KPMG

Security Analytics

IFA 2017 - L.I.V.E. The Global Experience: Leadership.Innovation.Value. Effectiveness

Luís Lobo

21 de Junho de 2017

KPMG.pt

1 Agenda

1) Agenda

2) Global Profiles of the Fraudester

Principais Resultados

3) Security Analytics

Evolução do Security Analytics

Principais Desafios do Security Analytics

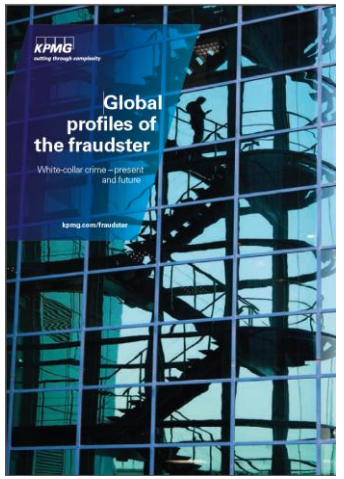
Principais Riscos do Security Analytics

Factores Críticos de Sucesso no Security Analytics

2

Global Profiles of the Fraudster

2010
348 casos em 69 países



2013
596 casos em 78 países

2015
750 casos em 81 países

Principais Resultados

Origem

42%

Fraude Interna

32% Fraude mista
25% Fraude externa

Idade

37%

36 a 45 Anos de Idade

31% 46 a 55 anos de idade
15% menos de 35 anos de idade
8% mais de 56 anos de idade

Anos de Serviço

51%

Mais de 6 Anos de Serviço

25% 1 a 4 anos de serviço
19% 4 a 6 anos de serviço
3% menos de 1 ano e serviço

Cargo

34%

Executivos/Directores

32% Gerentes
23% Outros colaboradores
2% Sócios/Accionistas

Facilitadores

62%

Controlos Internos Fracos

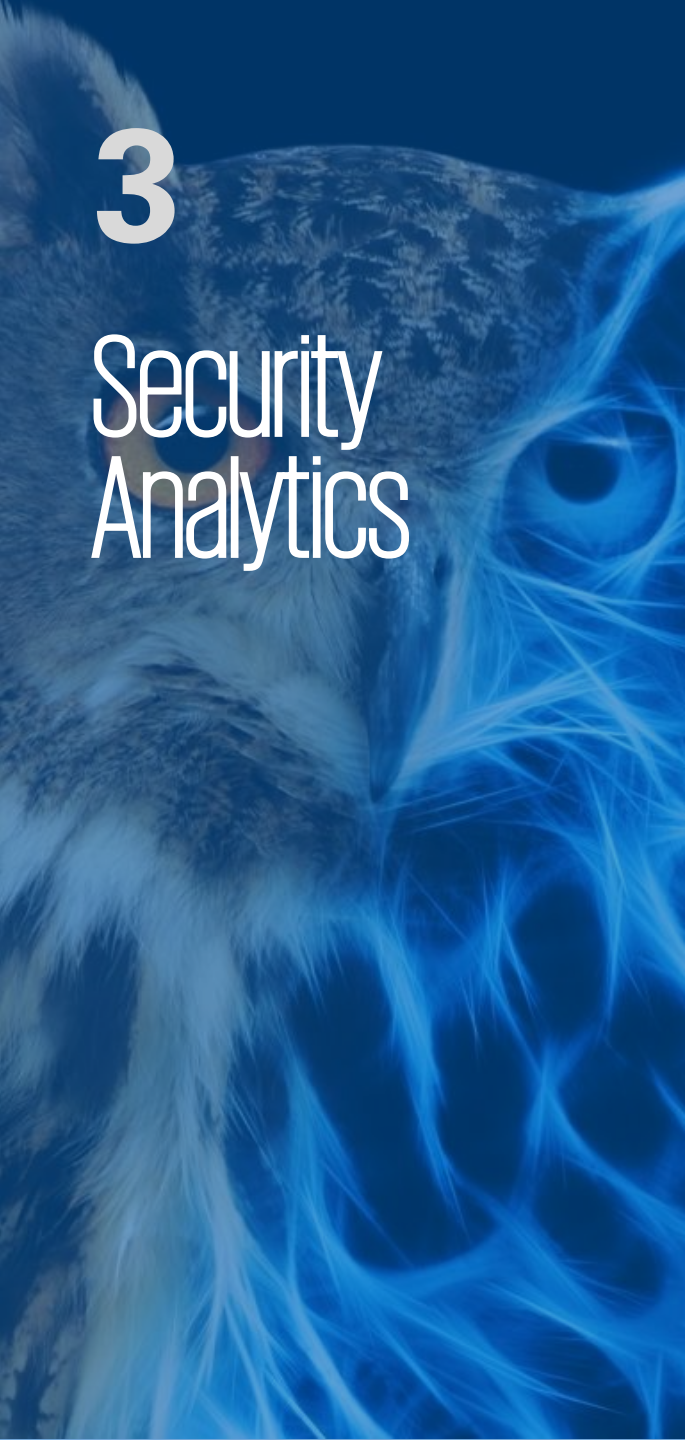
22% Desonestidade imprudente
11% Conluio
5% Outros

