

Formação com Impacto
Liderar a Cibersegurança, transformar a Organização

Formação Intermédia em Cibersegurança

Bruno Horta Soares
Data: 15/10/2026



Quem sou

Bruno Horta Soares

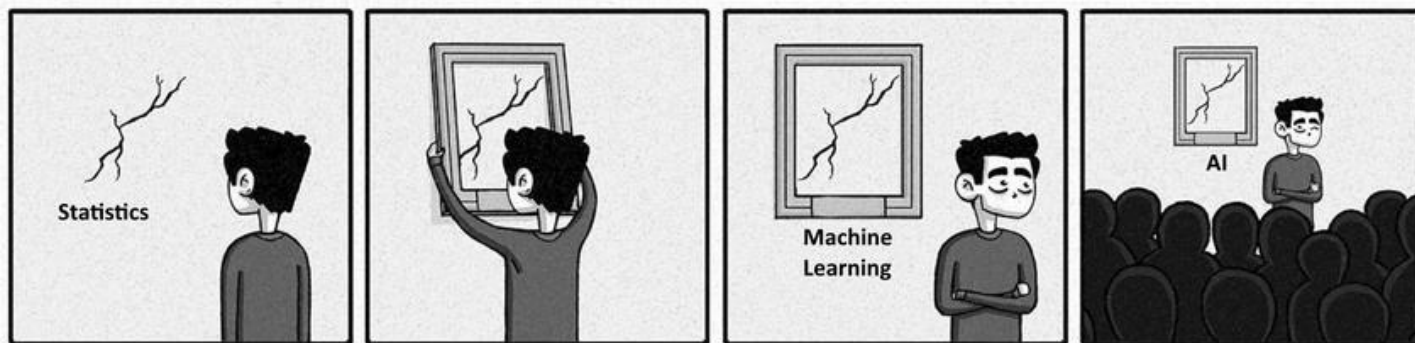
CISA®, *CGEIT®*, *CRISC™*, *PMP®*, *LEGO® Serious Play®*

Assistant Professor

bruno.soares@govaas.com

[/in/brunohsoares/](#)

Executive advisor nas áreas de governança, transformação digital, risco, cibersegurança e inteligência artificial. Fundador da GOVaaS (Governance Advisors as-a-Service), trabalha com conselhos de administração e equipas executivas no alinhamento entre governança e tecnologia, em Portugal e em mercados internacionais. Fundador e past-president do ISACA Lisbon Chapter. Docente em programas executivos e de pós-graduação em Portugal, Angola e Brasil.



A mensagem desta tarde

A segurança da informação só cria valor quando é governada como um sistema integrado. Nenhuma framework, sozinha, chega para isso.

1

Sem objetivo de negócio, não há argumento

A cascata de objetivos do COBIT liga cada prática de segurança a um objetivo da empresa. É isso que aguenta o "porquê?" da administração.

2

As frameworks sobrepõem-se mais do que competem

COBIT, ISO 27001, NIST CSF e CIS Controls respondem a perguntas diferentes sobre a mesma realidade. O trabalho é articulá-las, não escolher uma.

3

A integração é operacionalizável

Do DSS05 descemos aos controlos CIS e às subcategorias NIST, e subimos com métricas até à administração.

Sete blocos, cada um responde a uma pergunta

0	Linguagem comum	De que falamos quando falamos de segurança?	Porquês, complexidade, I&T, âmbito e confiança
A	O caso AQUÁRIA	Esta empresa tem ou não um desafio de cibersegurança?	Caso + pitch em grupo, com IA generativa
B	Da estratégia ao controlo	Porque é que a segurança importa a esta empresa em particular?	Cascata de objetivos COBIT 2019 e AG07
C	Dentro do DSS05	Como se gere, mede e organiza a segurança operacional?	Ficha do objetivo, dashboard e 7 componentes
D	Do risco ao incidente	Como acontece um ataque, e o que fazer antes e depois?	Kill Chain, ATT&CK, NIST CSF, risco vs. incidente, NIS2
E	Integrar frameworks	Como falam entre si COBIT, ISO 27001, NIST CSF e CIS?	Related Guidance, matriz e rastreabilidade
F	Voltar à CEO	O que dizemos agora, que aguento o "porquê?"	Pitch 2.0 e síntese

O compromisso com a Axians: cada tema do programa tem um lugar nesta tarde

Objetivo do módulo: desenvolver competências para prevenir riscos, responder a incidentes e promover uma cultura de cibersegurança na organização.

Prevenir riscos
B • C • E

Responder a incidentes
D

Promover cultura
D • F

Tema do programa	Conteúdos previstos	Onde	Como o trabalhamos
Engenharia social	Tipologias (phishing, pretexting, baiting...); técnicas dos atacantes	Bloco D	Engenharia social como fase de entrega no Kill Chain e técnicas ATT&CK; simulação (15:40)
Gestão de incidentes e comunicação de crise	Ciclo de gestão de incidentes; comunicação interna e externa em situações de risco	Blocos B e D	Risco vs. incidente; NIS2 antes e depois do ataque; incidente como esforço de toda a organização; mensagens na simulação
Cultura de cibersegurança	Papel dos colaboradores; boas práticas; sensibilização e capacitação contínua	Blocos C e D	Componente Cultura do DSS05; quem reporta cedo trava o ataque; áreas que têm de trabalhar juntas
Contextos críticos e serviços essenciais	Riscos em infraestruturas críticas; continuidade e resiliência; políticas e medidas	Todos	Caso AQUÁRIA (entidade essencial, OT); DSS04 e EG06; ATT&CK for ICS; NIS2 arts. 20, 21 e 23

Fonte: Proposta de Formação NOVA FCT Executive Education para a Axians, módulo 4 (Formação Intermédia em Cibersegurança).



Bloco 0

Linguagem comum

De que falamos quando falamos de segurança?

A era dos porquês: o perigo está na pergunta, não na resposta

“ Os erros mais graves não resultam de respostas erradas.
O verdadeiramente perigoso é fazer a pergunta errada.

Peter Drucker

Conformidade

“A quem deve reportar a cibersegurança?”

RGPD
AI Act
NIS2
...

Risco

“Que risco aceitamos correr, e para alcançar o quê?”

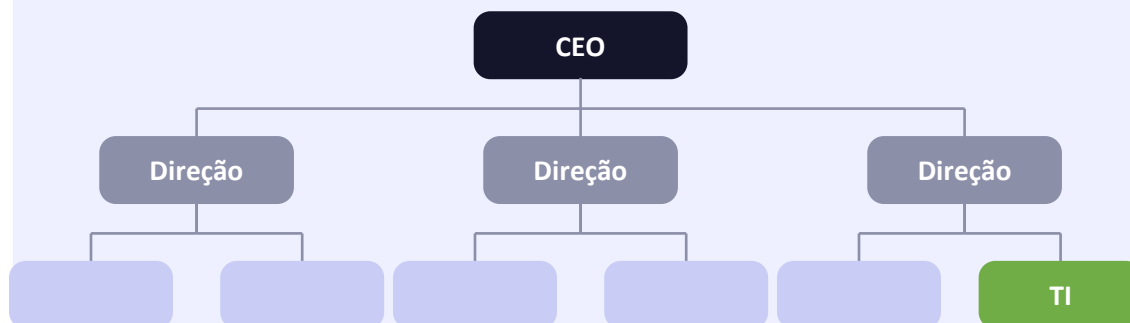
A regulação empurra a conversa para a conformidade. A pergunta que cria valor está do lado do risco.

