

SUMÁRIO

ÍNDICE DE FIGURAS.....	27
ÍNDICE DE TABELAS.....	29
ABREVIATURAS E SIGLAS	31

1

INTRODUÇÃO.....	33
-----------------	----

2

O ESTADO DA ARTE E HIPÓTESE DE INVESTIGAÇÃO.....	39
2.1. Diplomas Legais de Proteção de Dados.....	46
2.2. Normas Técnicas Internacionais.....	52
2.3. Ferramentas <i>Cloud Forensics</i>	57
2.4. Hipótese de Investigação.....	61

3

CLOUD FORENSICS	63
3.1. Desafios	65
3.2. Resposta a Incidentes de Segurança Informática	69

4

CONFORMIDADE LEGAL	71
4.1. Teoria Pentadimensional do Direito (Fato-Valor-Norma- -Tempo-Espaço)	72
4.2. Diplomas de Cooperação Internacional.....	76
4.3. <i>Code d'instruction Criminalle</i>	80
4.4. Transferência Internacional de Dados.....	82
4.5. Acesso Legítimo.....	83
4.6. Acesso às Credenciais	86

5

CONFORMIDADE TÉCNICA	89
5.1. Aquisição via Ferramentas <i>Cloud Forensics</i>	95
5.1.1. E3:DS da Paraben Corporation	97
5.1.2. Evidence Center da Belkasoft/Belkasoft X.....	99
5.1.3. Análise Comparativa	105
5.2. Aquisição de VM e/ou <i>buckets</i> em <i>Cloud IaaS</i>	107
5.2.1. Google <i>Cloud</i>	109
5.2.2. Microsoft Azure	116
5.2.3. Amazon AWS.....	119

SUMÁRIO

5.3. Aquisição via download direto.....	123
5.3.1. Google Drive.....	124
5.3.2. Dropbox.....	125
5.3.3. OneDrive	127
5.3.4. Correio eletrônico.....	128

6

CONSIDERAÇÕES FINAIS	131
6.1. Considerações Técnicas.....	132
6.2. Considerações Legais	134
6.3. Conclusão.....	136

7

APÊNDICES	137
7.1 PNSI – Política Nacional de Segurança da Informação.	137
7.2 ENSC – Estratégia Nacional de Segurança Cibernética	141
7.3 Diretiva SRI da UE.....	151
7.4 Instrução Normativa N° 5	156
REFERÊNCIAS	165

ÍNDICE DE FIGURAS

<i>Figura 1 – Modelagem de Cloud</i>	42
<i>Figura 2 – Características Cloud Computing</i>	44
<i>Figura 3 – ISO para Conformidade Técnica</i>	53
<i>Figura 4 – Grau de Complexidade – Composição</i>	66
<i>Figura 5 – Resumo dos Desafios do Cloud Forensics</i>	68
<i>Figura 6 – Teoria Pentadimensional do Direito</i>	74
<i>Figura 7 – Exemplo de Sequência de Investigação</i>	87
<i>Figura 8 – Exemplo de processo nas políticas de compliance</i> ...	88
<i>Figura 9 – Forense em Cloud por mandado judicial</i>	91
<i>Figura 10 – Forense em Cloud por determinação da Organização</i>	92
<i>Figura 11 – Processo Forense</i>	92
<i>Figura 12 – WebBrowserPassView</i>	93
<i>Figura 13 – Remote Desktop PassView</i>	94
<i>Figura 14 – Paraben Corporation Tela 1</i>	97
<i>Figura 15 – Ícone do Cloud Import no Paraben</i>	98
<i>Figura 16 – Sucesso na Aquisição do Correio Eletrônico da Google</i>	98
<i>Figura 17 – Sucesso na Aquisição do Conteúdo do Google Drive</i>	99
<i>Figura 18 – Tela Acquire Cloud Belkasoft</i>	100
<i>Figura 19 – Tela Acquire Cloud (E-Mail) Belkasoft</i>	101
<i>Figura 20 – Tela Acquire Cloud (Google) Belkasoft</i>	101

<i>Figura 21 –</i> Árvore de aquisição de <i>e-mail</i>	102
<i>Figura 22 –</i> Dashboard Belkasoft X.....	103
<i>Figura 23 –</i> Opções de Aquisição Belkasoft X.....	103
<i>Figura 24 –</i> Opções de Aquisição em Cloud Belkasoft X.....	104
<i>Figura 25 –</i> Árvore do Correio Eletrônico recolhido.....	104
<i>Figura 26 –</i> Google Cloud – Recursos.....	109
<i>Figura 27 –</i> Google Cloud – Instâncias de VM.....	110
<i>Figura 28 –</i> Google Cloud – Criar um Imagem.....	111
<i>Figura 29 –</i> Google Cloud – Exportar Imagem para Google Cloud Storage.....	112
<i>Figura 30 –</i> Cloud Storage – <i>bucket</i> "backupipbeja".....	113
<i>Figura 31 –</i> Download do arquivo "recolhagooglegcloud.vmdk".....	113
<i>Figura 32 –</i> <i>Add Evidence</i> do "recolhagooglegcloud.vmdk" no AccessData FTK Imager.....	114
<i>Figura 33 –</i> Sequência para Conformidade e Eficiência na Aquisição no Google Cloud.....	115
<i>Figura 34 –</i> Microsoft Azure – URL para download.....	117
<i>Figura 35 –</i> Download do arquivo "abcd" com formato VHD.....	117
<i>Figura 36 –</i> Recursos Microsoft Azure.....	118
<i>Figura 37 –</i> Sequência para Conformidade e Eficiência na Aquisição de VM no Microsoft Azure.....	118
<i>Figura 38 –</i> Amazon S3 – <i>bucket</i> e arquivo para download.....	120
<i>Figura 39 –</i> Tela de exportação da imagem da VM para o <i>bucket</i>	122
<i>Figura 40 –</i> Download do arquivo "recolhaawsipbeja.vmdk".....	122
<i>Figura 41 –</i> Sequência para Conformidade e Eficiência na Aquisição de VM no Amazon AWS.....	123
<i>Figura 42 –</i> Google Drive.....	125
<i>Figura 43 –</i> Configurações, Segurança.....	126
<i>Figura 44 –</i> Selecionar tudo.....	126
<i>Figura 45 –</i> Atividades OneDrive.....	127
<i>Figura 46 –</i> Dispositivos Conectados.....	128

ÍNDICE DE TABELAS

<i>Tabela 1</i> – Funcionalidades oferecidas pelas ferramentas	60
<i>Tabela 2</i> – Tabela de Desafios	67
<i>Tabela 3</i> – Legenda Descritiva	95
<i>Tabela 4</i> – Funcionalidades oferecidas pelas ferramentas que serão testadas	96
<i>Tabela 5</i> – Sucesso na aquisição por ferramenta	106