Detecção

3%

Data Analytics Proactiva

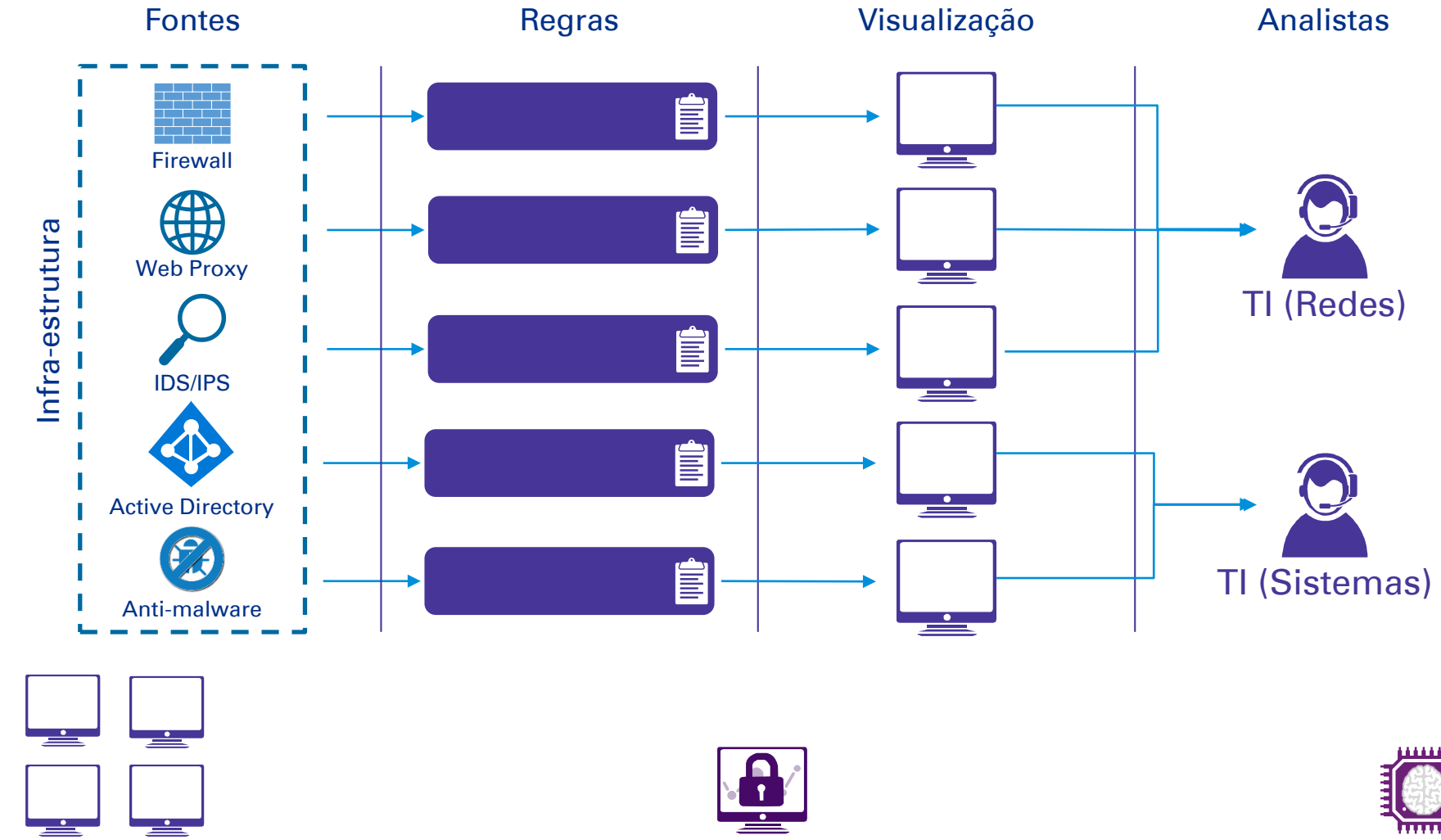
54% Queixas, desconfiança
42% Função de auditoria
17% acidental, admitida



