

Transformando Incidentes em Inteligência

A Sinergia entre Gestão de Riscos e Resposta a Incidentes

Ingrid Barbosa

CAIS - RNP

SEXTA-FEIRA – 11:00



SEXTA-FEIRA – 12:00



DOMINGO – 03:00



Como evitamos que isso aconteça de novo?

Estamos documentando...

mas estamos aprendendo?

RESPONDER
DOCUMENTAR
ESQUECER
REPETIR



Transformar incidentes em **INTELIGÊNCIA**



Temos mais
tecnologia do
que nunca

Mas os mesmos problemas continuam acontecendo



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

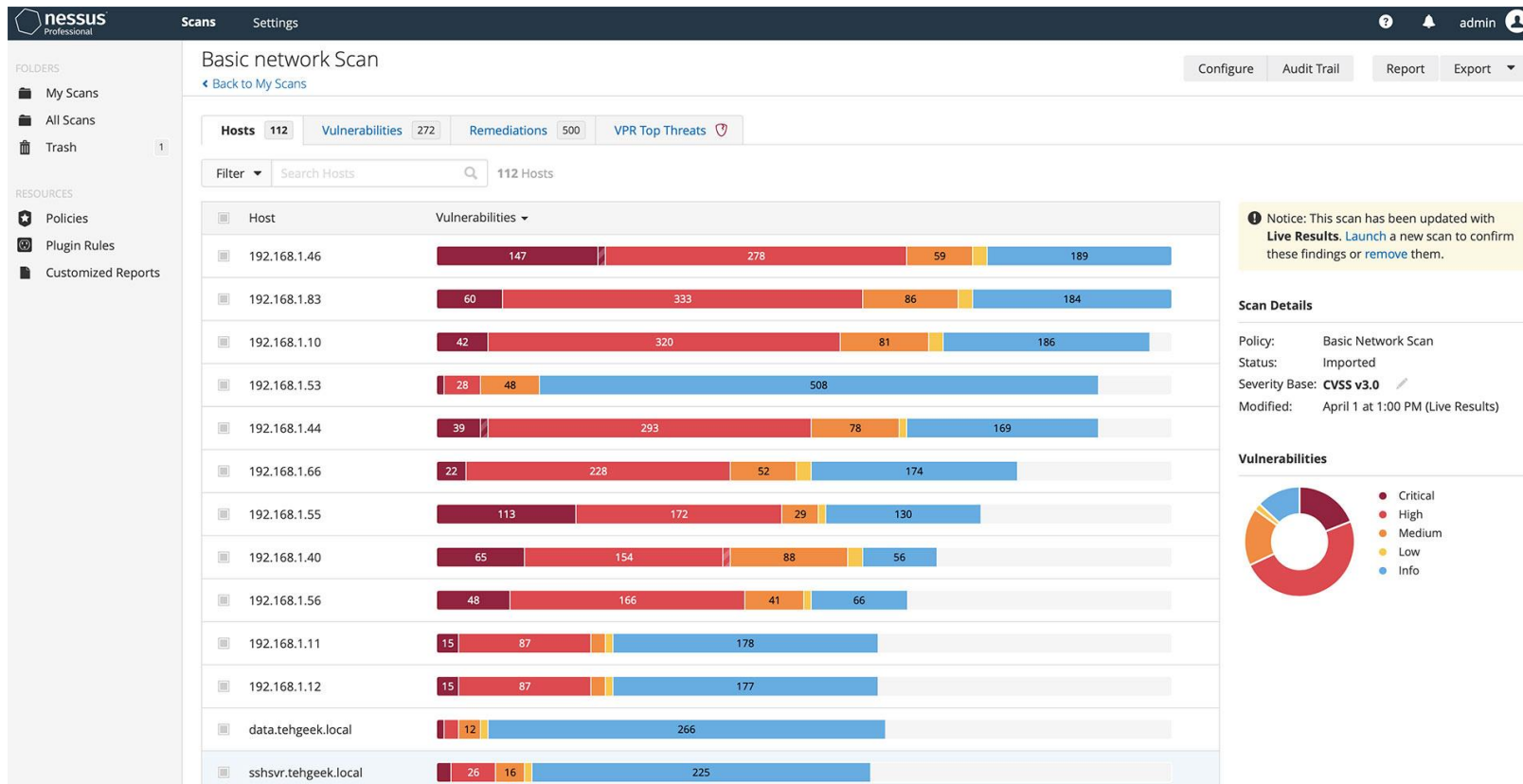


Estamos buscando as melhores soluções ...

...mas falhando no básico

RESPONDER
DOCUMENTAR
ESQUECER
REPETIR

Relatórios mostram falhas



FOLDERS

- 📁

My Scans
- 📁

All Scans
- 🗑️

Trash

1

RESOURCES

- 🌟

Policies
- 🔧

Plugin Rules
- 📄

Customized Reports

Basic network Scan

[← Back to My Scans](#)

Configure

Audit Trail

Report

Export

Hosts 112

Vulnerabilities 272

Remediations 500

VPR Top Threats 🛡️

Filter

Search Hosts



112 Hosts

Host	Vulnerabilities			
192.168.1.46	147	278	59	189
192.168.1.83	60	333	86	184
192.168.1.10	42	320	81	186
192.168.1.53	28	48	508	
192.168.1.44	39	293	78	169
192.168.1.66	22	228	52	174
192.168.1.55	113	172	29	130
192.168.1.40	65	154	88	56
192.168.1.56	48	166	41	66
192.168.1.11	15	87		178
192.168.1.12	15	87		177
data.tehgeek.local	12		266	
sshsrvr.tehgeek.local	26	16	225	

📢

Notice: This scan has been updated with **Live Results**. [Launch](#) a new scan to confirm these findings or [remove](#) them.

Scan Details

Policy:

Basic Network Scan

Status:

Imported

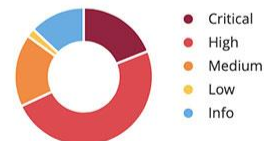
Severity Base:

CVSS v3.0

Modified:

April 1 at 1:00 PM (Live Results)

