CNCS
Centro Nacional de Cibersegurança PORTUGAL

COMUNICADO DE IMPRENSA



Exercício Nacional de Cibersegurança testa ecossistema dos Transportes

Ação de capacitação envolveu mais de 90 participantes de 20 entidades

Lisboa, dia 12 de junho, 2026 – Nos dias **10 e 11 de junho**, decorreu, em **Lisboa,** o Exercício Nacional de Cibersegurança (ExNCS´26) dedicado ao Ecossistema dos Transportes – Subsetores Aquático e Ferroviário**.** Esta edição integrou o exercício bianual pan-europeu — Cyber Europe, organizado em parceria com a ENISA - Agência da União Europeia para a Cibersegurança e restantes Estados-Membros. Durante os dois dias, as diferentes equipas envolvidas, analisaram e responderam a incidentes de cibersegurança e lidaram com situações de continuidade de negócio e gestão de crises, testando fluxos e processos de decisão e sua articulação com autoridades, comunicação social e outras partes interessadas.

"O objetivo não é que tudo bem, é sim, identificar o que precisamos de melhorar e o que corre menos bem, e perceber o que cada um de nós precisa de melhorar num cenário deste tipo", disse o coordenador do Centro Nacional de Cibersegurança, Lino Santos, na sua intervenção no arranque do **CyberEurope/ExNCS´26.**

Nesta edição da ação de treino participaram **30 Estados**, e em Portugal, foram mais de **90 participantes** e **20 entidades**, que tiveram de lidar com incidentes de cibersegurança de diversas tipologias, que se interconectaram, provocando o escalar de uma crise de larga escala e geraram **mais de 1 300 interações** ao longo dos dois dias.

Entidades participantes:

- Administração dos Portos do Douro, Leixões e Viana do Castelo (APDL)
- Administração do Porto de Lisboa (APL)
- Administração dos Portos de Setúbal e Sesimbra (APSS)
- Administração dos Portos da região Autónoma da Madeira (APRAM)
- Administração dos Portos dos Açores
- YILPORT
- Infrestruturas de Portugal (IP)

Rua da Junqueira, 69, 1300-342, Lisboa • Tel (+351) 210 497 400 • cncs@cncs.gov.pt

- Comboios de Portugal (CP)
- Fertagus
- Captrain Portugal
- Medway
- Instituto da Mobilidade e dos Transportes Terrestres (IMT)
- Direção-Geral de Recursos Naturais, Segurança e Serviços Marítimos (DGRM)
- Sistema de Segurança Interna (SSI)
- Centro Nacional de Cibersegurança (CNCS)
- Polícia Judiciária (PJ)
- Serviço de Informações Estratégicas de Defesa (SIED)
- Serviço de Informações de Segurança (SIS)
- Comando de Operações de Ciberdefesa (COCiber)
- LUSA – Agência de Notícias

Para José Carlos Gonçalves, CISO da Infraestruturas de Portugal, a participação desta entidade no Exercício Nacional de Cibersegurança, "evidenciou o papel crítico destes exercícios na validação das capacidades de resposta da IP, permitindo testar, em ambiente simulado, cenários complexos com impacto em infraestruturas críticas". Durante o exercício foram avaliadas situações concretas, como ataques a sistemas operacionais e serviços essenciais (ex. incidentes simulados e comprometimento de sistemas de informação). Para este participante, esta iniciativa reforçou a coordenação da IP com o CNCS e outras entidades, "contribuindo para a melhoria contínua dos processos, da articulação interinstitucional e do nível de preparação face a ameaças emergentes."

Hugo Bastos, Diretor de Sistemas de Informação da APDL – Administração dos Portos do Douro, Leixões e Viana do Castelo, considera que a participação desta autoridade portuária, que gere infraestruturas críticas e assegura a articulação de múltiplos intervenientes da comunidade portuária, em exercícios de simulação de *tabletop* e *roleplay,* assume um papel estratégico no reforço da preparação para incidentes de cibersegurança. Para o dirigente, "o atual contexto de crescente digitalização das operações marítimas e logísticas, que amplia a superfície de exposição a ameaças, estes exercícios são fundamentais para testar a capacidade de resposta, melhorar a tomada de decisão e reforçar a resiliência operacional (...) e proporcionou uma experiência de cooperação e aprendizagem conjunta de elevado valor, permitindo fortalecer mecanismos de coordenação interinstitucional e de resposta a cenários complexos que dificilmente seriam replicáveis num exercício individual e local".

O **CyberEurope/ExNCS´26**, concebido para testar e criar bases de análise crítica baseou-se num conjunto de 4 cenários distintos que decorreram em simultâneo. No **subsetor Aquático**, a audiência de treino foi confrontada com perturbações, significativas, dos sistemas e processos operacionais, que comprometeram a gestão das operações e afetaram a normal circulação de navios, de mercadorias e serviços associados.

Já no **subsetor ferroviário**, o cenário contemplou a ocorrência de incidentes com impacto na operação das linhas ferroviárias e nos sistemas de suporte ao serviço, incluindo plataformas de bilhética e de informação ao passageiro. Estas perturbações originaram constrangimentos operacionais, atrasos e dificuldades na prestação regular dos serviços de transporte.

Em paralelo, foram simulados incidentes dirigidos à autoridade do setor dos transportes, que afetaram a sua capacidade de atuação e credibilidade.

Principais indicadores da avaliação preliminar:

Maturidade organizacional

Os resultados do Cyber Europe 2026 apontam para um nível de maturidade organizacional relevante por parte das entidades participantes. De uma forma geral, verificou-se a ativação dos procedimentos internos previstos, a mobilização das equipas adequadas e uma resposta estruturada aos diferentes incidentes de

cibersegurança simulados. De realçar que o exercício permitiu, igualmente, identificar oportunidades de melhoria em alguns fluxos operacionais e de reporte de incidentes às autoridades, reforçando a importância de continuar a exercitar e a aperfeiçoar estes mecanismos.

Funcionamento da cadeia de confiança

O exercício demonstrou a importância da cadeia de confiança entre as entidades dos subsetores ferroviário e aquático. Nos cenários que envolveram interdependências entre organizações, verificou-se uma articulação próxima e uma partilha de informação eficaz, suportadas por contactos já estabelecidos e por relações consolidadas. No subsetor aquático destacou-se, particularmente, a colaboração entre entidades desde os primeiros momentos do exercício, refletindo o trabalho desenvolvido pelo ISAC Portos PT, Comunidade de Cibersegurança que tem vindo a criar relações de proximidade e confiança entre os seus membros. Esta experiência reforça a importância das Comunidades de Cibersegurança dinamizadas pelo CNCS, que constitui um dos fatores que sustenta a criação do ISAC Transportes Terrestres PT.

Escalada da crise e articulação institucional

Tratando-se quatro cenários, com elevado grau de complexidade, a decorrer em simultâneo e uma evolução progressiva de anomalia para incidente de larga escala, observou-se uma forte articulação institucional ao longo de todo o exercício. Verificou-se uma partilha regular de informação entre as autoridades e forças de segurança presentes no exercício, bem como a ativação do Gabinete de Crise de Cibersegurança em diversos momentos, acompanhando a evolução da situação e apoiando a tomada de decisão estratégica. De forma geral, os mecanismos de escalada e coordenação funcionaram em linha com o que estava inicialmente previsto para o **Cyber Europe 2026**.

Para mais informações:
Clara Santos Silva
Comunicação e Imagem
Centro Nacional de Cibersegurança
Tlm: +351 919 592 662
comunicacao@cncs.gov.pt