



Cibersegurança na era Industrial 4.0

Como proteger uma PME industrial do Tâmega e Sousa contra *ransomware*, fraude, intrusão e interrupção da produção

01/10/2026

Marco Gomes | mfg@estg.ipp.pt



whoami



Professor e Investigador

Inteligência Artificial <-> Segurança Informática

mailto: mfg@estg.ipp.pt

UTPORTO Universidade Técnica
do Porto

Agenda

- Objetivo
- Definição conceptual e terminológica
- Contextualização
- A fábrica digital
- I.A. e (Ciber)segurança
- Exercício de incidente
- Boas práticas

Cibersegurança na era Industrial 4.0

Como proteger uma PME industrial do Tâmega e Sousa contra *ransomware*, fraude, intrusão e interrupção da produção

Objetivo



Principais Ideias

- ◆ Prevenir
- ◆ Detetar
- ◆ Responder
- ◆ Adaptar

Uma PME industrial resistente não é aquela que apenas evita ataques, mas aquela que consegue prevenir, detetar, responder e adaptar-se quando estes acontecem.

A abordagem será concretizada através de exemplos práticos da indústria do Tâmega e Sousa de como um incidente cibernético pode afetar não apenas os sistemas informáticos, mas também máquinas, processos produtivos, propriedade intelectual, fornecedores e continuidade da atividade.

Definição: Indústria 4.0

International Journal on Interactive Design and Manufacturing (IJIDeM) (2025) 19:667–679

669

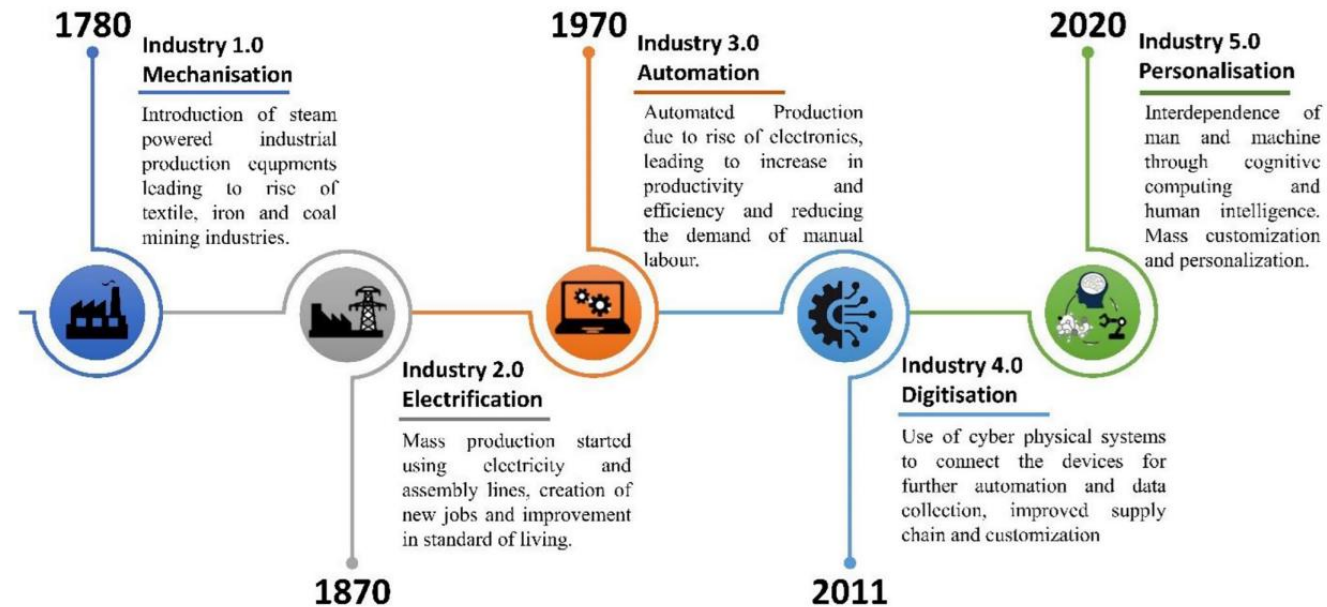


Fig. 1 Timeline and essentials of industrial revolutions

Fonte: <https://link.springer.com/content/pdf/10.1007/s12008-024-01943-7.pdf>

Definição: Indústria 4.0

Simplificando:

- Industrial Internet of Things (IIoT)

Sensores industriais, controladores, etc., ligados à Internet

- Smart Manufacturing

Transformação de processos de manufatura/indústria através de dados, analítica, aprendizagem computacional, etc.

- Industry 4.0

Poder-se-á definir como a combinação de IIoT e Smart Manufacturing

Definição: (Ciber)Segurança

De acordo com os referenciais do Centro Nacional de Cibersegurança (CNCS), a **cibersegurança** foca-se na proteção do ciberespaço e de ativos digitais contra ameaças virtuais, enquanto a **segurança da informação** (ou segurança informática num sentido clássico de salvaguarda de dados) possui um âmbito mais transversal que abrange a proteção da informação em qualquer formato

Definição: IT vs OT

	Information Technology	Operational Technology
Foco	Informação e sistemas digitais	Operações e processos físicos
Objetivo	Gerir dados, aplicações e comunicações	Monitorizar/controlar máquinas e processos
Exemplos	PC, servidores, nuvem, ERP, e-mail, redes	PLC, SCADA, sensores, robôs, sistemas industriais
Impacto de uma falha	Perda de dados, indisponibilidade de serviços	Paragem de produção, danos em equipamentos ou riscos de segurança
Prioridades	Confidencialidade, integridade, disponibilidade	Segurança física, continuidade e disponibilidade

Contexto: legal e normativo

- O contexto legal e normativo da cibersegurança em Portugal aplicável à indústria sofreu uma reformulação profunda. O país transitou de recomendações técnicas para obrigações legais vinculativas e severas, impulsionadas pela legislação europeia.
- O **Decreto-Lei n.º 125/2025** transpôs para o ordenamento jurídico nacional a Diretiva Europeia **NIS2**. Este regime alargou drasticamente o número de empresas e setores industriais abrangidos.

Contexto: legal e normativo

- Quem está abrangido na Indústria? Médias e grandes empresas (geralmente com mais de 50 colaboradores e volume de negócios superior a 10 milhões de euros) que operem em setores críticos. Isto inclui a indústria transformadora (ex: automóvel, química, farmacêutica, têxtil, alimentar), gestão de resíduos, energia e fornecedores digitais.
- As empresas são divididas entre Entidades Essenciais e Entidades Importantes, dependendo do impacto e tamanho do negócio

Contexto: legal e normativo

- Quem está abrangido na Indústria? Médias e grandes empresas (geralmente com mais de 50 colaboradores e volume de negócios superior a 10 milhões de euros) que operem em setores críticos. Isto inclui a indústria transformadora (ex: automóvel, química, farmacêutica, têxtil, alimentar), gestão de resíduos, energia e fornecedores digitais.
- As empresas são divididas entre Entidades Essenciais e Entidades Importantes, dependendo do impacto e tamanho do negócio

Contexto: legal e normativo

Para cumprir a lei, as indústrias devem basear os seus controlos em referenciais estruturados:

- **QNRCS (Quadro Nacional de Referência para a Cibersegurança):** Anexo ao Regulamento n.º 756/2026, define as medidas mínimas e os níveis de conformidade técnica exigidos.
- **ISO/IEC 27001:** O padrão global para Sistemas de Gestão de Segurança da Informação. Indústrias que já possuem esta certificação têm grande parte do caminho de conformidade legal simplificado.
- **IEC 62443:** A norma internacional de referência específica para a Cibersegurança em Automação Industrial e Sistemas de Controlo (OT). Essencial para proteger as linhas de produção fabris (scada, PLCs) das ameaças que o ecossistema puramente cor.porativo (TI) enfrenta

Contexto: incidentes ciberfísicos

Malware May Have Targeted Iran's Nuclear Program—and Predates Stuxnet

Researchers have finally cracked Fast16, mysterious

Contexto: incidentes ciberfísicos



- 2012: Em poucas horas, 35 mil computadores foram parcial ou totalmente “destruídos”.
- O *malware* apagou o Master Boot Record (MBR), substituindo os dados por uma imagem de uma bandeira americana em chamas e tornando as máquinas incapazes de inicializar.