TI é um departamento. I&T é uma responsabilidade

Na quinta do meu avô não se davam nomes aos animais, para não haver apego. Prova rural de uma verdade simples: **os nomes importam.**

TI

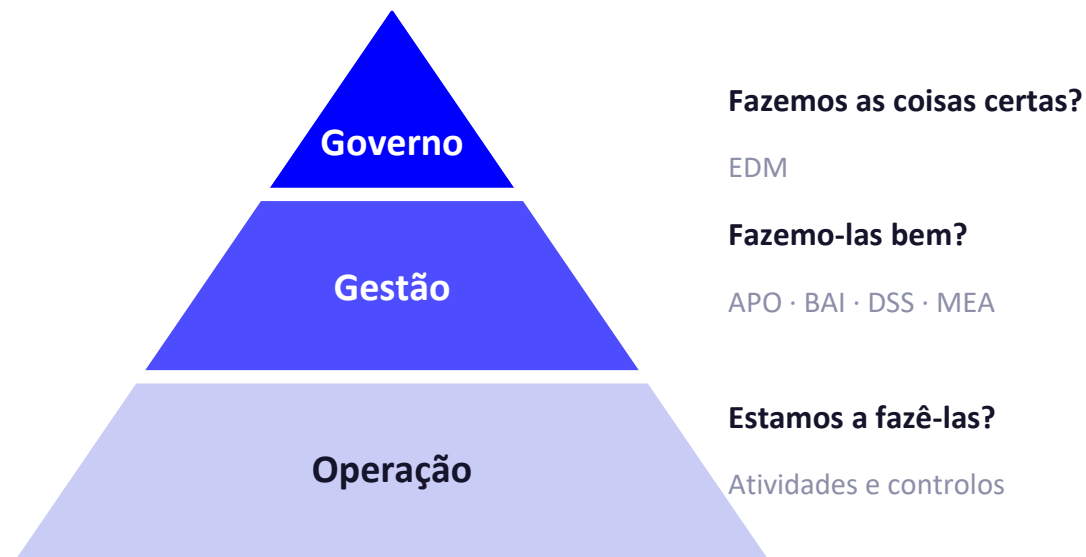
O departamento: é sobre autoridade



No organograma, a TI é uma caixa: tem um chefe, um orçamento e uma linha de reporte. Discute-se a quem responde.

I&T

Informação e Tecnologia: é sobre responsabilidade



Complicado vs. complexo: a segurança tem as duas naturezas

Uma equipa técnica é treinada para pensar de forma linear. Proteger uma organização exige também o oposto.

COMPLICADO

Pensamento linear

- Muitas peças, mas o comportamento é previsível
- Causa e efeito são claros e repetíveis: a regra bloqueia ou não bloqueia
- Existe uma resposta certa: encontra-se com análise, testes e mais dados
- O especialista resolve o problema

RESOLVER · DESCOMPLICAR

Exemplo: configurar uma firewall, corrigir uma vulnerabilidade, ativar MFA.

COMPLEXO

Pensamento não linear

- Causa e efeito só se percebem em retrospectiva
- Os padrões emergem: atacantes, pessoas e fornecedores adaptam-se aos controlos
- Não há uma resposta certa: há riscos aceites melhor ou pior
- A gestão decide na incerteza e mede o que acontece a seguir

DECIDIR · MEDIR

Exemplo: o risco de cibersegurança de uma empresa, a cultura, uma crise.

O erro mais comum de quem vem da técnica: tentar **RESOLVER** a cibersegurança como um problema de engenharia. A segurança governa-se: **DECIDIR** com informação incompleta e medir o que acontece a seguir.

Inspirado no Cynefin Framework (Snowden).

Governance, gestão e operação: cada nível com a sua pergunta

As organizações lidam com este dilema em três níveis, cada um com a sua pergunta, o seu domínio e a sua forma de agir.

GOVERNANCE

Porquê?

Estamos a fazer as coisas certas? Estamos a obter os benefícios com o risco no nível aceite?

COBIT EDM · NIST CSF GV

COMPLEXO

Decidir · Medir valor

GESTÃO

O quê?

Estamos a fazer bem as coisas? Da forma correta?

COBIT APO, BAI, DSS, MEA · SGSI ISO 27001

PONTE

Priorizar · Alocar

OPERAÇÃO

Como?

Estamos a fazer? O controlo funciona como planeado?

CIS Controls · ISO Anexo A · NIST ID, PR, DE, RS, RC

COMPLICADO

Resolver · Executar

Nesta sessão, o objetivo não é aprender mais tecnologia. É pensar a segurança como **GESTOR**, não só como **TÉCNICO**.

A (r)evolução da segurança: cada nome novo alargou o âmbito

A passagem da segurança informática para a segurança da informação, e agora para a cibersegurança, é mais do que uma mudança de nome. **É um alargamento de âmbito e de complexidade.**

A melhor forma de a captar é pensar a segurança como uma abordagem integrada.

Cada nome novo alargou o objeto.

O dever de governar manteve-se.

Na AQUÁRIA, o âmbito certificado parou na segurança de TI. A rede SCADA e a Rede Inteligente ficaram de fora.