Vulnerabilities



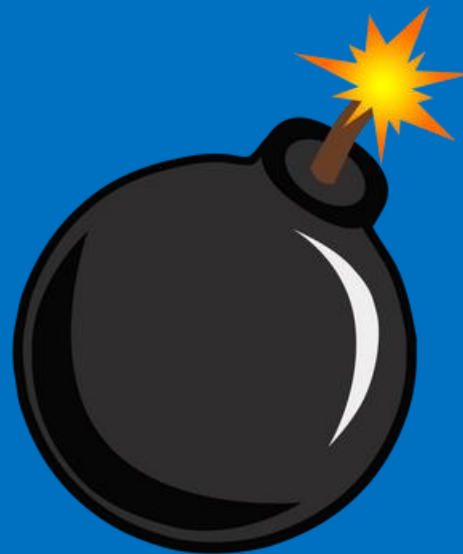


Não
podemos
nos proteger
contra tudo



O risco é o que pode acontecer





O incidente é o que já aconteceu

INCIDENTE é o RISCO que se materializou



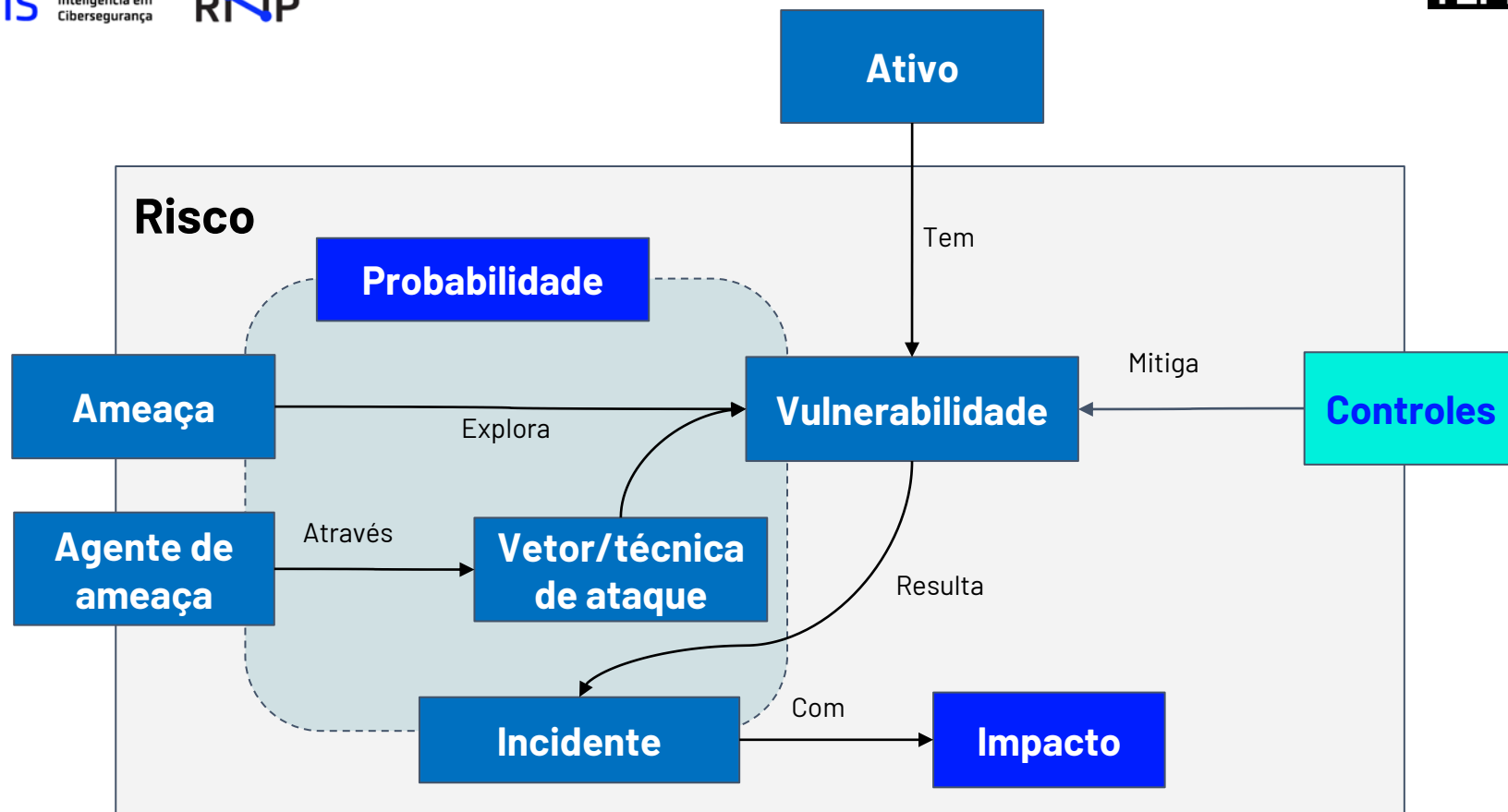
“Preservação da Confidencialidade, Integridade e Disponibilidade da Informação, a partir de um processo de gestão de riscos (...)”

ISO/IEC 27001:2022

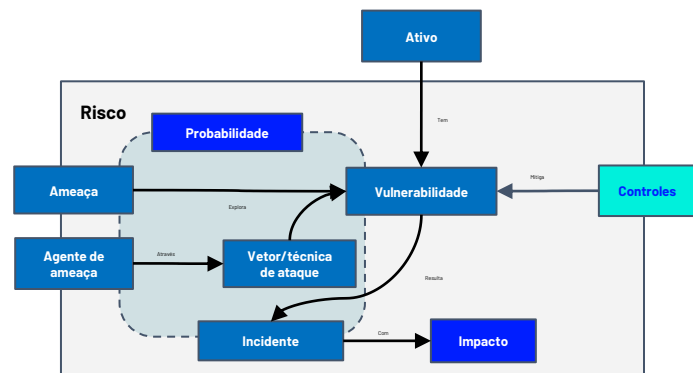


Avaliar riscos é uma habilidade inerente dos seres humanos

Mas nossas decisões são baseadas em nossas vivências



Efetividade dos controles







Com qual frequência sua organização toma decisões formais baseada em riscos?

1 – Falta de clareza em como levar os conceitos teóricos para a prática

2 – Tendência de priorizar o que parece urgente, em detrimento do que é realmente importante



O CAIS-RNP foi pioneiro ao começar discussões em segurança da informação, sendo um dos primeiros grupos de resposta a incidentes (Csirts) a atuar no Brasil.

Hoje, a área abrange diversas competências e é reconhecida nacional e internacionalmente pela experiência e amplo escopo de atuação.

Há 26 anos, o CAIS-RNP garante a segurança em centenas de instituições de educação e pesquisa brasileiras. A área de inteligência em cibersegurança da RNP desenvolve ações preventivas, educativas e corretivas em incidentes e ameaças na rede acadêmica, que enfrenta diariamente os desafios ligados ao aumento da complexidade de ameaças cibernéticas.