Contexto: incidentes ciberfísicos

Merck settles with insurance companies over \$1.4B claim tied to 2017 cyberattack: report

By Kevin Dunleavy · Jan 5, 2024 8:13am

Merck

cyberattack

Ransomware

- O ciberataque com o *malware* NotPetya à farmacêutica Merck em 2017 custou mais de 1,3 mil milhões de dólares em danos operacionais e de vendas perdidas, gerando uma longa batalha jurídica com as seguradoras
- Mais de 40.000 máquinas da empresa foram infetadas.
- A produção e redes de investigação paralisadas durante cerca de uma semana.

Contexto: *status quo*

Políticas e Práticas de Cibersegurança dos Técnicos Operacionais na Indústria 4.0 Estimar os custos de um incidente

Estimativa dos custos da recuperação da automação no caso de incidente, por tamanho da organização, na Indústria 4.0, Portugal, 2021 (segundo TO)

Tamanho da organização	Número de trabalhadores	Custo médio (euros)	% de Respondentes
Micro	até 9	16 867	38%
Pequena	de 10 a 49	66 266	14%
Média	de 50 a 249	14 014	33%
Grande	250 ou mais	83 333	14%
Total			9%

4. É capaz de estimar o custo de recuperação da automação no caso de uma interrupção provocada por um incidente:

9%



- Para apenas 9% dos técnicos operacionais as suas organizações são capazes de estimar o custo de recuperação de um incidente;
- Entre estes, resulta que as grandes empresas têm custos mais elevados (média de cerca de 83 mil euros), mas também têm menos capacidade de estimativa do que as micro e médias empresas (para estas os custos são em média de 66 mil euros).

Fonte: <https://www.cncs.gov.pt/docs/inquerito-industria-40.pdf>

Contexto: *status quo*

Políticas e Práticas de Cibersegurança dos Técnicos Operacionais na Indústria 4.0 Estimar os custos de um incidente

Estimativa dos custos da recuperação da automação no caso de incidente, por tamanho da organização, na Indústria 4.0, Portugal, 2021 (segundo TO)

Tamanho da organização	Número de trabalhadores	Custo médio (euros)	% de Respondentes
Micro	até 9	16 867	38%
Pequena	de 10 a 49	66 266	14%
Média	de 50 a 249	14 014	33%
Grande	250 ou mais	83 333	14%
Total			9%

4. É capaz de estimar o custo de recuperação da automação no caso de uma interrupção provocada por um incidente:

9%

- Para apenas 9% dos técnicos operacionais as suas organizações são capazes de estimar o custo de recuperação de um incidente;
- Entre estes, resulta que as grandes empresas têm custos mais elevados (média de cerca de 83 mil euros), mas também têm menos capacidade de estimativa do que as micro e médias empresas (para estas os custos são em média de 66 mil euros).



Fonte: <https://www.cncs.gov.pt/docs/inquerito-industria-40.pdf>

A fábrica digitalizada

Se amanhã, às 8:00, todos os seus sistemas computacionais deixassem de funcionar, conseguiria continuar a produzir?

A fábrica digitalizada

Numa fábrica conectada, também designada por *smart factory*, os equipamentos industriais, sensores, sistemas de controlo e plataformas digitais estão permanentemente ligados e partilham informação entre si.

A principal vantagem deste modelo é a elevada eficiência que resulta da integração e da troca contínua de informação entre os diferentes sistemas. Contudo, esta mesma conectividade representa também uma das suas principais vulnerabilidades.