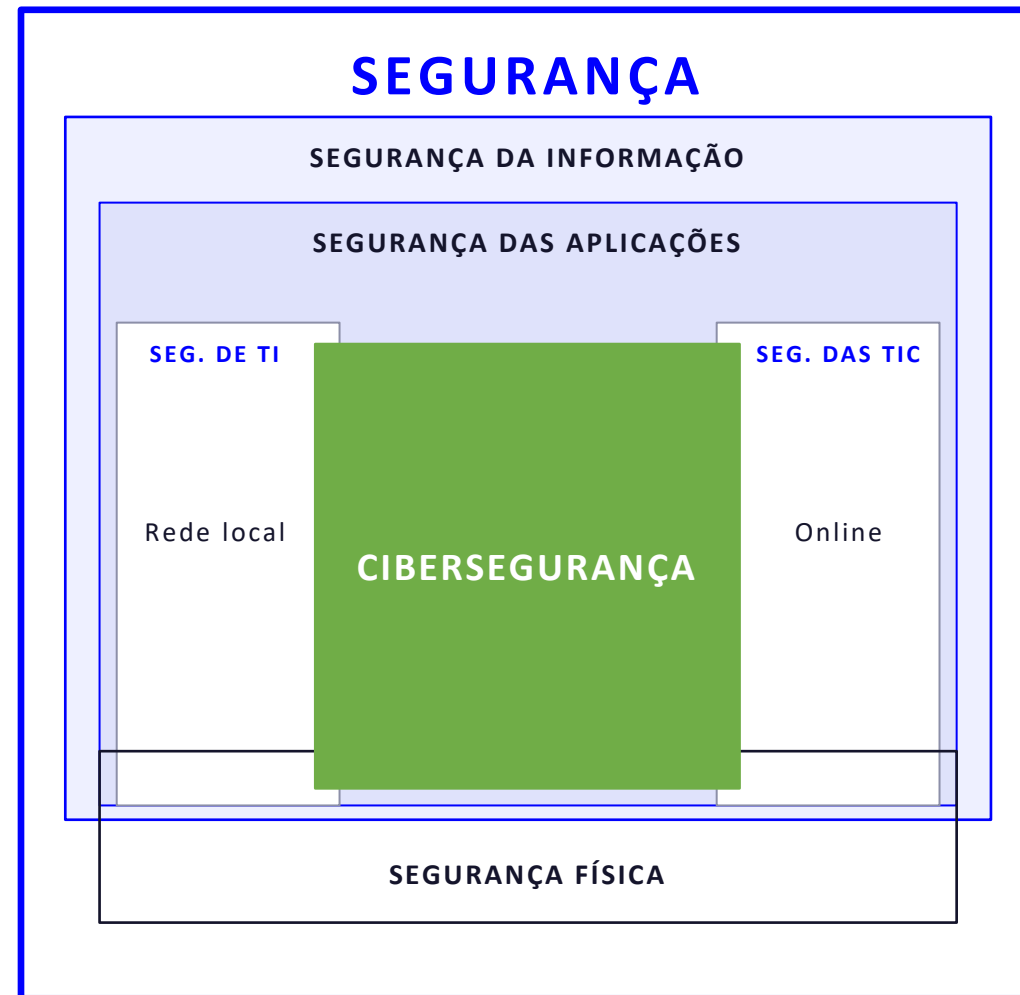


Diagrama adaptado de The FAIR Institute.

IA em todo o lado, confiança em lado nenhum

“

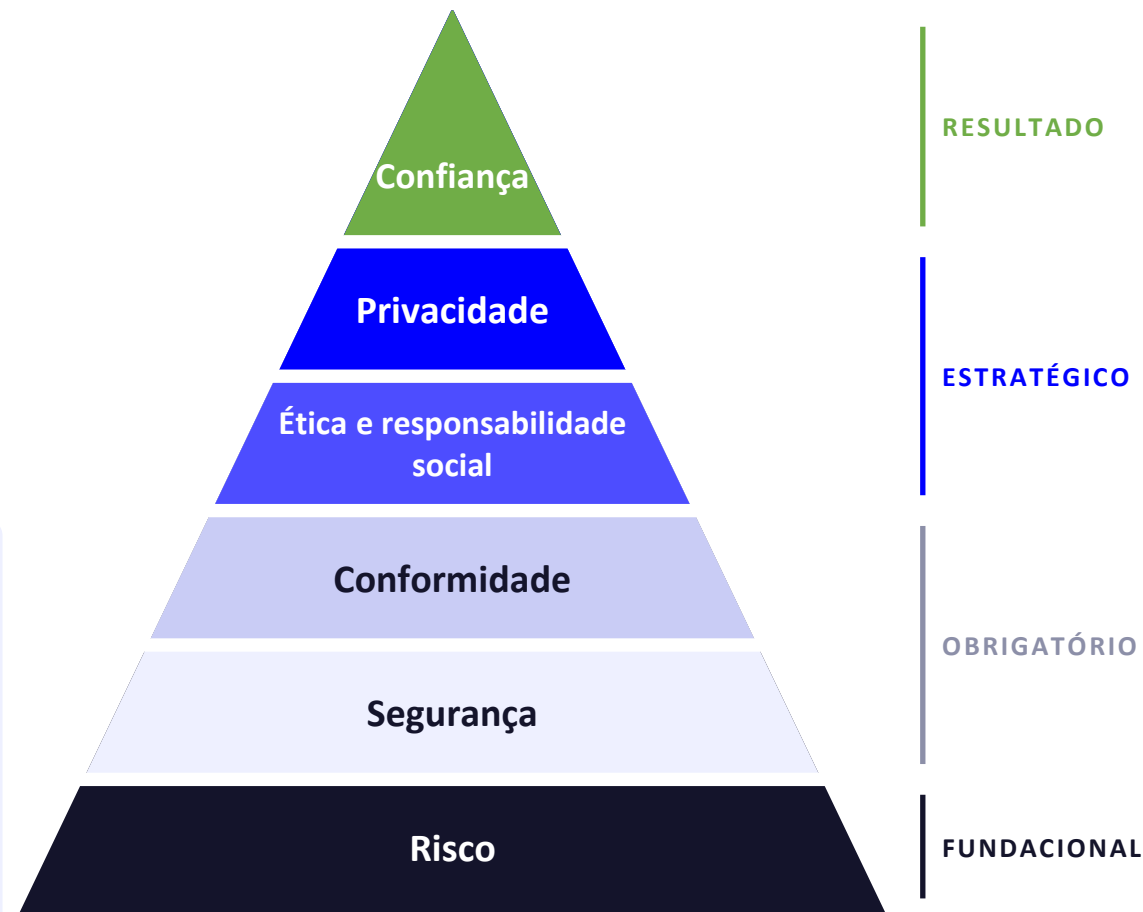
Confia, mas verifica.

Provérbio russo que Ronald Reagan repetiu a Mikhail Gorbachev nas negociações de desarmamento (1987).

Um certificado é uma garantia: quem o recebe confia.

Um controlo testado é uma verificação: quem o testa sabe.

Na AQUÁRIA, "temos certificação" foi confiança. O incidente de março foi a verificação.



Resultados de confiança: no governo · no ecossistema · na economia digital

Pirâmide adaptada de IDC, Future of Trust.



Bloco A

O caso AQUÁRIA

Esta empresa tem ou não um desafio de cibersegurança?

AQUÁRIA – Águas do Vale Verde: uma concessão em ano decisivo

410 mil

habitantes servidos

7

municípios

580

colaboradores

96 M€

volume de negócios

2028

fim da concessão

Estratégia 2025–2028 aprovada pela administração

Renovar a concessão

Negociação com os municípios e o regulador a partir de 2027. Critérios: continuidade do abastecimento, qualidade de serviço, perdas de água, reclamações.

Programa Rede Inteligente

140 mil contadores inteligentes e telemetria em 220 estações e reservatórios. Plataforma de dados na cloud de uma start-up. Meta: perdas de 27% para 18%.

Crescer por aquisição

Integrar em 2026 os serviços municipalizados de um município vizinho (+60 mil habitantes).

Eficiência

Reduzir 8% do custo operacional até 2028.

Caso ilustrativo. A empresa e os dados são fictícios. Texto completo no documento do caso (Moodle).

O que diz o último relatório ao Comité de Risco

Certificação ISO/IEC 27001

Desde 2023. Âmbito: faturação, ERP e sede.

Investimento

Orçamento de cibersegurança +45% em dois anos: EDR, SIEM e SOC externo 24x7 sobre a rede de IT.

Pentest anual

Aplicações web de cliente: sem vulnerabilidades críticas.