VELOCIDADES DAS CONEXÕES



Capacidade para expansão 4 Tb/s



300 Gb/s



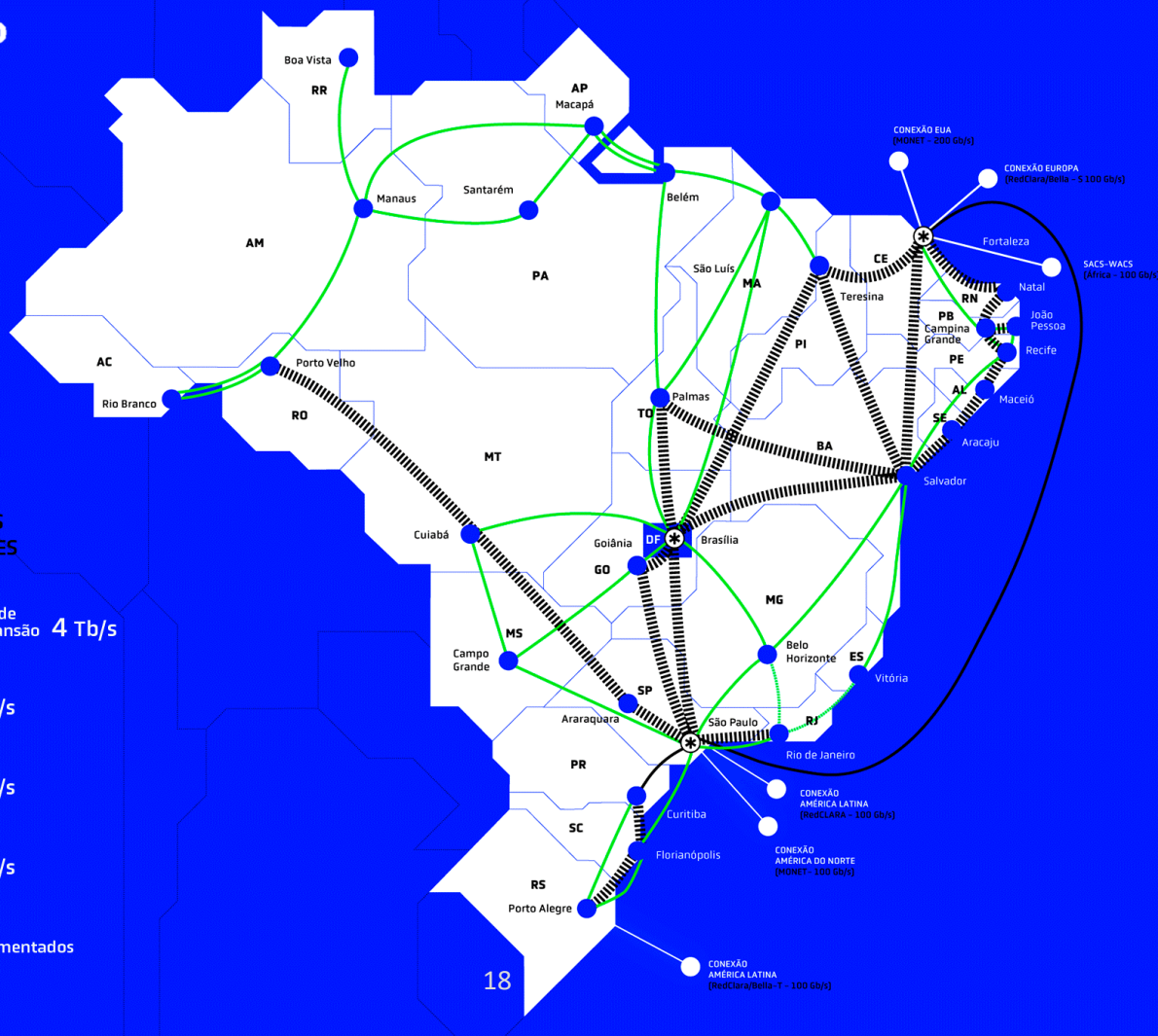
200 Gb/s



100 Gb/s

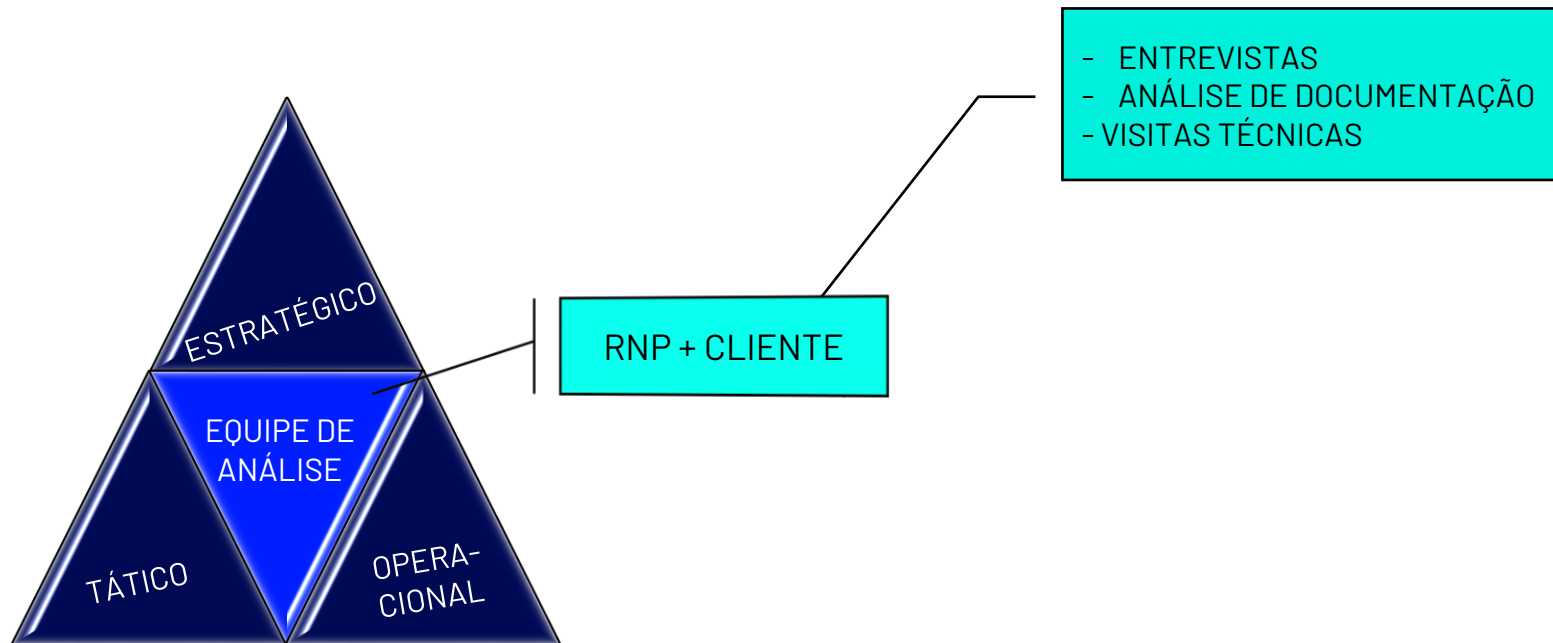


3 CNDs implementados



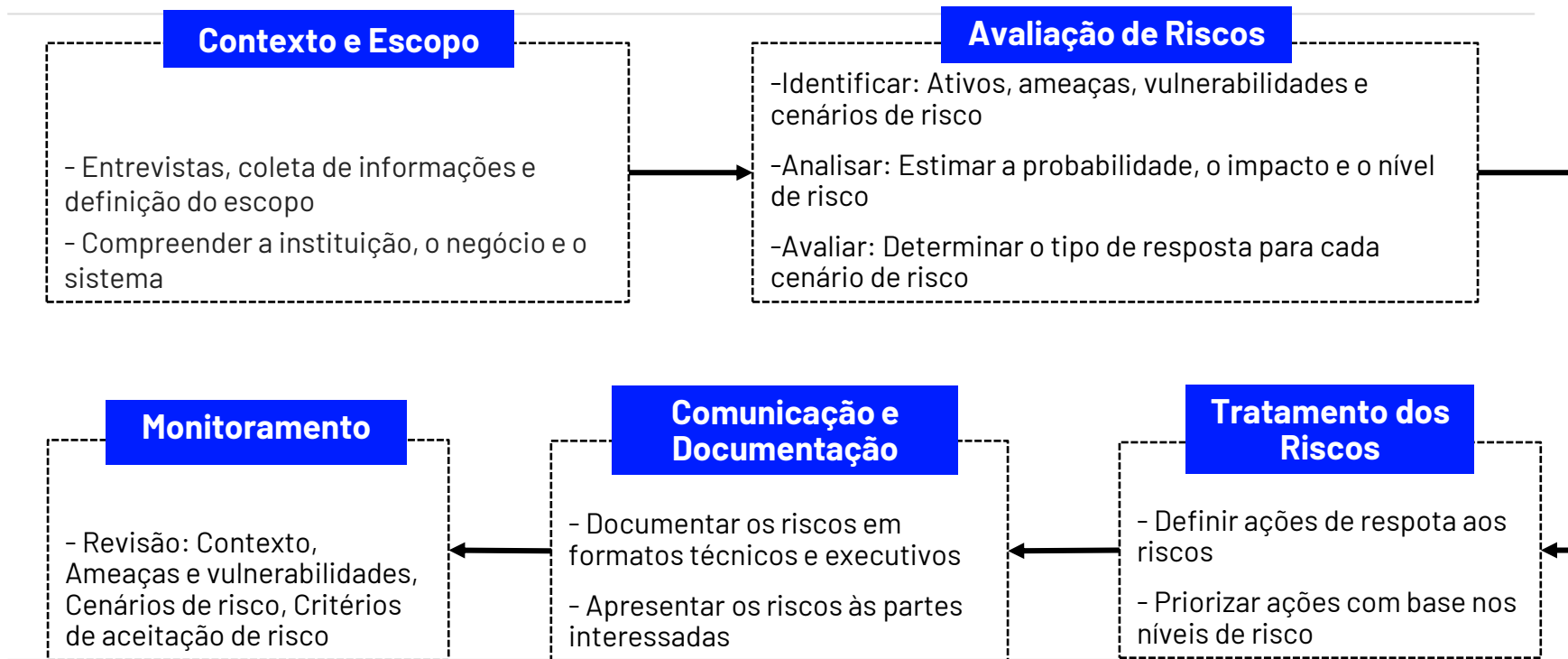


Abordagem tridimensional





Gerenciamento de Riscos Cibernéticos





Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Setor financeiro – envolve valores monetários diretamente – desenvolvedores de empresa terceira – nível júnior, menor cultura organizacional voltada para ética e integridade. Desenvolvedor com permissões de acesso e escrita em servidor crítico.



Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema



Avaliação de Riscos

- Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco
- Analisar: Estimar a probabilidade, o impacto e o nível de risco
- Avaliar: Determinar o tipo de resposta para cada cenário de risco

Ativo: Workforce (humano) – desenvolvedor júnior terceirizado



Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

- Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco
- Analisar: Estimar a probabilidade, o impacto e o nível de risco
- Avaliar: Determinar o tipo de resposta para cada cenário de risco



Spoofing - Falsificação

Privilégios desnecessários ou mal controlados

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

- Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco
- Analisar: Estimar a probabilidade, o impacto e o nível de risco
- Avaliar: Determinar o tipo de resposta para cada cenário de risco





Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

- Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco
- Analisar: Estimar a probabilidade, o impacto e o nível de risco
- Avaliar: Determinar o tipo de resposta para cada cenário de risco



Falha,
Destruição,
Perda, Mau
Funcionamento,
Roubo,
Interrupção e
outros...

Roubo de valores monetários
mascarado de atividade legítima



Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

- Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco
- Analisar: Estimar a probabilidade, o impacto e o nível de risco
- Avaliar: Determinar o tipo de resposta para cada cenário de risco