3 Security Analytics

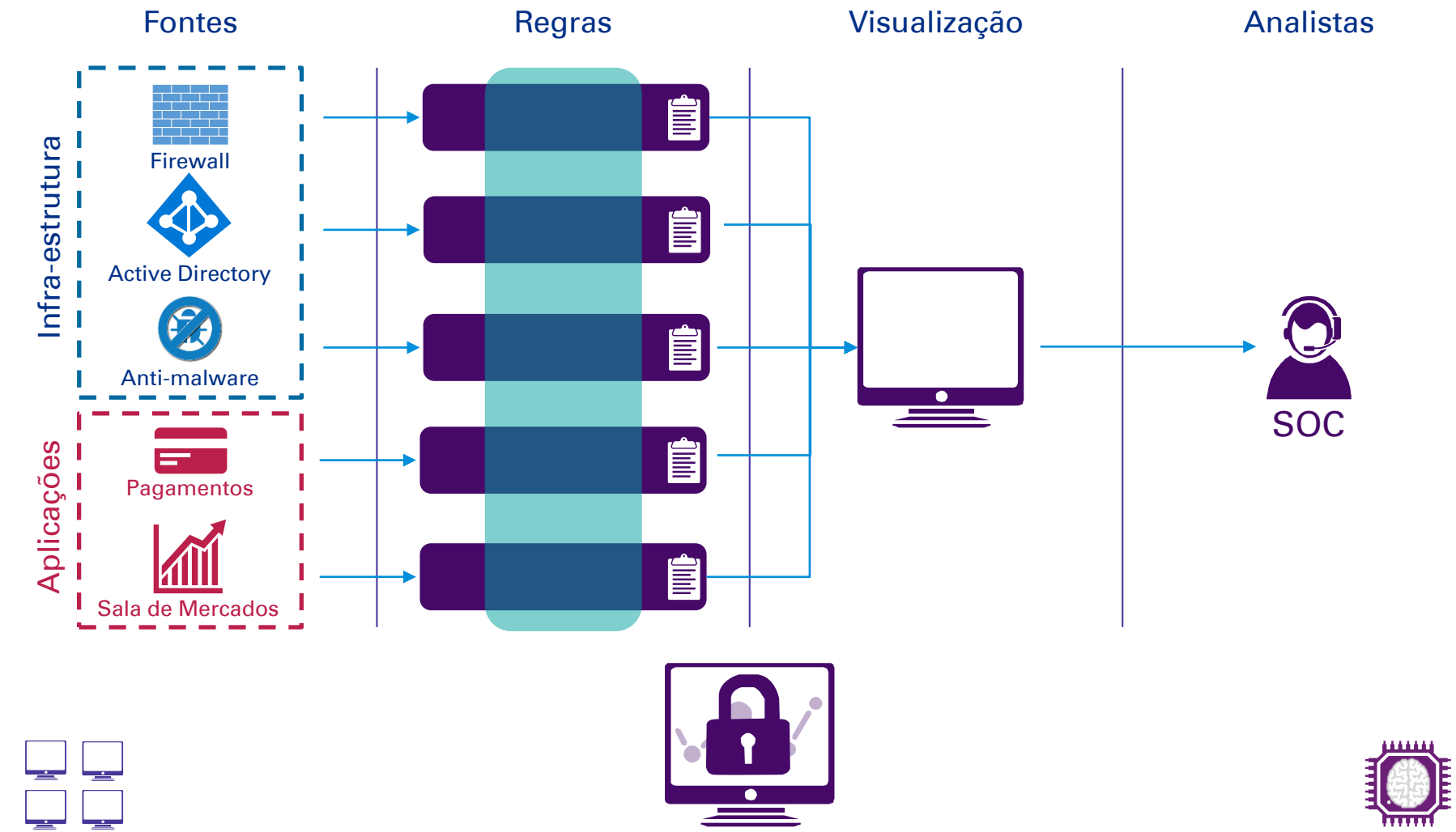
Capacidade de descobrir, interpretar e apresentar padrões num conjunto de eventos nos sistemas de informação de modo a detectar e compreender potenciais incidentes de segurança ou comportamento anómalos na organização.