A fábrica digitalizada

«Quanto mais digitalizada e conectada está a fábrica, maior é a superfície de ataque!»

As fábricas tradicionais tinham uma vantagem de segurança por obscuridade: sistemas isolados, desconectados, funcionavam de forma previsível e controlada. Um atacante precisaria de acesso físico à instalação para causar danos. Numa fábrica conectada, o cenário é radicalmente diferente.

A fábrica digitalizada

«Quanto mais digitalizada e conectada está a fábrica, maior é a superfície de ataque!»

As fábricas tradicionais tinham uma vantagem de segurança por obscuridade: sistemas isolados, desconectados, funcionavam de forma previsível e controlada. Um atacante precisaria de acesso físico à instalação para causar danos. Numa fábrica conectada, o cenário é radicalmente diferente.

Fonte: <https://mintforpeople.pt/noticias/seguranca-cibernetica-industria-4-0-fabricas-conectadas/>

A fábrica digitalizada

«Quanto mais digitalizada e conectada está a fábrica, maior é a superfície de ataque!»

- *Qualquer falha ou ataque pode parar linhas de produção inteiras.*
- *Riscos de roubo de propriedade intelectual, sabotagem ou violação de dados.*
- *Aumento da superfície de ataque devido à conectividade entre sistemas.*

Fonte: <https://mintforpeople.pt/noticias/seguranca-cibernetica-industria-4-0-fabricas-conectadas/>

A fábrica digitalizada

«Quanto mais digitalizada e conectada está a fábrica, maior é a superfície de ataque!»

*Além disso, os sistemas industriais foram historicamente desenvolvidos com foco em funcionamento e confiabilidade, não em segurança. Muitos PLCs e máquinas **industriais funcionam com softwares com dezenas de anos**, sem atualizações de segurança. Quando esses sistemas foram criados, a ideia de conectá-los à internet era impensável e a segurança cibernética não era considerada.*

Fonte: <https://mintforpeople.pt/noticias/seguranca-cibernetica-industria-4-0-fabricas-conectadas/>

O Tâmega e Sousa como “laboratório industrial”

Setor	Empresa fictícia	Dependência digital
Calçado	#1	ERP + CAD + máquinas + produção
Têxtil	#2	ERP + teares + sensores + nuvem
Mobiliário	#3	CNC + CAD/CAM + ERP
Metalomecânica	#4	CNC + PLC + SCADA + ERP

Caso #1 “O ransomware entra pelo escritório e chega à fábrica

- Uma empresa de calçado tem:

Internet | Firewall | Rede administrativa | AD / Windows / ERP | Servidor de produção | Máquinas industriais

- Um funcionário recebe: “Fatura urgente – pagamento em atraso”
- Abre o ficheiro e
- “Onde deveriam existir barreiras para impedir que o ataque chegasse à produção?”

Caso #2 - quando a máquina passa a ser um alvo

- Uma empresa de metalomecânica tem:

ERP | Servidor de produção | SCADA | PLC | CNC | Peça produzida

- Um acesso remoto utilizado pelo fabricante da máquina está permanentemente ativo.
- “Se essa VPN for comprometida, o que consegue o atacante alcançar?”

Caso #3 - A máquina precisa de manutenção

- Uma máquina CNC apresenta uma falha:

ERP | Servidor de produção | SCADA | PLC | CNC | Peça produzida

- O técnico do fabricante pede: "Preciso de acesso remoto à máquina."
- O responsável de IT cria: VPN → rede interna → máquina
- Qual a abordagem que permite à empresa continuar a ter assistência técnica sem entregar a fábrica inteira ao fornecedor?