Phishing

Taxa de clique nas simulações trimestrais: 4%.

Rede SCADA

Gerida por um fornecedor de automação. Acesso remoto de manutenção com conta partilhada. Postos de operação em Windows 7.

Rede Inteligente

Dados dos contadores na cloud da start-up. Contrato sem cláusulas de segurança nem direito de auditoria.

Incidente em março

Ransomware no prestador de pagamentos: portal e faturação parados 3 dias, 2.300 reclamações, pedido de explicações do regulador. Classificado como "incidente de terceiro".

Governo

Entidade essencial no novo regime de cibersegurança (NIS2). CISO reporta ao CIO. Diretor de Operações fora do Comité de Segurança. Plano de continuidade revisto em 2019.

Na última reunião, a administração concluiu: "A segurança está controlada. Temos certificação, temos SOC e não tivemos nenhum incidente grave."

Exercício 1 · Pitch de 2 minutos à CEO

1**Leiam o caso**

Documento completo no Moodle.
Grupos de 4 a 5 pessoas.

2**Decidam**

A AQUÁRIA tem ou não um desafio de cibersegurança? Qual?

3**Preparem o pitch**

2 minutos para a CEO, Marta Figueiredo: diagnóstico e o que propõem fazer.

Podem usar IA generativa

Use a ferramenta que usam no dia a dia. Guardem o prompt: vamos olhar para ele mais tarde.

Regra: o pitch é vosso. Têm de o defender sem ler o ecrã.

Plenário · 15 min: cada grupo apresenta. A CEO só faz uma pergunta.

"Porquê?"

Porque é que isso importa à AQUÁRIA? Porque é que devo decidir isso agora, e não outra coisa?

Marta Figueiredo, CEO

Um argumento de segurança só aguenta o "porquê?" quando chega ao negócio

Respostas que desmoronam

"Porque os ataques estão a aumentar."

"Porque a NIS2 obriga."

"Porque as boas práticas recomendam zero trust."

"Porque o nosso nível de maturidade é 2 e devia ser 4."

"Porque um concorrente foi atacado."

Falam de segurança, não da empresa. Valem para qualquer organização, por isso não ajudam esta a decidir.

Respostas que aguentam

Objetivo em risco Que objetivo da empresa fica comprometido?

Valor em jogo Quanto vale, em continuidade, receita, multa ou reputação?

Evidência Que dados mostram que o risco é real aqui?

Decisão O que só a gestão pode decidir: âmbito, dono, apetite de risco, investimento?



Bloco B

Da estratégia ao controle

*Porque é que a segurança importa a esta
empresa em particular?*

A cascata de objetivos traduz necessidades das partes interessadas em prioridades de I&T

Drivers e necessidades das partes interessadas

Estratégia, regulação, mercado, acionistas, reguladores

Objetivos da empresa

13 objetivos genéricos (EG01–EG13), organizados pelas perspectivas do balanced scorecard

13

Objetivos de alinhamento

13 objetivos de I&T (AG01–AG13) que suportam os objetivos da empresa

13

Objetivos de governo e de gestão

40 objetivos do core COBIT 2019, nos domínios EDM, APO, BAI, DSS e MEA

40

Como ler

Cada nível responde ao "porquê?" do nível de baixo.

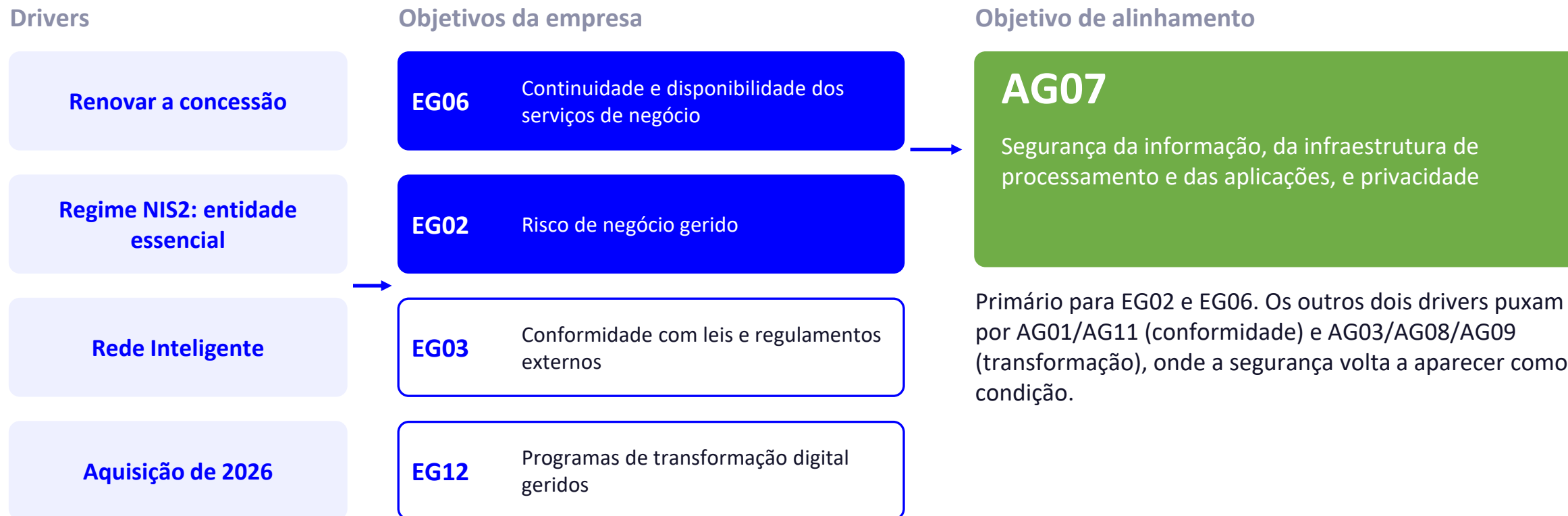
As tabelas de mapeamento indicam relações primárias (P) e secundárias (S).

Os mapeamentos são genéricos: o ponto de partida, não a resposta. Cada organização ajusta-os ao seu contexto.

Funciona nos dois sentidos: de cima para baixo para priorizar, de baixo para cima para justificar.

Fonte: ISACA, COBIT 2019 Framework: Introduction and Methodology; COBIT 2019 Framework: Governance and Management Objectives, Apêndice A.

Na AQUÁRIA, a segurança é primária para dois objetivos de negócio: risco e continuidade



A pergunta da CEO passa a ter resposta: a segurança importa porque sem ela a AQUÁRIA não garante continuidade do abastecimento, e é isso que decide a renovação da concessão.

Fonte: COBIT 2019, Figura A.1 (mapeamento EG-AG). Seleção de drivers e EG para o caso: elaboração própria.

AG07 apoia-se em 15 dos 40 objetivos do core: a segurança não é um processo, é um resultado



Fonte: COBIT 2019 Framework: Governance and Management Objectives, Figura A.2 (mapeamento objetivos de governo e gestão – AG).