Evolução - Ponto de Partida



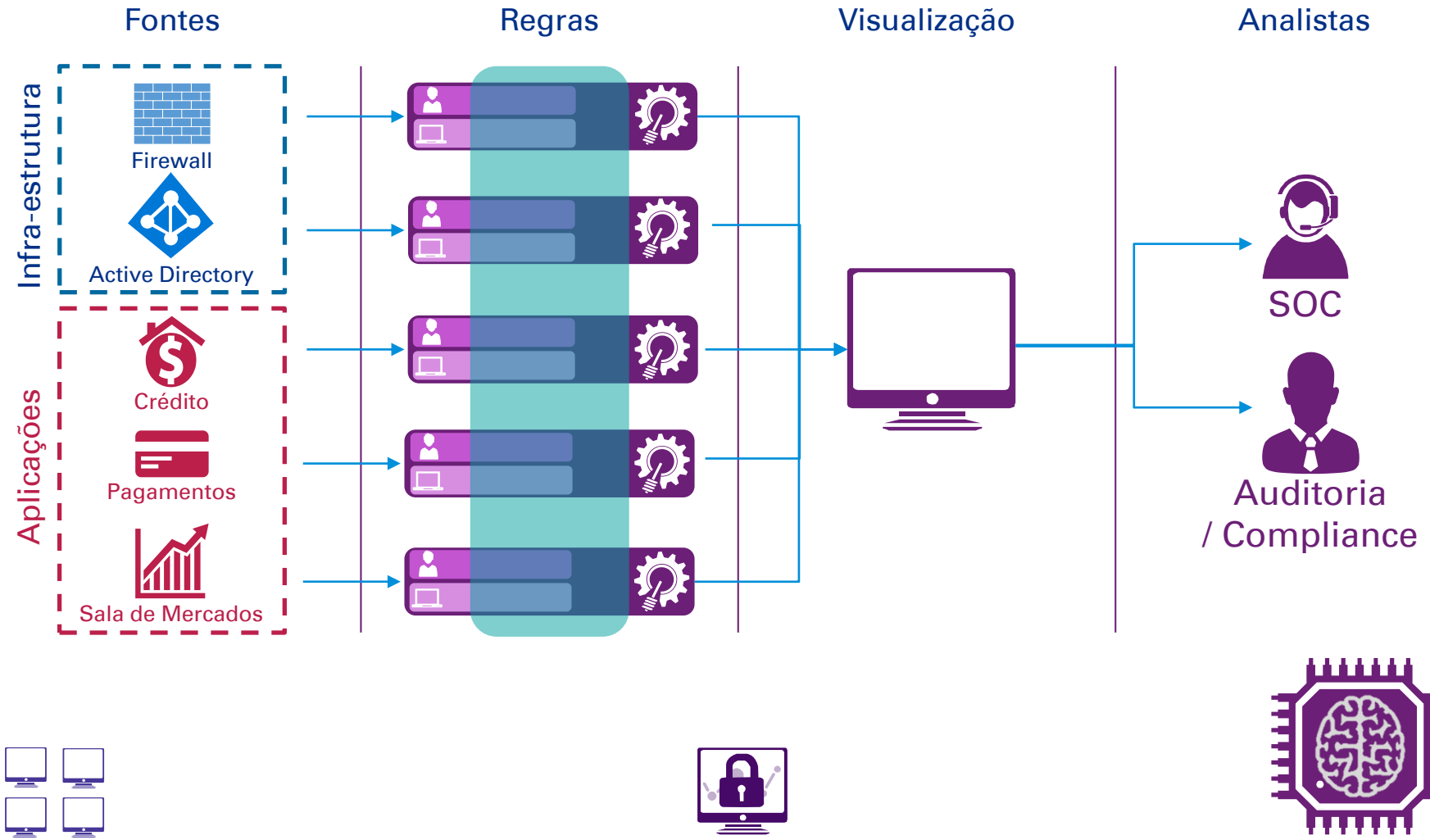
Security Analytics

Evolução - Detecção do Conhecido



Security Analytics

Evolução - Detecção do Desconhecido



Principais Desafios

Na implementação de processos e mecanismos de Security Analytics tipicamente enfrentam diversos desafios que tornam esta disciplina exigente e complexa:

ACESSO À INFORMAÇÃO

Os sistemas e aplicações, muitas vezes não são capazes de gerar ou transmitir os eventos necessários para uma monitorização eficaz.

INFORMAÇÃO RELEVANTE

Os sistemas e aplicações geram grandes quantidades de eventos, mas nem todos são relevantes para os objectivos da Organização.

FALSOS POSITIVOS

As regras de alarmística, se não forem afinadas devidamente, podem gerar uma quantidade significativa de falsos positivos.

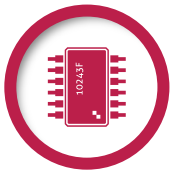
SOFISTICAÇÃO

Os ciberataques e fraudes são cada vez mais sofisticados demonstrando profundo do negócio e dos sistemas, dificultando a sua detecção.

Principais Riscos

De acordo com a experiência da KPMG, muitas destas iniciativas de Security Analytics, não atingem os objectivos propostos. As principais causas incluem:

ENFOQUE TECNOLÓGICO



O excessivo enfoque nos aspectos tecnológicos/ infra-estrutura, negligenciando os processos e activos do negócio.