Caso #4 - Phishing dirigido ao diretor financeiro

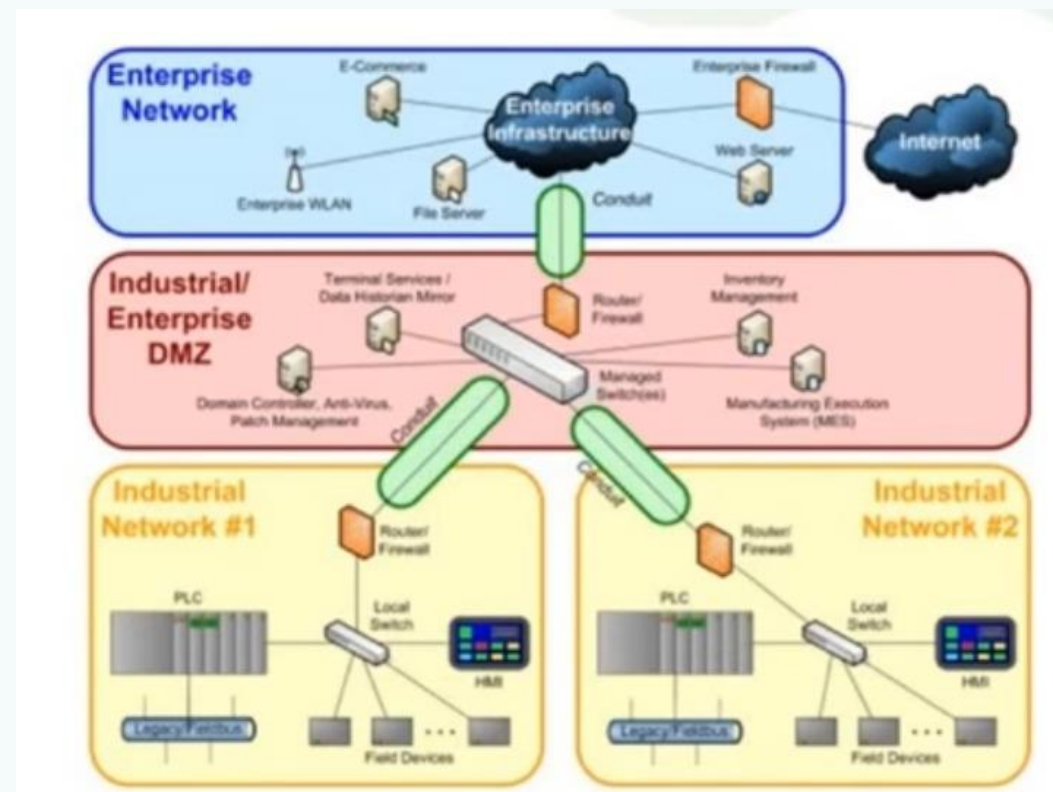
- O diretor financeiro recebe: «Alteração da conta bancária do fornecedor X»
- A mensagem parece vir do fornecedor.
- O atacante já comprometeu a conta de e-mail de um funcionário.
- A empresa altera o IBAN.
- É feita uma transferência de €42.000.

Caso #4 - Phishing dirigido ao diretor financeiro

- O diretor financeiro recebe: «Alteração da conta bancária do fornecedor X»
- A mensagem parece vir do fornecedor.
- O atacante já comprometeu a conta de e-mail de um funcionário.
- A empresa altera o IBAN.
- É feita uma transferência de €42.000.