O NIST CSF 2.0 toca 39 dos 40 objetivos COBIT, e o DSS05 é o mais referenciado

106

subcategorias do NIST CSF 2.0

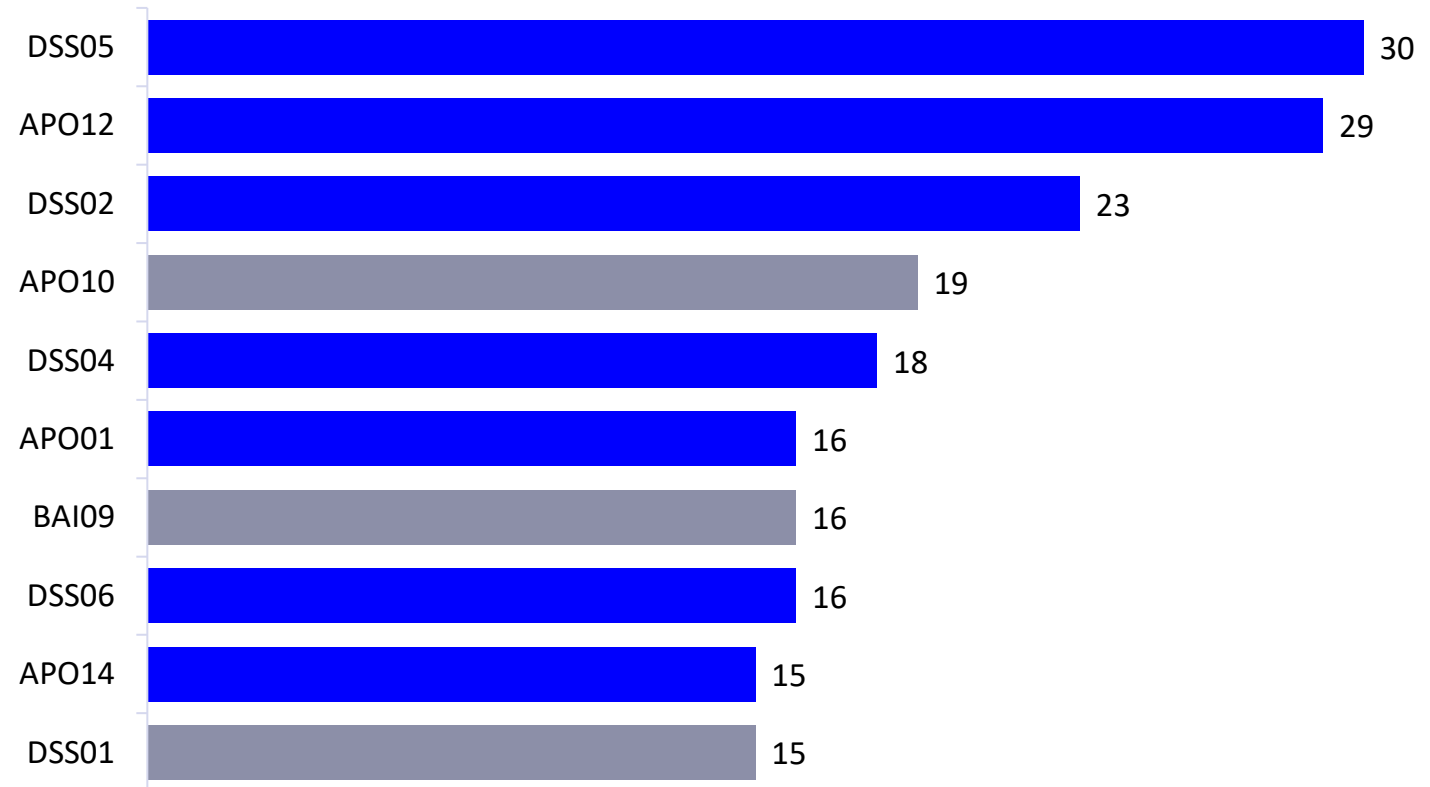
39/40

objetivos COBIT referenciados

85%

das subcategorias ligam-se aos 15 objetivos do AG07

Top 10 objetivos COBIT por nº de subcategorias NIST CSF 2.0 que os referenciam



Azul: objetivos ligados ao AG07. Cinzento: fora do AG07 (fornecedores, ativos, operações).

Fonte: ISACA, Cybersecurity Audit Program – NIST Cybersecurity Framework 2.0 (coluna COBIT References). Contagem e análise: elaboração própria.

Os quatro temas do módulo cabem na mesma cascata

Engenharia social

DSS05.01, atividade 3 (sensibilização sobre malware e phishing) e métrica "% de colaboradores que falham testes de phishing". NIST PR.AT-01. CIS 14.

Gestão de incidentes e comunicação de crise

DSS02 (secundário no AG07), alimentado pelo DSS05.07: os tickets de incidente de segurança seguem para o DSS02.02. NIST RS e RC. CIS 17.

Cultura de cibersegurança

Componente "Cultura, ética e comportamento" do DSS05: responsabilidade de cada utilizador pela segurança e privacidade. ISO 27001 A.6.3.

Contextos críticos e serviços essenciais

DSS04 (primário no AG07) e EG06. Regime NIS2: medidas de gestão de risco, notificação de incidentes e responsabilização do órgão de gestão.



Bloco C

Dentro do DSS05

Como se gere, mede e organiza a segurança operacional?

DSS05 · Managed Security Services: o propósito é de negócio, não técnico

Descrição

Proteger a informação da empresa para manter o nível de risco de segurança da informação aceitável, de acordo com a política de segurança. Estabelecer e manter funções de segurança e privilégios de acesso. Realizar monitorização de segurança.

Propósito

Minimizar o impacto no negócio das vulnerabilidades e incidentes operacionais de segurança da informação.

Domínio DSS (Deliver, Service and Support) · Focus area: COBIT core model

Objetivos primários que suporta

EG02

Risco de negócio gerido

EG06

Continuidade e disponibilidade dos serviços de negócio

AG02

Risco relacionado com I&T gerido

AG07

Segurança da informação, infraestrutura, aplicações e privacidade

É o mesmo par EG02 + EG06 a que chegámos pela cascata da AQUÁRIA.

Fonte: COBIT 2019 Framework: Governance and Management Objectives, DSS05 (tradução livre).

Sete práticas de gestão, 49 atividades com níveis de capacidade de 2 a 4

Prática		Exemplo de métrica da própria ficha
DSS05.01	Proteger contra software malicioso	% de colaboradores que falham testes de phishing
DSS05.02	Gerir a segurança de rede e conectividade	% de tempo de indisponibilidade por incidente de segurança
DSS05.03	Gerir a segurança dos endpoints	Nº de dispositivos não autorizados detetados na rede
DSS05.04	Gerir a identidade dos utilizadores e o acesso lógico	Nº de contas vs. nº de utilizadores autorizados
DSS05.05	Gerir o acesso físico aos ativos de I&T	Nº de incidentes de segurança física
DSS05.06	Gerir documentos sensíveis e dispositivos de output	% de documentos e dispositivos sensíveis inventariados
DSS05.07	Gerir vulnerabilidades e monitorizar a infraestrutura	Tempo de remediação de vulnerabilidades

Fonte: COBIT 2019, DSS05, Componente A: Processo. Atividades por prática: 5, 9, 10, 8, 7, 5, 5.