EXPECTATIVAS EXAGERADAS

As expectativas exageradas pretendendo obter um aumento significativo na maturidade de security analytics num curto espaço de tempo.

PROJECTOS ONE-OFF

A implementação de iniciativas de security analytics em projectos one-off, sem garantir estruturas de gestão que acompanhem a evolução da Organização.

CONFORMIDADE

O foco exclusivo no cumprimento de uma obrigação regulamentar.

Factores Críticos de Sucesso

O sucesso de uma iniciativa de Security Analytics depende, entre outros aspectos, da capacidade da Organização em garantir:

PATROCÍNIO

O patrocínio dos Órgãos de Gestão e o envolvimento activo dos responsáveis do negócio e TI.

PRIORIZAÇÃO

A priorização focada no que é realmente importante para a organização, efectuando exercícios de *Threat Modeling* para identificar o que se deve proteger.

ACTUALIZAÇÃO CONTÍNUA

O alinhamento continuo com o negócio, a arquitectura de sistemas de informação da Organização e as tendências de ciberataques/fraude.

NORMALIDADE

A identificação do que é expectável no decorrer do dia-a-dia da organização.

Contacte-nos

Rui Gomes
Partner – IT Advisory
rgomes@kpmg.com

Tiago Reis
Senior Manager – Cybersecurity, IT Advisory
treis@kpmg.com

Luís Lobo
Manager – Cybersecurity, IT Advisory
luislobo@kpmg.com

kpmg.pt