

Como comunicar incidentes e vulnerabilidades ativamente exploradas através da Plataforma Única de Comunicação (SRP)

Ficha informativa em português, adaptada a partir do factsheet original da ENISA sobre o Cyber Resilience Act (CRA)

O QUE É

A partir de 11 de setembro de 2026, o CRA obriga fabricantes a comunicar vulnerabilidades ativamente exploradas e incidentes graves que afetem produtos com elementos digitais vendidos na UE. Responsáveis por software de código aberto (OSS) têm a mesma obrigação, na medida em que participem no desenvolvimento desses produtos.

PARA QUEM

Fabricantes de produtos com elementos digitais e responsáveis (stewards) de projetos de software de código aberto envolvidos no seu desenvolvimento, que coloquem esses produtos no mercado da União Europeia.

A **Single Reporting Platform (SRP)** é a ferramenta eletrónica criada pela ENISA para cumprir esta obrigação com uma única submissão. Em vez de contactar separadamente cada autoridade nacional, a entidade reporta uma vez e a plataforma encarrega-se de distribuir a informação a todos os destinatários relevantes, com medidas de segurança para proteger a confidencialidade dos dados.

O que tem de comunicar

Vulnerabilidades ativamente exploradas

- Falhas em produtos com elementos digitais que se saiba estarem, no momento, a ser exploradas por um agente malicioso (artigo 3.º, n.º 42, do CRA).

Incidentes graves

- Incidentes com impacto grave na segurança do produto — comprometendo disponibilidade, autenticidade, integridade ou confidencialidade — nos termos do artigo 3.º, n.º 44; os critérios de gravidade constam do artigo 14.º, n.º 5.

Os três prazos a cumprir

24h

Alerta precoce

A partir do momento em que toma conhecimento da vulnerabilidade ou incidente.

72h

Notificação

Informação geral e uma avaliação inicial do caso.

F

Relatório final

Vulnerabilidades: até 14 dias após haver correção disponível.
Incidentes graves: até 1 mês após a notificação das 72 horas.

A quem reportar

A entidade nacional a quem deve reportar através da SRP é determinada, em regra, pelo **local principal de estabelecimento** da organização — o artigo 14.º, n.º 7, do CRA detalha como identificar o CSIRT nacional competente. Uma única submissão é depois encaminhada automaticamente para o CSIRT nacional que a recebe, para os CSIRT de outros Estados-membros onde o produto esteja também disponível, e para a ENISA.

PT Em Portugal — as entidades abrangidas pelo Regime Jurídico da Cibersegurança (Decreto-Lei n.º 125/2025) já se relacionam com o Centro Nacional de Cibersegurança (CNCS) para efeitos de identificação, registo e comunicação de incidentes. Consulte o CNCS para confirmar o procedimento de acesso à SRP a partir de Portugal.

Como funciona a submissão

1**Iniciar sessão na plataforma****2****Selecionar o CSIRT nacional****3****Preencher os dados e submeter**

Após a submissão, o CSIRT que recebe a notificação partilha-a sem demora com os restantes CSIRT relevantes da UE onde o produto também esteja disponível, e a ENISA recebe a informação em simultâneo. Alguns dados são ainda partilhados com as autoridades de fiscalização de mercado, para que possam cumprir as suas funções. Em circunstâncias excecionais, a divulgação da informação pode ser diferida, nos termos do artigo 16.º, n.º 2, do CRA e do Regulamento Delegado (UE) 2026/881.

Nota de proveniência: este documento é uma adaptação em português, produzida pela Cibersegurança.PT, do factsheet oficial "How to Report Incidents and Actively Exploited Vulnerabilities via the Single Reporting Platform (SRP)", publicado pela Agência da União Europeia para a Cibersegurança (ENISA). O conteúdo foi reescrito e reorganizado para leitura em português, com enquadramento adicional para o contexto português; não substitui o documento original nem a informação legal vinculativa da ENISA e da Comissão Europeia.

Documento original (inglês): [enisa.europa.eu — ENISA CRA SRP Factsheet v1.0.0 \(PDF\)](https://enisa.europa.eu/enisa-cra-srp-factsheet-v1.0.0)

Mais informação: enisa.europa.eu/topics/product-security/single-reporting-platform-srp · Apoio: cra-srp-helpdesk@enisa.europa.eu