A Segurança na Crise Energética e as Dependências entre Estados

Infraestruturas Criticas – Estratégias, Abordagem e Desafios

Lisboa, 1 de junho de 2026

PRINCIPAIS DESAFIOS DE SEGURANÇA ENFRENTADOS

A Europa e Portugal enfrentam ameaças crescentes

Ameaças híbridas

Combinação de diferentes vetores de ataque, incluindo desinformação, sabotagem e pressão económica, por vezes promovidas por atores estatais.

Dependência energética e tecnológica

Elevada exposição a choques externos, incluindo a autonomias estratégicas e fragilidade das cadeias de abastecimento.

Cibersegurança

As infraestruturas críticas (energia, transportes, comunicações, saúde) são alvos preferenciais de ataques cibernéticos.

Alterações Climáticas

Eventos climáticos extremos, impactam diretamente a resiliência das infraestruturas e exigem adaptações urgentes.

A **Diretiva CER (UE) 2022/2557** surge como resposta a estes desafios, reconhecendo que a proteção de ativos individuais já não é suficiente, propondo uma abordagem mais integrada e coordenada para garantir a **resiliência das entidades críticas** (que prestam serviços essenciais ao normal funcionamento da sociedade)

COMO CONTRIBUIR PARA UMA EUROPA MAIS RESILIENTE

Diversificar as fontes de fornecimentos estratégicos
Reduzir dependências externas, especialmente em setores como energia e tecnologias emergentes.

Investimento em ciberdefesa e segurança digital
Reforçar a proteção das redes críticas e apoiar a capacitação das entidades para assegurar a implementação das medidas adequadas.

Cooperação europeia e partilha de informação
Fortalecer os mecanismos existentes, para assegurar a manutenção de uma permanente partilha e articulação e entre operadores de serviços essenciais.

Capacitação e formação
Melhorar o desenvolvimento de competências técnicas e estratégicas em segurança, continuidade do negócio e gestão de crises.

A **Diretiva CER (UE) 2022/2557**
(**Decreto-Lei n.º 22/2025, de 19 de março)**
estabelece obrigações claras para os Estados-Membros:

- Avaliação nacional de riscos;
- Estratégia Nacional para a Resiliência das Entidades Críticas;
- Identificação e designação de entidades críticas.

VULNERABILIDADES E OPORTUNIDADES

Infraestruturas "envelhecidas" e com **necessidades de financiamentos significativos** para aumentar a sua resiliência;

Interdependências crescentes entre setores (energia, comunicações, transportes, digital);

Dependência extrema dos **Sistemas Lógicos** e elevada **exposição cibernética;**

Limitações nas **redundâncias e interconectividade** entre redes e serviços críticos;

Exposição a riscos naturais e tecnológicos

Transição energética e digital **como motor de modernização;**

Desenvolvimento de **infraestruturas resilientes e sustentáveis;**

Financiamento europeu para digitalização, inovação e resiliência;

Criação de **centros de competência nacionais** para apoio ao desenvolvimento das necessidades das entidades críticas.

Investimentos no quadro de reforço em Security**, no âmbito da EU e das obrigações NATO**