OWASP Risk Rating Calculator

Likelihood Factors

Threat Agent Factors

Skill Level

1 - No technical skills 1

2 - Low or no reward 2

3 - Some access or resources required 3

4 - Full access 4

5 - Full access 5

6 - Full access 6

7 - Full access 7

8 - Full access 8

9 - Full access 9

10 - Full access 10

11 - Full access 11

12 - Full access 12

13 - Full access 13

14 - Full access 14

15 - Full access 15

16 - Full access 16

17 - Full access 17

18 - Full access 18

19 - Full access 19

20 - Full access 20

21 - Full access 21

22 - Full access 22

23 - Full access 23

24 - Full access 24

25 - Full access 25

26 - Full access 26

27 - Full access 27

28 - Full access 28

29 - Full access 29

30 - Full access 30

31 - Full access 31

32 - Full access 32

33 - Full access 33

34 - Full access 34

35 - Full access 35

36 - Full access 36

37 - Full access 37

38 - Full access 38

39 - Full access 39

40 - Full access 40

41 - Full access 41

42 - Full access 42

43 - Full access 43

44 - Full access 44

45 - Full access 45

46 - Full access 46

47 - Full access 47

48 - Full access 48

49 - Full access 49

50 - Full access 50

51 - Full access 51

52 - Full access 52

53 - Full access 53

54 - Full access 54

55 - Full access 55

56 - Full access 56

57 - Full access 57

58 - Full access 58

59 - Full access 59

60 - Full access 60

61 - Full access 61

62 - Full access 62

63 - Full access 63

64 - Full access 64

65 - Full access 65

66 - Full access 66

67 - Full access 67

68 - Full access 68

69 - Full access 69

70 - Full access 70

71 - Full access 71

72 - Full access 72

73 - Full access 73

74 - Full access 74

75 - Full access 75

76 - Full access 76

77 - Full access 77

78 - Full access 78

79 - Full access 79

80 - Full access 80

81 - Full access 81

82 - Full access 82

83 - Full access 83

84 - Full access 84

85 - Full access 85

86 - Full access 86

87 - Full access 87

88 - Full access 88

89 - Full access 89

90 - Full access 90

91 - Full access 91

92 - Full access 92

93 - Full access 93

94 - Full access 94

95 - Full access 95

96 - Full access 96

97 - Full access 97

98 - Full access 98

99 - Full access 99

100 - Full access 100

101 - Full access 101

102 - Full access 102

103 - Full access 103

104 - Full access 104

105 - Full access 105

106 - Full access 106

107 - Full access 107

108 - Full access 108

109 - Full access 109

110 - Full access 110

111 - Full access 111

112 - Full access 112

113 - Full access 113

114 - Full access 114

115 - Full access 115

116 - Full access 116

117 - Full access 117

118 - Full access 118

119 - Full access 119

120 - Full access 120

121 - Full access 121

122 - Full access 122

123 - Full access 123

124 - Full access 124

125 - Full access 125

126 - Full access 126

127 - Full access 127

128 - Full access 128

129 - Full access 129

130 - Full access 130

131 - Full access 131

132 - Full access 132

133 - Full access 133

134 - Full access 134

135 - Full access 135

136 - Full access 136

137 - Full access 137

138 - Full access 138

139 - Full access 139

140 - Full access 140

141 - Full access 141

142 - Full access 142

143 - Full access 143

144 - Full access 144

145 - Full access 145

146 - Full access 146

147 - Full access 147

148 - Full access 148

149 - Full access 149

150 - Full access 150

151 - Full access 151

152 - Full access 152

153 - Full access 153

154 - Full access 154

155 - Full access 155

156 - Full access 156

157 - Full access 157

158 - Full access 158

159 - Full access 159

160 - Full access 160

161 - Full access 161

162 - Full access 162

163 - Full access 163

164 - Full access 164

165 - Full access 165

166 - Full access 166

167 - Full access 167

168 - Full access 168

169 - Full access 169

170 - Full access 170

171 - Full access 171

172 - Full access 172

173 - Full access 173

174 - Full access 174

175 - Full access 175

176 - Full access 176

177 - Full access 177

178 - Full access 178

179 - Full access 179

180 - Full access 180

181 - Full access 181

182 - Full access 182

183 - Full access 183

184 - Full access 184

185 - Full access 185

186 - Full access 186

187 - Full access 187

188 - Full access 188

189 - Full access 189

190 - Full access 190

191 - Full access 191

192 - Full access 192

193 - Full access 193

194 - Full access 194

195 - Full access 195

196 - Full access 196

197 - Full access 197

198 - Full access 198

199 - Full access 199

200 - Full access 200

201 - Full access 201

202 - Full access 202

203 - Full access 203

204 - Full access 204

205 - Full access 205

206 - Full access 206

207 - Full access 207

208 - Full access 208

209 - Full access 209

210 - Full access 210

211 - Full access 211

212 - Full access 212

213 - Full access 213

214 - Full access 214

215 - Full access 215

216 - Full access 216

217 - Full access 217

218 - Full access 218

219 - Full access 219

220 - Full access 220

221 - Full access 221

222 - Full access 222

223 - Full access 223

224 - Full access 224

225 - Full access 225

226 - Full access 226

227 - Full access 227

228 - Full access 228

229 - Full access 229

230 - Full access 230

231 - Full access 231

232 - Full access 232

233 - Full access 233

234 - Full access 234

235 - Full access 235

236 - Full access 236

237 - Full access 237

238 - Full access 238

239 - Full access 239

240 - Full access 240

241 - Full access 241

242 - Full access 242

243 - Full access 243

244 - Full access 244

245 - Full access 245

246 - Full access 246

OWASP Risk Rating Calculator

Likelihood Factors

Threat Agent Factors

Skill Level

9 - No technical skills

Motive

1 - Low or no reward

Opportunity

7 - Some access or resources required

Size

5 - Partners

Threat Agent Factor:
Medium (TAF: 5.5)

Likelihood Factor: Medium (LF: 5.75)

Vulnerability Factors

Ease of Discovery

3 - Difficult

Ease of Exploit

3 - Difficult

Awareness

9 - Public knowledge

Intrusion Detection

9 - Not logged

Vulnerability Factor: High
(VF: 6)

L = Média

Impact Factors

Technical Impact Factors

Loss of Confidentiality

6 - Minimal critical data or extensive non

Loss of Integrity

3 - Minimal seriously corrupt data

Loss of Availability

0 - N/A

Loss of Accountability

9 - Completely anonymous

Technical Impact Factor:
Medium (TIF: 4.5)

Impact Factor: Low (IF: 1.5)

Business Impact Factors

Financial Loss

3 - Minor effect on annual

Reputation Damage

1 - Minimal damage

Non-compliance

2 - Minor violation

Privacy Violation

0 - N/A

Business Impact Factor:
Low (BIF: 1.5)

L = Muito Alto

Overall Risk Severity: Low

L = Alto



Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

- Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco
- Analisar: Estimar a probabilidade, o impacto e o nível de risco
- Avaliar: Determinar o tipo de resposta para cada cenário de risco

OWASP Risk Rating Calculator

Likelihood Factors

Threat Agent Factors

Skill Level	4 - No technical skills	2
Motive	3 - Difficult	5
Opportunity	4 - Low or no reward	5
Size	4 - Some access or resources required	2
	5 - Fastness	2

Threat Agent Factor:

Medium (TAF: 5.5)

Vulnerability Factors

Ease of Discovery	3 - Difficult	5
Ease of Exploit	3 - Difficult	5
Awareness	9 - Robust knowledge	5
Intrusion Detection	9 - Not logged	5

Vulnerability Factor: High

(VF: 6)

Impact Factors

Technical Impact Factors

Loss of Confidentiality	5 - Minimal critical data or extensive exploit	1
Loss of Integrity	1 - Minimal personally corrupt data	5
Loss of Availability	4 - Not	5
Loss of Accountability	9 - Completely anonymous	5

Technical Impact Factor:

Medium (TIF: 4.5)

Business Impact Factors

Financial Damage	3 - Minor effect on annual profit	5
Reputation Damage	1 - Minimal damage	5
Non-compliance	2 - Minor violation	5
Privacy Violation	0 - N/A	5

Business Impact Factor:

Low (BIF: 1.5)

Likelihood Factor: Medium (LF: 5.75)

Impact Factor: Low (IF: 1.5)

Overall Risk Severity: Low

Falha,
Destruição,
Perda, Mau
Funcionamento,
Roubo,
Interrupção e
outros...