Arquitetura de Cibersegurança

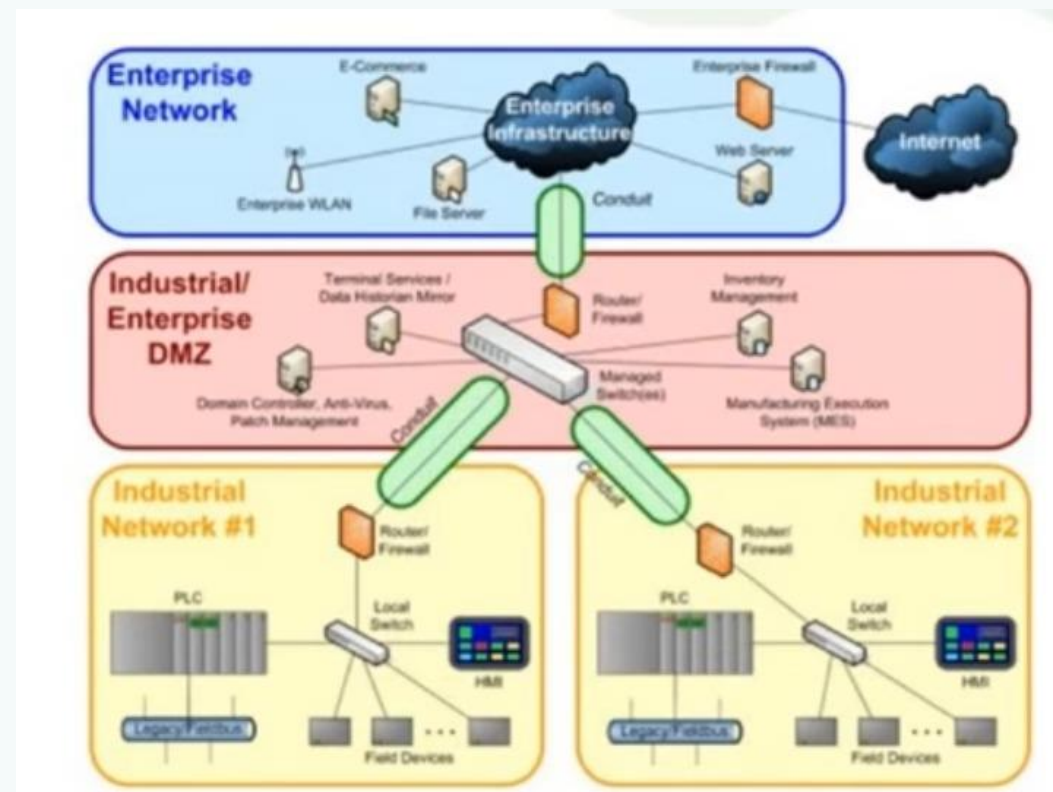
- Defesa em camadas
 - Profundidade
 - Diversidade
 - Desconfiança total (zero-trust)
 - Defesa ativa
- Standards/referenciais



Fonte: <https://www.youtube.com/watch?v=HMi802kb4tg>

Arquitetura de Cibersegurança

- Defesa em camadas
- Standards/referenciais
 - IEC 62443
 - Cibersegurança de sistemas de automação e controlo industrial (IACS/OT)
 - ISO/IEC 27001:2022
 - Sistema de gestão de segurança da informação (ISMS/SGSI)
 - NIST SP 800-82 Rev. 3
 - Guia específico para segurança de OT/ICS
 - IEC 61508 / IEC 61511
 - Segurança funcional de sistemas industriais
 - IEC 62443-4-1 / 4-2
 - Segurança de produtos/componentes industriais



Fonte: <https://www.youtube.com/watch?v=HMi802kb4tg>

Arquitetura de Cibersegurança

As 10 perguntas que uma fábrica deve conseguir responder

- Sabemos quais são todos os nossos ativos IT e OT?
- Sabemos quais estão ligados à Internet?
- Existe separação entre IT e OT?
- Temos MFA nas contas críticas?
- Sabemos quem tem acesso remoto às máquinas?
- Os acessos dos fornecedores são temporários e registados?
- Temos backups offline/imutáveis?
- Conseguimos detetar comportamento anómalo?
- Sabemos o que fazer se amanhã perdermos o ERP?
- Já testámos a recuperação de uma fábrica após um incidente?

