

# A importância das Parcerias Público-Privadas na proteção de infraestruturas críticas

 [dinheirovivo.pt/5905166344/a-importancia-das-parcerias-publico-privadas-na-protECAo-de-infraestruturas-criticas](https://dinheirovivo.pt/5905166344/a-importancia-das-parcerias-publico-privadas-na-protECAo-de-infraestruturas-criticas)

Infraestruturas e setores críticos - energia, transporte, telecomunicações, abastecimento de água, saúde, entre outros - são cada vez mais o alvo principal de ciberataques, ciberespionagem e operações de influência motivadas por ciberguerra. A maioria das infraestruturas críticas são operadas por entidades privadas, e mesmo que privados trabalhem para tornar essas infraestruturas mais seguras e resilientes, isso não pode acontecer sem a cooperação e apoio contínuos de autoridades públicas e do governo – órgão soberano. A colaboração entre governos e o setor privado (Parcerias Público-Privadas/PPP's) permite a criação de estratégias conjuntas de prevenção e resposta a ciberameaças, incluindo a partilha de inteligência, investimentos em tecnologia de segurança e o desenvolvimento de políticas de cibersegurança.

Numa primeira instância, estas parcerias podem garantir que as infraestruturas estejam em conformidade com as regulamentações de segurança e que haja uma coordenação eficaz em emergências. O setor privado, principalmente aquele que opera em setores regulamentados, já está familiarizado com os requisitos de cibersegurança e as melhores práticas para proteger dados confidenciais.

O setor privado desempenha também um papel central na resposta a incidentes e na deteção de ameaças em tempo real, pelo que a sua integração em PPP's fortalece as capacidades de defesa e torna a resposta a ciberataques mais rápida e eficiente. Uma vez que estas são as empresas que estão na linha da frente na deteção de intrusões, o seu trabalho é crucial para entender a origem e a natureza dos ciberataques, garantindo que a resposta a incidentes é coordenada e facilitadora de uma recuperação rápida e segura das operações.

Os privados tornam-se ainda grandes aliados em termos de expertise humana ao colmatar a escassez de recursos humanos especializados – especialmente, em áreas como a informática e a cibersegurança que estão frequentemente na vanguarda da inovação e dispõe de profissionais altamente qualificados para lidar com ameaças digitais complexas e dinâmicas. Ao estabelecer parcerias com empresas privadas, os governos podem ter acesso a essa expertise, beneficiando de soluções avançadas que muitas vezes não estão disponíveis ou são economicamente inviáveis no setor público. Sendo os privados ainda os principais fornecedores de serviços, o seu conhecimento prático deve ser tido em consideração nos processos de tomada de decisão estratégica.

Ciberataques bem-sucedidos frequentemente exploram lacunas de conhecimento entre diferentes entidades e quando os setores públicos e privados operam de forma isolada, as vulnerabilidades podem não ser identificadas a tempo. Uma parceria eficaz deve facilitar o fluxo de informações sobre ameaças emergentes, técnicas de ataque e melhores práticas de defesa. Contudo, faltam ainda meios, processos e confiança mútua

para possibilitar essa partilha de informações. A questão que se impõe é: como criar essa cultura e confiança de partilha? É importante criar incentivos de partilha de informações para o setor privado e estabelecer uma cultura de confiança com condições para que essa partilha aconteça sem repercussões. Além disso, faltam ainda centros de partilha para esse efeito, isto é, estruturas que sejam geridas num modelo 50-50, entre setor público e privado. Esta é uma responsabilidade partilhada e somente a formalização das PPP's e de Centros de Partilha poderá efetivamente criar condições para que se consiga trabalhar em conjunto na proteção de infraestruturas críticas.

Muitas empresas privadas – como a Microsoft, a Google e outros gigantes tecnológicos – têm estado na vanguarda da definição de normas e práticas seguras para a utilização do ciberespaço ao incentivar a criação de normas internacionais para a segurança digital, e ainda atuarem como intermediários em fóruns globais para promover o diálogo sobre proteção de dados e privacidade. Estas empresas influenciam a ciberdiplomacia, colaboram com governos e organizações internacionais para criar um ciberespaço mais seguro e transparente. A Microsoft, por exemplo, propôs a ideia da criação de uma “Convenção de Genebra Digital” para proteger os utilizadores civis contra ciberataques.

Dada a crescente complexidade e sofisticação dos ciberataques, uma colaboração estreita entre o setor público e privado é vital para combater a fragmentação em termos de responsabilidades e governança e, por sua vez, garantir a resiliência das infraestruturas que sustentam a sociedade digital.