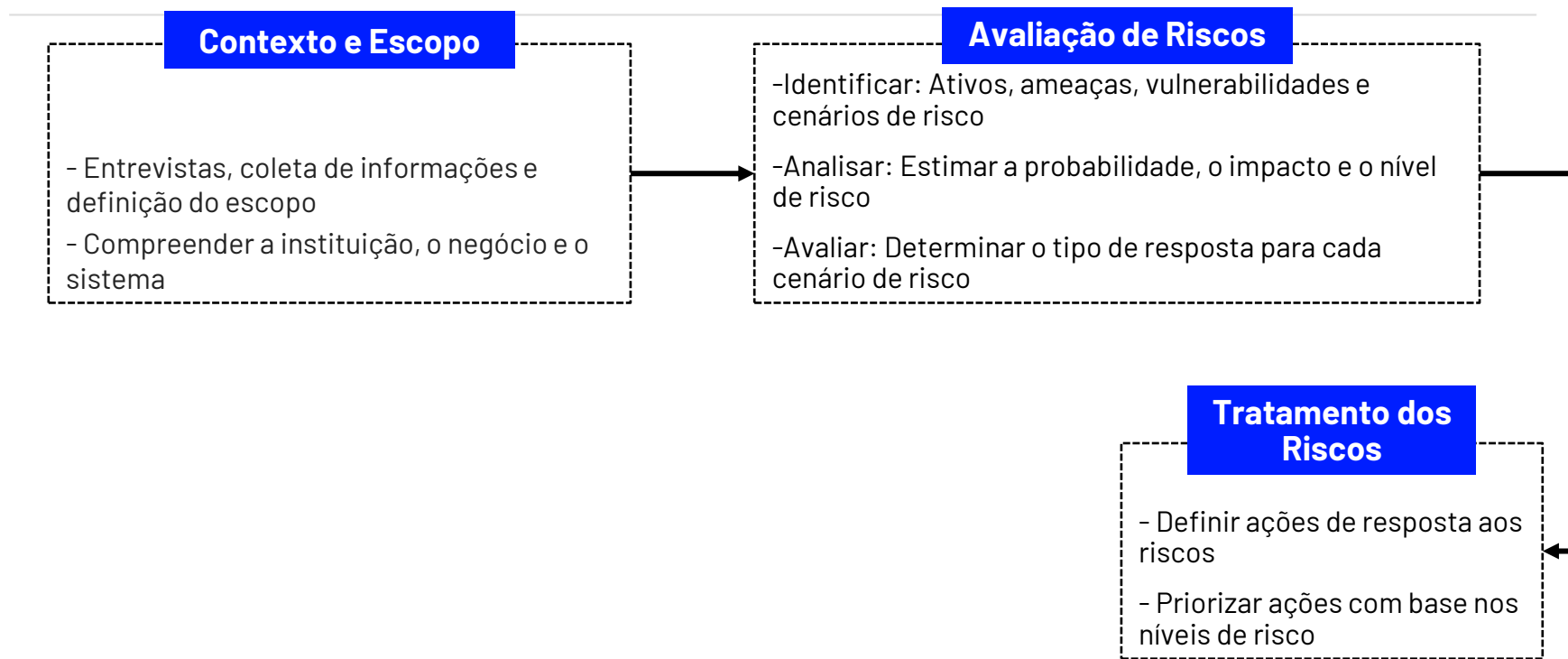
1. Evitar
2. Mitigar
3. Transferir
4. Aceitar