As métricas para um dashboard de segurança já estão na ficha: falta ligá-las

Administração

Objetivos da empresa

EG06

Horas de processamento perdidas por interrupções não planeadas

EG06

Custo de negócio dos incidentes

EG02

% de serviços críticos cobertos por avaliação de risco

EG02

Incidentes significativos não previstos na avaliação de risco

Gestão de I&T

AG07

AG07

Incidentes de confidencialidade com perda financeira, disrupção ou dano reputacional

AG07

Incidentes de integridade com o mesmo impacto

AG07

Incidentes de disponibilidade com o mesmo impacto

Operação

Práticas DSS05

05.01

% que falha testes de phishing

05.03

Dispositivos não autorizados

05.04

Contas vs. utilizadores

05.07

Tempo de remediação de vulnerabilidades

Fonte: COBIT 2019, DSS05 (example metrics para EG, AG e práticas). Seleção e organização: elaboração própria.

Gerir a segurança exige sete componentes, e só um deles é tecnologia

Processo

1 7 práticas, 49 atividades com níveis de capacidade e métricas

Estruturas organizacionais

2 CISO accountable em 6 das 7 práticas (CIO no DSS05.06). Donos de processos de negócio responsáveis no DSS05.01 e DSS05.04

Fluxos e itens de informação

3 Ex.: tickets de incidente do DSS05.07 para o DSS02.02; resultados de pentest para o MEA04.07

Pessoas, competências

4 Segurança da informação (SFIA SCTY), testes de intrusão (PENT), administração de segurança (SCAD), e-CF E.8

Políticas e procedimentos

5 Política de segurança da informação

Cultura, ética e comportamento

6 Cultura de responsabilidade de cada utilizador pela segurança e privacidade

Serviços, infraestrutura e aplicações

7 IAM, diretório, filtragem de email e URL, SIEM, SOC, sensibilização, avaliação de segurança de terceiros

Na AQUÁRIA, o investimento de dois anos foi quase todo para o componente 7.

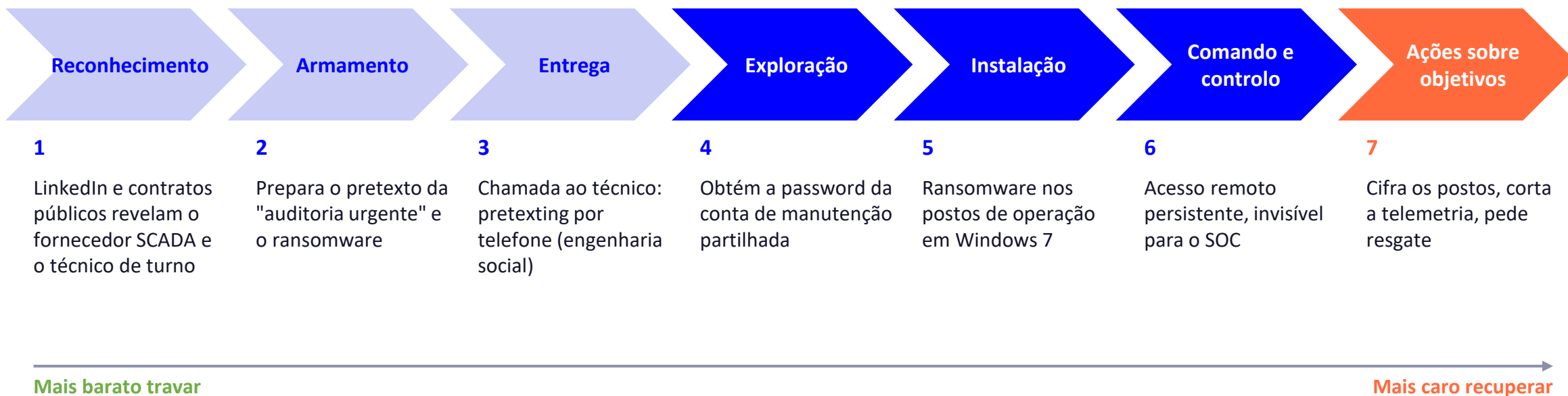


Bloco D

Quando o incidente acontece

*Como prevenimos, respondemos e
comunicamos?*

Um ataque não é um momento: tem um ciclo de vida, do reconhecimento ao impacto



Cada fase é uma oportunidade para detetar e travar o ataque antes do impacto. Na AQUÁRIA, um técnico que desconfiasse da chamada e a reportasse travava tudo na fase 3: é aqui que a cultura de segurança entra na defesa.

Modelo: Lockheed Martin, Cyber Kill Chain (2011). Exemplos: simulação AQUÁRIA.

O MITRE ATT&CK detalha o mesmo ciclo com táticas e técnicas observadas no mundo real

As 14 táticas do ATT&CK Enterprise, e as técnicas que a AQUÁRIA teria visto



Linguagem comum

Atacantes, SOC, fornecedores e auditores descrevem o mesmo ataque com os mesmos códigos

Cobertura de deteção

Para cada técnica: temos forma de a ver? Onde estão os pontos cegos?

Defesa informada pela ameaça

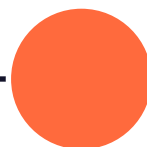
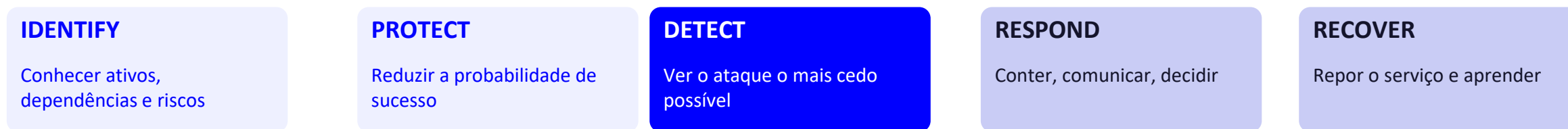
Priorizar controlos pelas técnicas que os grupos ativos no nosso setor usam

Fonte: MITRE ATT&CK Enterprise. Para redes industriais (SCADA) existe a matriz ATT&CK for ICS, com táticas como Inhibit Response Function e Impact.

O ciclo do ataque levou a defesa a organizar-se em ciclo

ANTES

DEPOIS



O ataque

GOVERN atravessa todo o ciclo: contexto, apetite de risco, papéis, políticas, supervisão e fornecedores (NIST CSF 2.0)

A lógica é a do atacante, invertida: as primeiras fases do Kill Chain combatem-se com Identify e Protect; a partir da entrega, com Detect; depois do impacto, com Respond e Recover.

Fonte: NIST Cybersecurity Framework 1.0 (2014), cinco funções; NIST CSF 2.0 (2024) acrescenta Govern.

Antes do ataque falamos de RISCO, depois falamos de INCIDENTE

RISCO

Uma possibilidade

Pergunta	O que pode acontecer, e quanto estamos dispostos a aceitar?
Linguagem	Probabilidade, impacto, apetite
Atividades	Identificar, avaliar, tratar, aceitar
Onde vive	COBIT EDM03, APO12 · NIST GV, ID, PR · ISO 27001 cl. 6 e 8

Na AQUÁRIA: a conta partilhada sem MFA no acesso do fornecedor.

