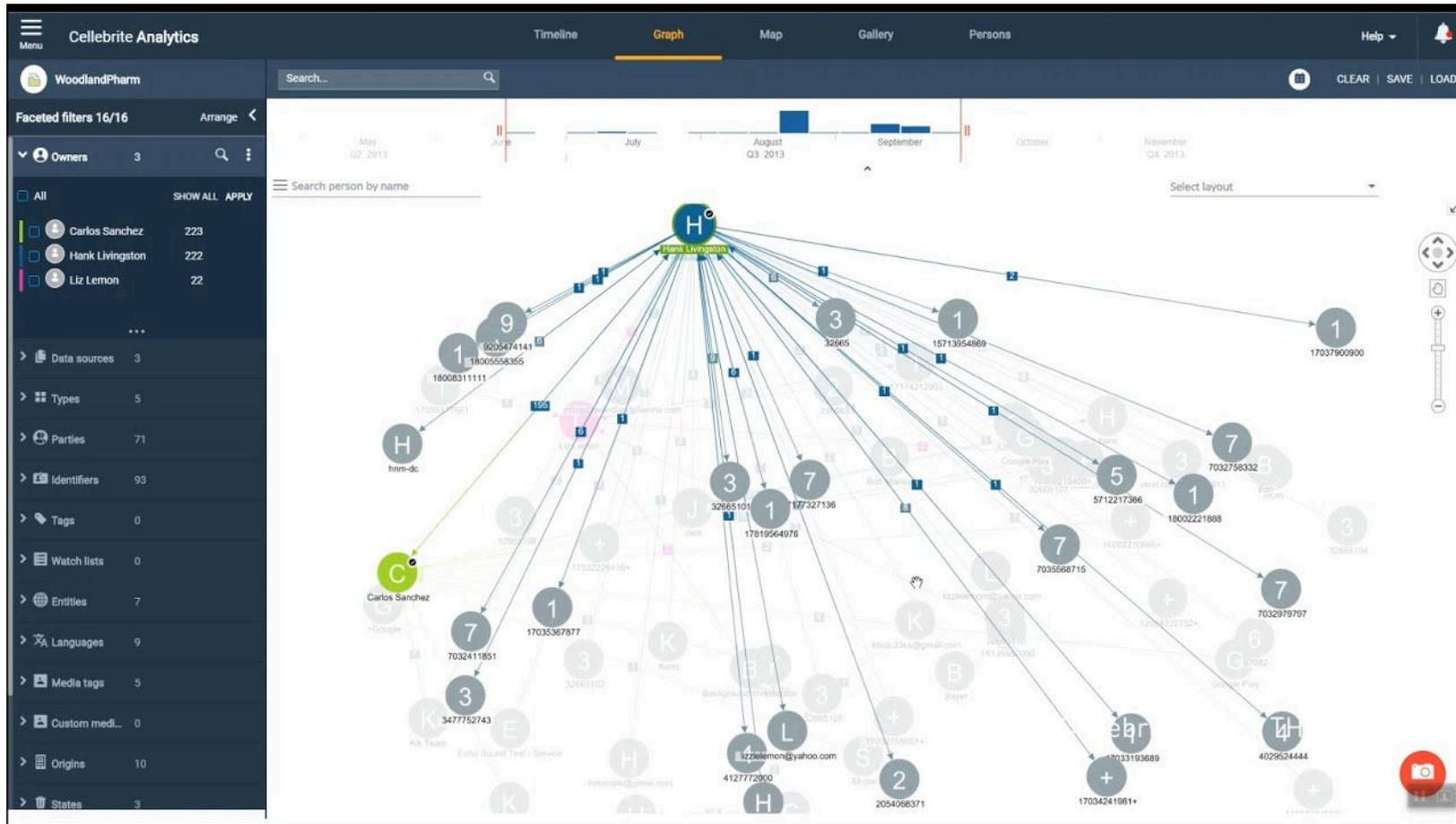
# FRAUDES, INVESTIGAÇÕES E DISPUTAS

## Ferramentas



# FRAUDES, INVESTIGAÇÕES E DISPUTAS

## Ferramentas



# FRAUDES, INVESTIGAÇÕES E DISPUTAS

## Ferramentas

The screenshot displays the UFED Cloud Analyzer interface. The top navigation bar includes 'FILE', 'VIEWS', 'REPORT', 'EXPORT', and 'HELP'. Below this, there are tabs for 'Extractions summary', 'Timeline table', 'Timeline feed', 'Files', 'Contacts', and 'Map'. The 'Map' tab is active, showing a map of the United States and Mexico with 392 events and 0 points of interest. A search bar for 'oren' is visible. The left sidebar lists data sources such as Facebook, Gmail, Google Calendar, Google Chrome Sync, Google Contacts, Google Drive, Google Location History, Google MyActivity, and Google Passwords, each with a 'Cloudio Brite' status indicator. The main map area shows a red pin on Houston, Texas, and a blue pin on Las Vegas, Nevada. Below the map, a table displays 68 events with columns for Time, Source, Category, Originator, and Content. The selected event is from 02/12/2016 23:33 +0200, with content 'Location: 29.9879577;-95.3325806'. The right sidebar shows a detailed view of the selected location, including a map snippet and the coordinates 29.9879577;-95.3325806, with an accuracy radius of 65 meters.

Time	Source	Category	Originator	Content
02/12/2016 00:22 +0200	Cloudio Brite	Location	Cloudio Brite	Location: 29.9866191;-95.3300896
02/12/2016 00:03 +0200	Cloudio Brite	Location	Cloudio Brite	Location: 29.9879417;-95.3326242
01/12/2016 23:49 +0200	Cloudio Brite	Location	Cloudio Brite	Location: 29.9879257;-95.3326149
02/12/2016 23:33 +0200	Cloudio Brite	Location	Cloudio Brite	Location: 29.9879577;-95.3325806
01/12/2016 23:28 +0200	Cloudio Brite	Location	Cloudio Brite	Location: 29.9879111;-95.3325827
01/12/2016 23:28 +0200	Cloudio Brite	Location	Cloudio Brite	Location: 29.9879111;-95.3325827