Arquitetura de Cibersegurança

Uma abordagem prática à cibersegurança das PME industriais pode ser estruturada em quatro momentos fundamentais:

- **Prevenir** - identificar ativos, vulnerabilidades e riscos, proteger redes e sistemas, controlar acessos e reforçar a segurança de pessoas, equipamentos e fornecedores.
- **Detetar** - reconhecer rapidamente comportamentos anómalos, intrusões, malware, *ransomware* e outras ameaças, recorrendo a monitorização, análise de eventos e, quando adequado, Inteligência Artificial.
- **Responder** - atuar perante um incidente, limitando o seu impacto na produção, informação e continuidade do negócio, através de procedimentos de contenção, comunicação, investigação e recuperação.
- **Adaptar** - aprender com os incidentes e transformar essa experiência em melhoria contínua, reforçando processos, tecnologias, competências e capacidade de resiliência.

Mudança: I.A. & Cibersegurança

Mudança no mercado

- Diferentes tipos de risco cibernético – o panorama das ameaças alterou-se
- *Deepfakes*
- (ph-v-sm)shing personalizados
- Exfiltração de dados
- Má utilização de privilégios

Mudança na tecnologia

- Atores com menor competência técnica
- Velocidade
- Escala
- Detecção e resposta a ameaças

Mudança: I.A. & Cibersegurança

Mudança no mercado

- Diferentes tipos de risco cibernético – o panorama das ameaças alterou-se
- *Deepfakes*
- (ph-v-sm)shing personalizados
- Exfiltração de dados
- Má utilização de privilégios

Mudança na tecnologia

- Atores com menor competência técnica
- Velocidade
- Escala
- Detecção e resposta a ameaças