MITIGAR



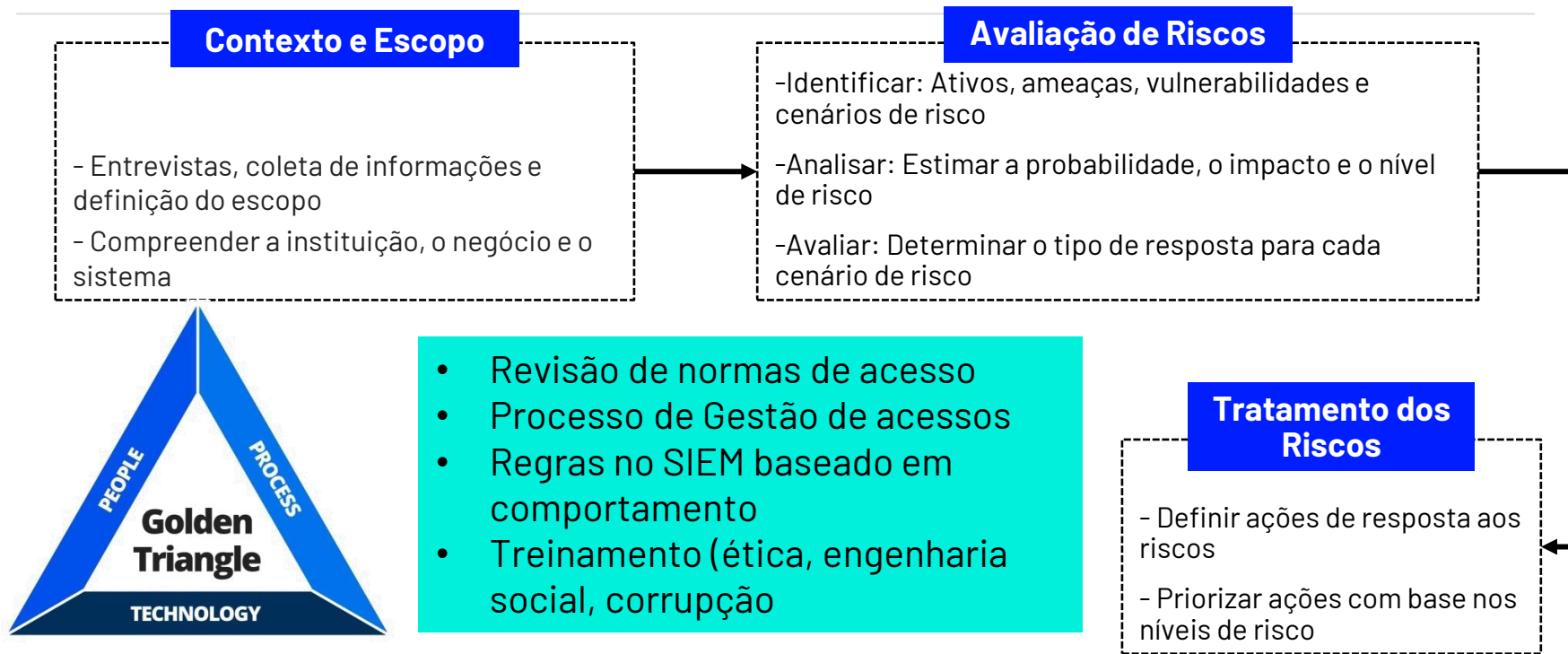


Gerenciamento de Riscos Cibernéticos



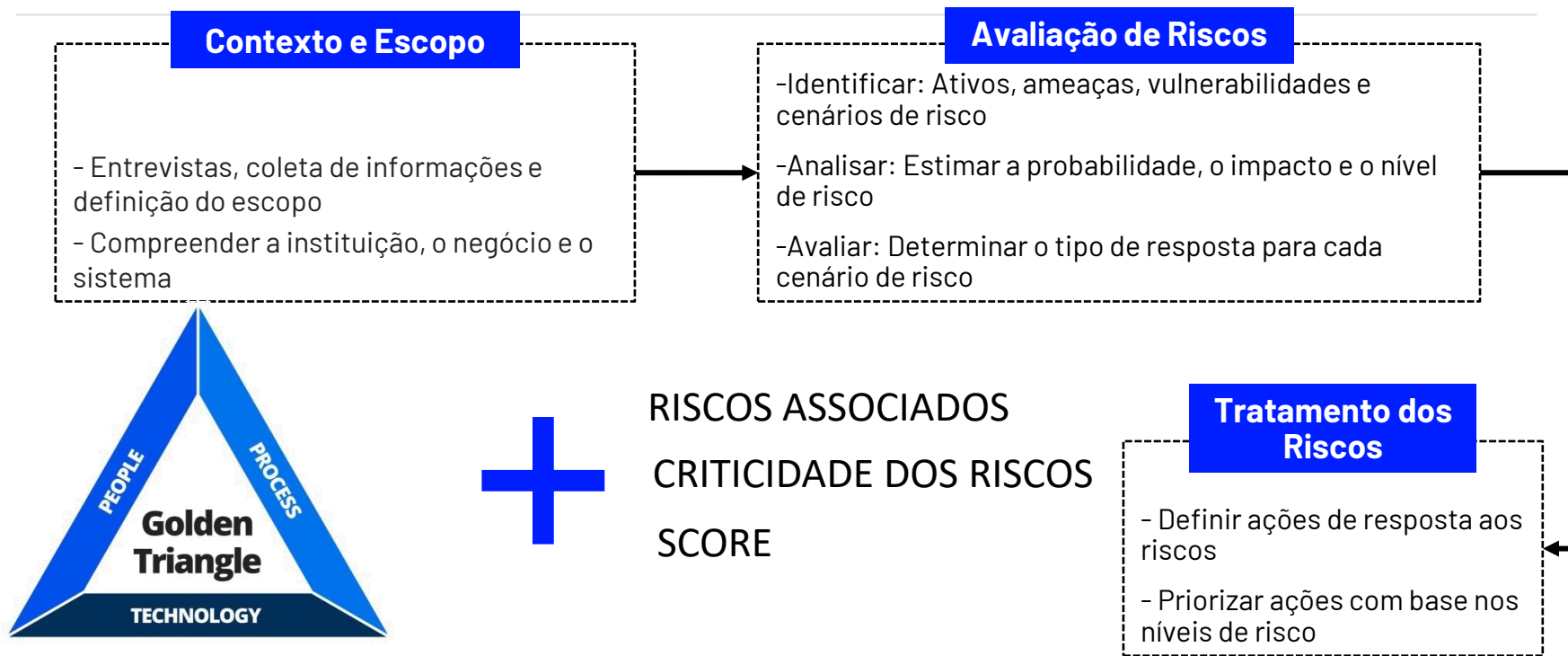


Gerenciamento de Riscos Cibernéticos



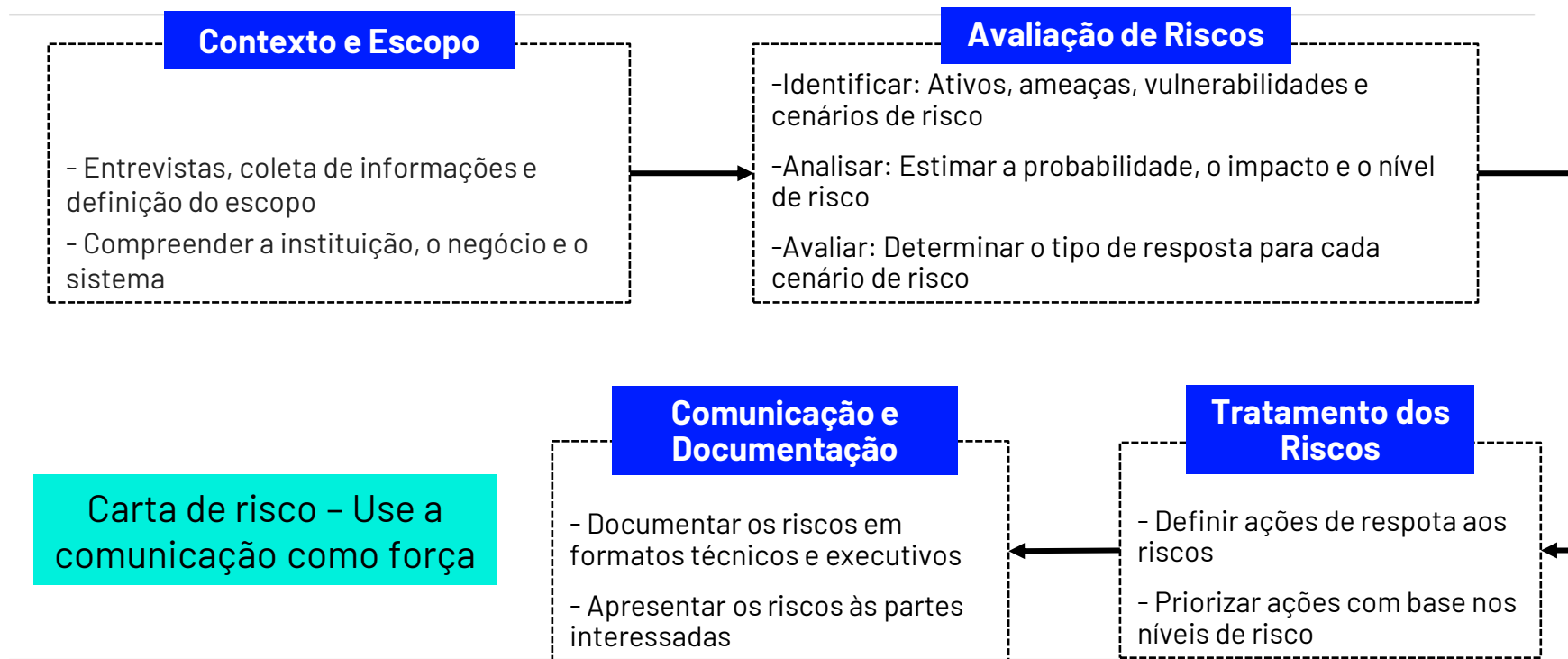


Gerenciamento de Riscos Cibernéticos



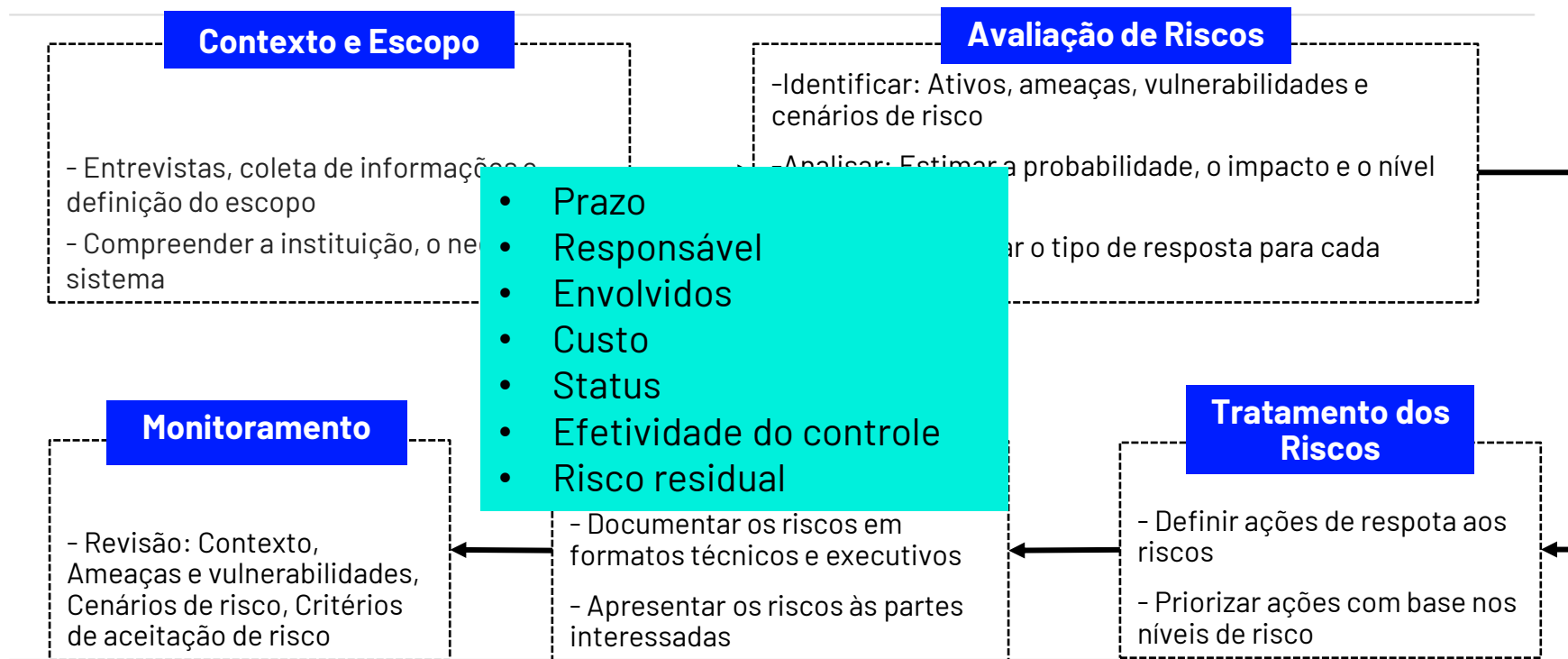


Gerenciamento de Riscos Cibernéticos



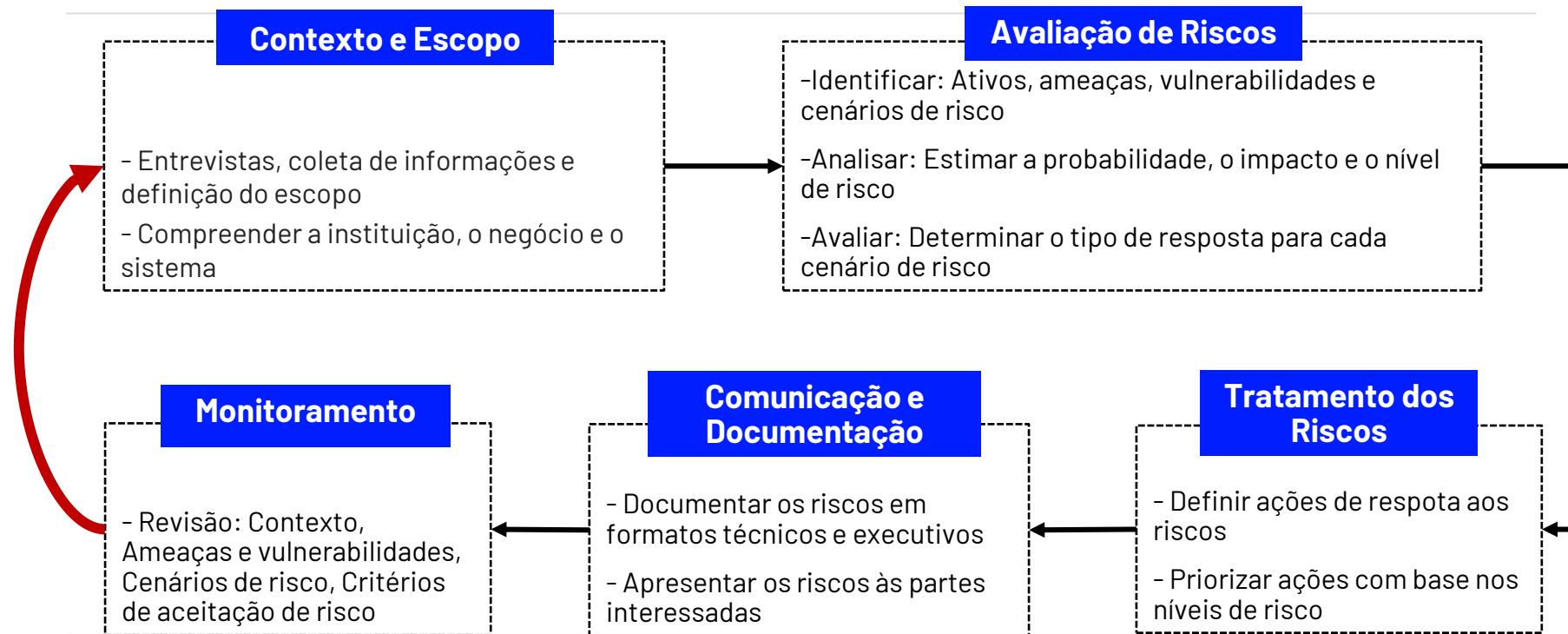


Gerenciamento de Riscos Cibernéticos





Gerenciamento de Riscos Cibernéticos





Lições aprendidas

- A gestão de riscos é viva. Sempre pergunte: “O que mudou? O que aprendemos com o último incidente?”
- Comece pequeno, escale com inteligência. Inicie com escopos menores e expanda conforme a maturidade aumenta.
- Comunique-se diretamente, sem intermediários. Clareza gera engajamento.
- Espere (e supere) resistência. Desconforto é sinal de que o status quo está sendo desafiado.
- Na dúvida, assuma o pior. Em avaliações, sempre erre pelo lado da cautela.
- Comemore as conquistas. Mesmo pequenas mitigações de risco merecem reconhecimento.
- Colaboração é inegociável. A cibersegurança é responsabilidade de todos.
- A cultura devora a estratégia. Com prática, o pensamento orientado a riscos e integrado às equipes de resposta a incidentes começa a se tornar algo natural.



Incidentes mostram onde o risco é
mais do que uma hipótese. Separados,
riscos e incidentes só reagem.
Juntos, antecipam.



Ingrid Barbosa

Information Security | Cyber risks | IoT and
Smart Cities | Blockchain |



OBRIGADA!

ingrid.barbosa@rnp.br