INCIDENTE

Um facto

Pergunta	O que está a acontecer, e como limitamos o impacto?
Linguagem	Severidade, tempo, serviços afetados
Atividades	Detetar, conter, comunicar, recuperar, aprender
Onde vive	COBIT DSS02, DSS04 · NIST DE, RS, RC · ISO 27001 A.5.24–A.5.30

Na AQUÁRIA: a chamada das 15:40 e tudo o que veio depois.

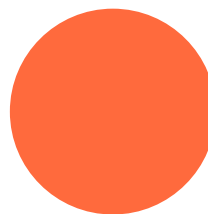
Confundir os dois tem custo: tratar um risco como incidente gera pânico; tratar um incidente como risco atrasa a resposta. As lições do incidente voltam a alimentar o risco.

A NIS2 não multa por ter sido atacado: multa pelo que se fez antes e depois

ANTES · RISCO

Art. 21 · Medidas de gestão de risco: análise de risco e políticas, tratamento de incidentes, continuidade e gestão de crises, cadeia de abastecimento, ciber-higiene e formação, criptografia, controlo de acessos e MFA.

Art. 20 · Órgão de gestão: aprova as medidas, supervisiona a sua aplicação, tem formação, e pode ser responsabilizado.



Ataque

Não é infração

DEPOIS · INCIDENTE

Art. 23 · Notificação de incidentes significativos: aviso prévio em 24 h, notificação em 72 h, relatório final no prazo de um mês.

Destinatários dos serviços: informar, quando apropriado, quem pode ser afetado e que medidas pode tomar.

Na prática: o regulador vai perguntar quando soube, o que fez e quem decidiu.

Coimas para entidades essenciais: até 10 M€ ou 2% do volume de negócios anual mundial, o que for mais elevado (art. 34).

Fonte: Diretiva (UE) 2022/2555 (NIS2), arts. 20, 21, 23 e 34. Confirmar no regime nacional de transposição.

Gerir incidentes obriga a trabalhar em conjunto áreas que normalmente não se falam



Muitas organizações têm vários processos de gestão de incidentes, um por tema.

Quando algo acontece, quem é afetado não é o departamento A ou B: é toda a organização.

Às 19:30 da simulação, a AQUÁRIA precisa do fornecedor SCADA, do SOC externo, das Operações, da DSI, da Comunicação, do Jurídico e da CEO na mesma sala, com uma só cadeia de decisão.

Por isso a gestão de incidentes é um tema de governance, não apenas de operação.



Bloco E

Integrar frameworks

Como falam entre si COBIT, ISO 27001, NIST CSF e CIS Controls?

Cada área tem a sua framework; a segurança só funciona se alguém as orquestrar



Áreas operacionais boas, cada uma do seu lado, não fazem uma boa gestão de segurança. É o tema do bloco E.

Quatro frameworks, quatro perguntas diferentes sobre a mesma realidade

Framework	Pergunta a que responde	Natureza	Estrutura
COBIT 2019	Porquê, e quem decide?	Governo e gestão de I&T ligados a objetivos da empresa	40 objetivos · 7 componentes · cascata de objetivos
ISO/IEC 27001:2022	Como gerimos de forma sistemática e verificável?	Sistema de gestão de segurança da informação, certificável	Cláusulas 4–10 · Anexo A com 93 controlos em 4 temas
NIST CSF 2.0	Que resultados queremos, e onde estamos?	Linguagem comum de resultados, perfis atual e alvo	6 funções · 22 categorias · 106 subcategorias
CIS Controls v8.1	O que fazemos primeiro?	Salvaguardas prescritivas e priorizadas por grupos de implementação	18 controlos · 153 salvaguardas · 56 no IG1

Para uma equipa técnica, a pergunta útil não é "qual adotar?" mas "que pergunta estou a tentar responder?"

As frameworks sobrepõem-se por camadas, e nenhuma cobre todas com a mesma profundidade

	COBIT 2019	ISO 27001	NIST CSF 2.0	CIS v8.1
Governar	EDM01–05	Cl. 5 Liderança	Função GV	—
Gerir o sistema	APO12, APO13	Cl. 4–10 SGSI	Perfis, níveis	—
Definir resultados	Metas e métricas AG/EG	Objetivos do SGSI	ID, PR, DE, RS, RC	Mapeamento CSF
Implementar controlos	Atividades + Related Guidance	Anexo A, 93 controlos	Exemplos de implementação	153 salvaguardas
	Cobertura forte	Cobertura parcial	Fora do âmbito	

O Related Guidance é a ponte do COBIT para o operacional, mas tem de ser atualizado

Exemplo: DSS05.04 · Gerir a identidade dos utilizadores e o acesso lógico

O que a ficha COBIT 2019 cita

ISO/IEC 27002:2013 · 7.3; 9 Controlo de acessos

CIS Controls v6.1 · CSC 1, 2, 5 e 16

NIST SP 800-53 Rev. 5 (draft 2017) · AC, MP, PE

ITIL V3 2011 · Access Management

HITRUST CSF v9 · ISF SoGP 2016



Referências atuais equivalentes

ISO/IEC 27001:2022 · A.5.15–A.5.18, A.8.2, A.8.5

CIS Controls v8.1 · Controlos 5 (contas) e 6 (gestão de acessos)

NIST CSF 2.0 · PR.AA-01 a PR.AA-05, DE.CM-03

NIST SP 800-53 Rev. 5 (final) · famílias AC e IA

As referências da ficha datam de 2011 a 2018. Integrar frameworks é manter um mapa vivo, revisto sempre que uma das referências muda de versão.

Fontes: COBIT 2019, DSS05.04 Related Guidance; ISACA Cybersecurity Audit Program – NIST CSF 2.0; mapeamento ISO e CIS: elaboração própria (indicativa).

Uma prática COBIT, três referenciais operacionais: a matriz de integração do DSS05

Prática DSS05	ISO/IEC 27001:2022 (Anexo A)	NIST CSF 2.0	CIS Controls v8.1
05.01 Malware	A.8.7, A.8.8, A.6.3	ID.RA-01/03, PR.AT-01, PR.DS-01/02, PR.PS-02/03/05	10, 9, 7, 14
05.02 Rede e conectividade	A.8.20, A.8.21, A.8.22, A.8.24	ID.AM-03, ID.RA-01, PR.DS-02, PR.IR-01, DE.CM-01	12, 13, 4, 3.10, 18
05.03 Endpoints	A.8.1, A.8.9, A.6.7, A.7.9, A.7.14	PR.DS-01/02, PR.IR-01, DE.CM-02, RS.MI-01	1, 4, 10, 3.6
05.04 Identidade e acesso lógico	A.5.15–A.5.18, A.8.2, A.8.5	PR.AA-01 a 05, DE.CM-03	5, 6
05.05 Acesso físico	A.7.1–A.7.4	PR.AA-06, PR.AT-01, DE.CM-02/03	Fora do âmbito
05.06 Documentos e dispositivos sensíveis	A.5.10, A.5.12, A.7.10, A.8.24	ID.AM-07, PR.AA-05, PR.DS-01/10	3
05.07 Vulnerabilidades e monitorização	A.8.8, A.8.15, A.8.16, A.5.7	ID.RA-01/04/08, DE.CM-01/09, DE.AE-02/03/06/07, RS.AN-03, RS.MI-01	7, 8, 13, 18

NIST CSF 2.0: ISACA Cybersecurity Audit Program (referências COBIT por subcategoria). ISO 27001 e CIS v8.1: mapeamento indicativo, elaboração própria; validar com os mapeamentos oficiais do CIS e da ISO.