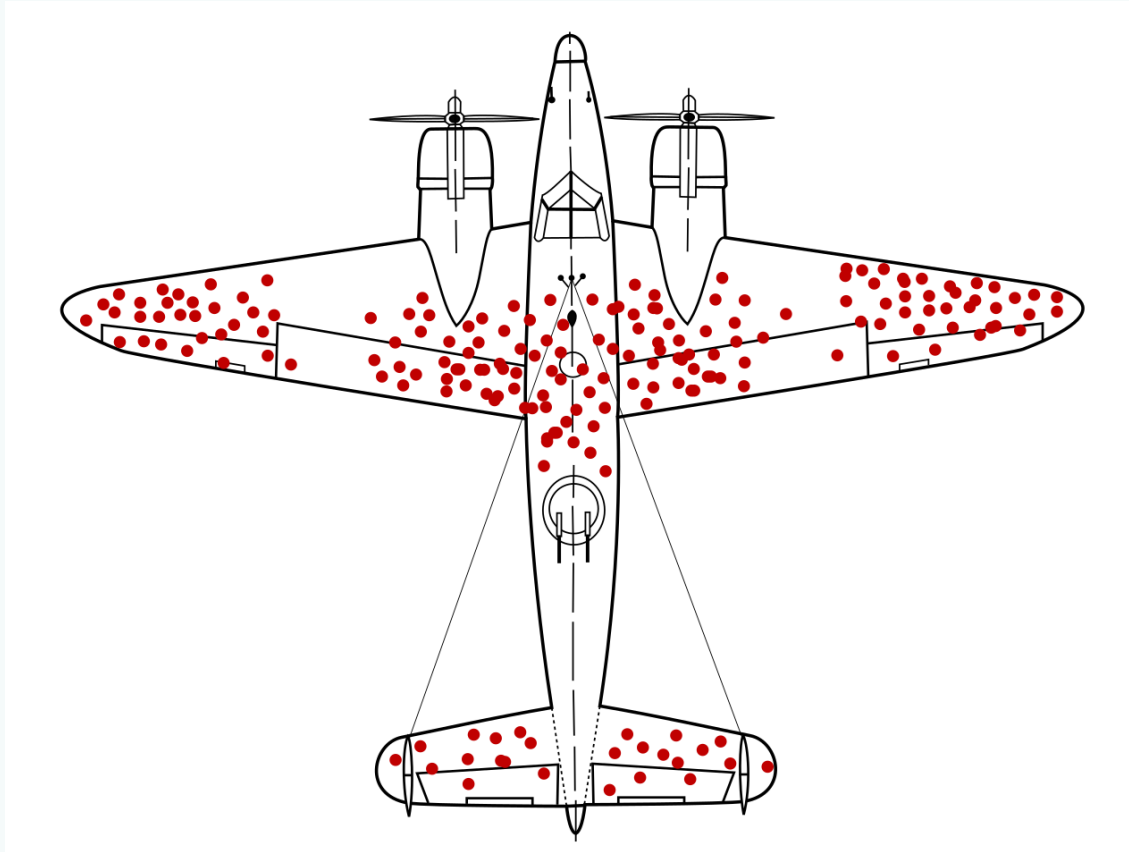
Mudança: I.A. & Cibersegurança

A I.A. não elimina o risco: aumenta a capacidade de o identificar, analisar e compreender em tempo útil.

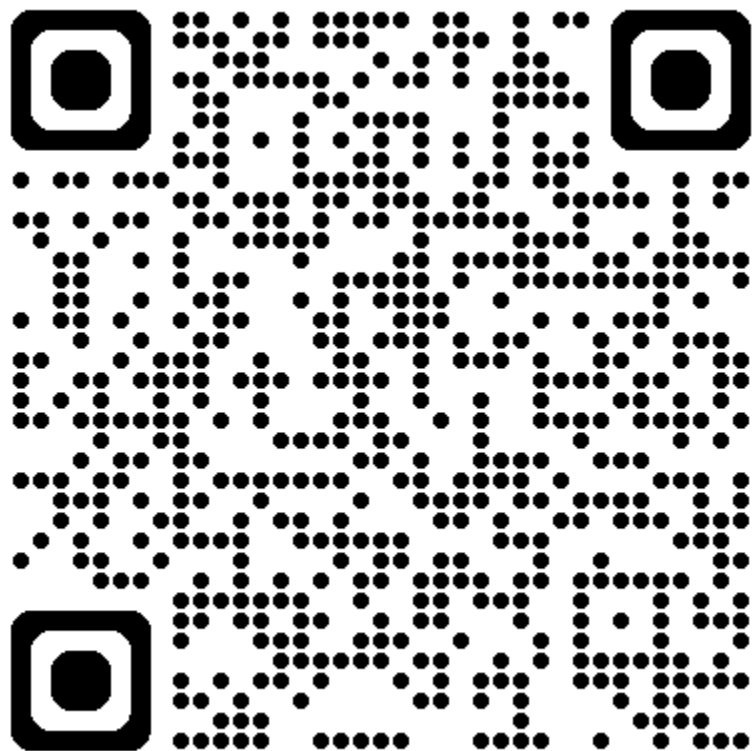
A I.A. não cria novos riscos, potencia os existentes.

Preocupação acrescida com os dados pessoais, segredos de negócio, dependência tecnológica e soberania digital.

Mudança: I.A. & Cibersegurança



Formulário



- <https://forms.gle/F1egKEeGUPgUUQMy6>



- **Email:** geral@twins4ts.pt
- **Site:** www.twins4ts.pt
- **LinkedIn:** linkedin.com/company/twins4ts
- **Marco Gomes:** mfg@estg.ipp.pt



Ficha Técnica

Designação do Projeto | TWINS4TS - Digital Twins & IA para as Indústrias Transformadoras do Tâmega e Sousa

Nº do projeto | 25480

Promotores |

CETS – Conselho Empresarial do Tâmega e Sousa

IPP-ESTG - Escola Superior de Tecnologia e Gestão

Aviso | COMPETE2030-2025-4

Designação do aviso | Ações Coletivas – Digitalização

Tipologia de Ação | Transição Digital das Empresas

Objetivos | Aproveitar as vantagens da digitalização para os cidadãos, as empresas, os organismos de investigação e as autoridades públicas (FEDER)

Marco Gomes



Cibersegurança na Era Industrial 4.0: Proteger PME Digitais

Como proteger uma PME industrial do Tâmega e Sousa contra *ransomware*, fraude, intrusão e interrupção da produção

01/10/2026

Marco Gomes | mfg@estg.ipp.pt