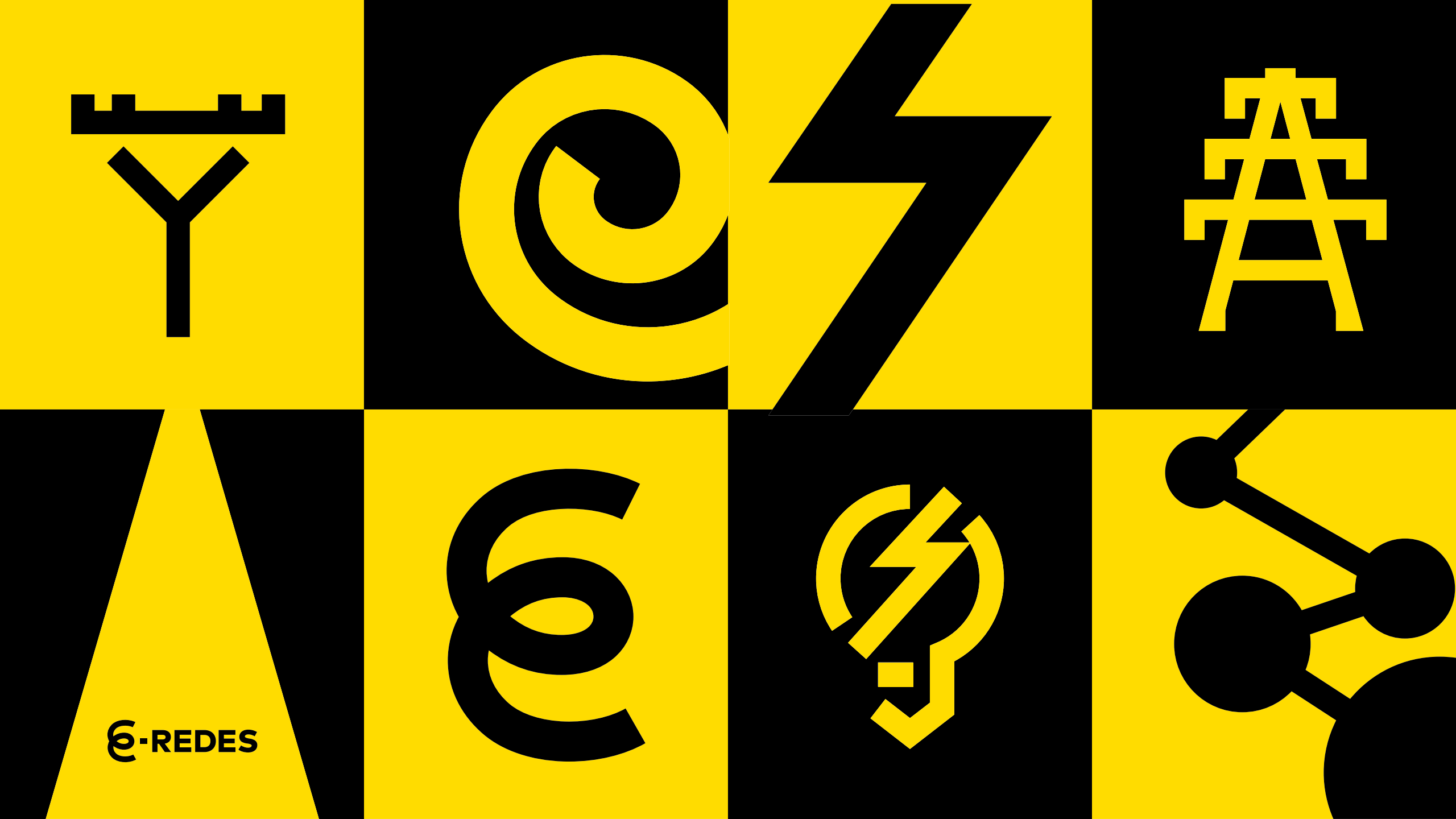
FOMENTAR O DIÁLOGO ENTRE AUTORIDADES, OPERADORES E SOCIEDADE CIVIL SOBRE INFRAESTRUTURAS CRÍTICAS!

- **Fóruns intersetoriais** para partilha de boas práticas;
- **Investigação aplicada** sobre interdependências e riscos emergentes;
- **Transparência e comunicação dos Riscos**
- **Formação contínua** para profissionais dos setores críticos, e autoridades com atribuições e responsabilidades na regulação;
- **Exercícios e Simulações de Crise,** entre diferentes setores de serviços essenciais.

Obrigado pela vossa atenção

paulo.alberto@e-redes.pt

E-REDES
Distribuição de Eletricidade


E-REDES