O que a matriz revela: sobreposição, lacunas e um elo que só a governance fornece

Sobreposição

Testar uma vez, reportar muitas

A revisão periódica de acessos (DSS05.04) é evidência para A.5.18, PR.AA-05 e CIS 6 ao mesmo tempo. Um programa integrado reduz trabalho de auditoria e de conformidade.

Lacunas

Cada referencial tem pontos cegos

Os CIS Controls não cobrem segurança física. O CIS e as funções PR/DE do CSF não dizem quem decide nem quanto risco aceitar. A ISO não prioriza salvaguardas técnicas.

O elo em falta

Sem cascata, não há valor

O CSF 2.0 abre com GV.OC-01: a missão orienta a gestão do risco. A ISACA mapeia-o para EDM01 e APO01. É o mesmo ponto de partida da cascata COBIT.

A função Govern do NIST CSF 2.0 fecha o círculo que abrimos com a pergunta da CEO

GV.OC

Contexto organizacional

COBIT: EDM01, EDM05, APO01, APO02, DSS04...

GV.RM

Estratégia de gestão do risco

COBIT: EDM03, APO12, APO13...

GV.RR

Papéis, responsabilidades e autoridade

COBIT: EDM01, EDM04, APO01, APO07...

GV.PO

Política

COBIT: EDM01, EDM03, APO01, DSS04...

GV.OV

Supervisão

COBIT: EDM02, MEA01, MEA02, MEA03...

GV.SC

Risco da cadeia de fornecimento

COBIT: APO10, APO12, EDM02, DSS01...

Porque importa

A versão 2.0 acrescentou o Govern para ligar resultados técnicos à estratégia e à supervisão.

As referências cruzadas mostram que essa ligação é, na prática, território COBIT.

Na AQUÁRIA, GV.SC é a categoria mais exposta: fornecedor SCADA, start-up da cloud, prestador de pagamentos.

Fonte: NIST CSF 2.0; ISACA Cybersecurity Audit Program – NIST CSF 2.0 (referências COBIT por categoria GV, seleção).

Rastrear um achado de ponta a ponta: do controlo técnico à renovação da concessão

Achado: acesso remoto do fornecedor à rede SCADA com conta partilhada

CIS v8.1

5.1 Inventário de contas · 6.4 MFA no acesso remoto (IG1) · 15.4 Requisitos de segurança nos contratos

NIST CSF 2.0

PR.AA-01 e PR.AA-03 · DE.CM-06 Monitorizar atividade de fornecedores · GV.SC-05 Requisitos na cadeia de fornecimento

ISO 27001:2022

A.5.16 Gestão de identidades · A.8.5 Autenticação segura · A.5.20 Segurança nos acordos com fornecedores

COBIT · prática

DSS05.04 atividade 6: todos os utilizadores, incluindo externos e temporários, identificáveis de forma única · APO10 Fornecedores

COBIT · objetivos

AG07 Segurança da informação e da infraestrutura → EG06 Continuidade dos serviços → EG02 Risco

Driver

Continuidade do abastecimento: critério da renovação da concessão e obrigação NIS2

Para cima: justificar. Para baixo: implementar.



Bloco F

Voltar à CEO

O que dizemos agora, que aguenta o "porquê?"

Pitch 2.0 · Uma recomendação que aguenta o "porquê?"

1

Objetivo em risco

Que EG e que driver?
(cascata)

2

Evidência

Que métricas de EG e
AG07 o mostram?
(dashboard)

3

Lacuna

Em que componentes e
práticas? (DSS05 e
vizinhos)

4

Decisão pedida

O que só a CEO pode
decidir: âmbito, dono,
apetite de risco,
investimento

5

Como vamos medir

Metas e referenciais de
controlo (CIS, NIST, ISO)

Comparem com o primeiro pitch e com o que a IA vos deu. O que mudou não foi a tecnologia proposta, foi o argumento.

A AQUÁRIA tem um desafio de segurança, mas não onde investiu

O diagnóstico

O perímetro de IT certificado está razoavelmente protegido. O valor em jogo (continuidade do abastecimento, renovação da concessão, Rede Inteligente, aquisição) depende de OT, fornecedores e continuidade, que estão fora do âmbito do que é governado e medido.

É um problema de governo, não de ferramentas.

Decisões que só a gestão pode tomar

Âmbito	Alargar o SGSI e o governo de segurança à OT, à Rede Inteligente e aos fornecedores críticos.
Dono	CISO com mandato transversal; Diretor de Operações no Comité de Segurança.
Continuidade	BIA e plano de continuidade revistos com cenários de ciberataque, incluindo em terceiros.
Fornecedores	Requisitos de segurança e direito de auditoria nos contratos; contas nominais e MFA no acesso remoto.
Métricas	Indicadores de EG06 no reporte à administração, incluindo incidentes com origem em terceiros.

Para levar para segunda-feira

1

Comecem pelo porquê

Antes de propor um controlo, identifiquem o objetivo de negócio que ele protege. Se não o encontram, o cliente também não vai encontrar.

2

Integrem, não escolham

COBIT para o porquê e o quem, ISO 27001 para o sistema, NIST CSF para os resultados, CIS para o que fazer primeiro. Um mapa vivo entre eles poupa trabalho e evita lacunas.

3

Meçam em camadas

Cada métrica operacional deve ter um caminho até uma métrica que a administração reconhece.

Questionário de Satisfação

- A sua opinião é muito importante para nós, na medida em que nos auxilia a identificar os aspetos que deverão ser alvo de melhoria. Deste modo, solicitamos que preencha o questionário, que nos permitirá melhorar a qualidade.

  01 Segurança de Redes 

Formador: Rui Duro | rui.duro@gmail.com

 QUESTIONÁRIO
Questionário - Rui Duro 

  02 Proteção e Privacidade de Dados 

Formador: Bruno Marques | bruno.armarques@gmail.com

 Assiduidade 

 QUESTIONÁRIO
Questionário - Bruno Marques 

  03 Princípios Técnicos em Cibersegurança 

Formador: Henrique Domingos | hj@fct.unl.pt

 QUESTIONÁRIO
Questionário - Henrique Domingos 

  04 Formação Intermédia em Cibersegurança 

Formador: Bruno Soares | bruno.soares@govaas.com

 QUESTIONÁRIO
Questionário - Bruno Soares 

Keep Learning. Keep in touch.

✉ info.executive@fct.unl.pt

