

# QUEM é QUEM

nos TET com Portugal  
2019



O Jornal Económico



**Paulo Pinto**

Diretor Geral | CESCE SI

No geral, verifica-se que as médias e grandes empresas são conhecedoras dos diversos riscos a que estão expostas e das eventuais implicações associadas. No entanto, serem conhecedoras não significa estarem adequadamente preparadas e, neste plano, existem entre as mesmas diferentes graus de preparação para enfrentarem os potenciais riscos a que estão sujeitas. Neste respeito, temos vindo a assistir ao longo dos últimos anos a uma crescente preocupação na adequação das infraestruturas de segurança das empresas e também a um reforço significativo

dos investimentos para mitigação dos riscos associados a ataques cibernéticos. As consequências que decorrem dos ataques cibernéticos estão dependentes do tipo de ataque propriamente dito, das vulnerabilidades que tenta explorar, e do grau de preparação e mitigação de riscos informáticos das instituições públicas que sejam, eventualmente, alvo destas ações. A forma de garantir a segurança dos produtos não é apenas por um mecanismo, mas sim de um conjunto de mecanismos, processos e recursos técnicos especializados. Neste último ponto, em particular, destacamos a importância da formação e sensibilização contínua em temas relacionados com a segurança, para as equipas de desenvolvimento, equipas de teste e qualidade, administradores dos produtos, mas também para os clientes/utilizadores finais. A segurança da informação deverá ser encarada como uma atitude transversal à organização que no limite deverá envolver todos os elementos da organização. Devemos ainda estar conscientes que os ataques realizados a sistemas de informação podem ser realizados através de recursos ou de pessoas (engenharia social) menos óbvios e que, nesse sentido, é necessário potenciar a incorporação de técnicas de “hardening” aplicacional, desde a fase embrionária de desenvolvimento dos produtos e soluções informáticas, para além de se testar continuamente a eficácia das medidas adotadas, garantir aplicação contínua de atualizações e, finalmente, realizar a monitorização regular de padrões e de desvios.