# FRAUDES, INVESTIGAÇÕES E DISPUTAS

## Ferramentas





# FRAUDES, INVESTIGAÇÕES E DISPUTAS

## Ferramentas

The screenshot displays an email client interface. At the top, there is a blue header bar with a back arrow and the text "Return to document list". Below this, the email ID "EN11" is shown. A dropdown menu is set to "Extracted Text". The email content includes a header with the following details:

- Sent: Wednesday, October 23, 2003 2:07 PM
- To: Paul Allen <pallen@enron.com>; John Arnold <jarnold@enron.com>
- Subject: Feedback requested
- Attach: ConfidentialEnron.docx

The body of the email reads:

Hi All,  
Could you take a look at the attached document and give me some feedb  
Thanks!  
Mike

Below the email content is a "Thread Group" diagram for "C00006b33". The diagram consists of eight numbered columns (1-8) representing messages. Column 1 contains a black square (Inclusive) with a red arrow pointing to it. Column 2 contains a black square (Inclusive). Column 3 contains a white square (Not Inclusive). Column 4 contains a black square (Inclusive). Column 5 contains a white square (Not Inclusive). Column 6 contains a black square (Inclusive). Column 7 contains a white square (Not Inclusive) with a smaller white square (Attachment) below it. Column 8 contains a black square (Inclusive). Arrows indicate the flow of the thread between these messages. A legend on the right side of the diagram defines the symbols: a black square for "Inclusive", a white square for "Not Inclusive", a square with a question mark for "Missing", a square with a document icon for "Duplicate Spare and Other", and a square with a document icon for "Attachment".

Carlos Dias da Silva - Sócio da área de FID  
(Fraudes, Investigações e Disputas)

BDO BRAZIL

[carlos.dias@bdo.com.br](mailto:carlos.dias@bdo.com.br)

[www.bdo.com.br](http://www.bdo.com.br)



ATTITUDE CHANGES  
EVERYTHING