BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

AGOSTO 2023 | nº 3/2023

DESTAQUES

Estratégia

A construção de uma estratégia de ação para os setores público e privado compreende a definição de objetivos, a análise de um contexto, o planeamento de recursos, a escolha das ações consideradas adequadas e a apresentação de uma visão de futuro e resultados esperados. O setor público em particular realça partes interessadas específicas, como o cidadão e a política, e implica a definição de prioridades com vista ao bem comum (Joyce 2015).

Cibersegurança

De modo a implementar boas práticas de cibersegurança na sociedade, desenvolveu-se uma dinâmica de criação de Estratégias Nacionais que promovem políticas públicas para a segurança, a defesa e a resiliência do ciberespaço, bem como a literacia digital dos cidadãos. A União Europeia (UE) tem estimulado a aplicação deste tipo de instrumento, nomeadamente através das Diretivas no âmbito da cibersegurança, como a Diretiva 2022/2555 (vulgo NIS 2).

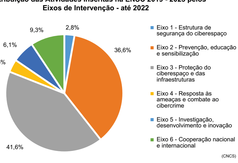
Portugal

Desde 2015 que Portugal tem uma Estratégia Nacional de Segurança do Ciberespaço (ENSC). A primeira ENSC vigorou entre 2015 e 2019, a que se seguiu a atual ENSC, que engloba os anos entre 2019 e 2023. Com o aproximar de 2024, encontra-se em desenvolvimento a próxima ENSC, processo realizado no âmbito do Conselho Superior de Segurança do Ciberespaço, sob coordenação do CNCS e com o contributo de partes interessadas da sociedade civil.

PANORÂMICA

- A atual ENSC assenta em 3 objetivos estratégicos: "maximizar a resiliência, promover a inovação e gerar e garantir recursos". Em 2019, preconizava-se para o futuro "um país mais seguro e próspero, através de uma ação inovadora, inclusiva e resiliente".
- Estes objetivos foram detalhados em 6 eixos de intervenção (ver gráfico). O Plano de Ação, até ao final de 2022, abrangeu 126 entidades, sobretudo da Administração Pública, na inscrição de atividades a desenvolver e concretizar até 2023.
- Estas entidades inscreveram 1467 atividades. O eixo de intervenção com mais atividades inscritas foi o "3 – Proteção do ciberespaço e das infraestruturas" (41,6% das atividades), a que se seguiu o "2 – Prevenção, educação e sensibilização" (36,6%).

Distribuição das Atividades Inscritas na ENSC 2019 - 2023 pelos Eixos de Intervenção - até 2022



- Ao fim de 4 anos, há indicadores positivos na cooperação institucional, na aplicação de boas práticas e na criação de formações. Todavia, as ameaças são mais sofisticadas, há ainda falta de recursos humanos e persistem insuficiências na inovação em cibersegurança (ver relatórios do Observatório de Cibersegurança).
- No National Cyber Security Index, índice da capacidade dos países para prevenir e gerir incidentes de cibersegurança, com base em políticas públicas, Portugal, a nível mundial, evoluiu do 16º lugar em 2019 (com 64% de pontuação) para 8º em 2023 (com 90%).

PERSPETIVA

1 A Diretiva 2022/2555 da UE define as Estratégias Nacionais na área da cibersegurança como "um quadro coerente mediante o qual um Estado-Membro define prioridades e objetivos estratégicos no domínio da cibersegurança e define a governação com vista à sua consecução no Estado-Membro em causa". Destacam-se, portanto, 2 elementos: a) a definição de propósitos considerados importantes; e b) a indicação do modo através do qual estes devem ser atingidos.

2 Um plano definido no âmbito de uma estratégia pode remeter apenas para um conjunto de objetivos ou acrescentar as instruções sobre como atingir esses objetivos. A integração de instruções permite, por um lado, tornar mais objetivas as ações a realizar, mas, por outro, define em demasia tarefas que podem ter de ser alteradas devido à incerteza dos contextos (Suchman 2012). A revisão regular das instruções ajuda a mitigar os efeitos da imprevisibilidade.

3 A Agência da União Europeia para a Cibersegurança (ENISA) elaborou alguns documentos de apoio aos Estados-Membros nas suas Estratégias Nacionais. Além de disponibilizar indicadores de performance, em *National Capabilities Assessment Framework*, a ENISA faz recomendações quanto aos modelos de governação para a implementação destas Estratégias, no *Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies*.

4 Entre os 27 Estados-Membros da UE, 9 encontram-se na sua terceira Estratégia Nacional; 14, na segunda (em que se inclui Portugal); e 4, na primeira (ENISA 2023a). Para avaliar o nível de maturidade de execução destas Estratégias Nacionais e dos países na área da cibersegurança, a ENISA propõe indicadores distribuídos por 4 *clusters*: governação e *standards*; desenvolvimento de capacidades e sensibilização; dimensão legal e regulatória; e cooperação (ENISA 2023b).

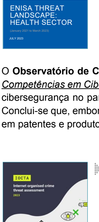
5 Com vista à aquisição de uma elevada maturidade e à efetiva implementação destas Estratégias Nacionais, a ENISA recomenda uma governação estratégica que coordene a definição do conteúdo da Estratégia e a mitigação de riscos; uma prática que assegure a tradução dos objetivos em ações; uma esfera técnica que indique normas e tecnologias; e um domínio de políticas que garanta a disponibilização de quadros de ação e a transparência dos processos (ENISA 2023a).

6 Em Portugal, o desenvolvimento da próxima ENSC encontra-se na fase de recolha de contributos, adotando-se uma metodologia de criação de políticas públicas aberta à comunidade e à participação das partes interessadas dos setores público e privado. Partindo-se de uma análise à situação atual quanto a ameaças e capacidades do país, pretende-se identificar objetivos claros e indicar um conjunto de tarefas-chave com vista a melhorar a cibersegurança nacional.

PUBLICAÇÕES E NOTÍCIAS

A **Direção-Geral de Estatísticas da Educação e Ciência (DGEEC)**, no dia 6 de junho, publicou os resultados anuais do *IUTIC - Inquérito à Utilização das Tecnologias da Informação e Comunicação na Administração Pública Central, Regional e nas Câmaras Municipais*. Um dos destaques é que 63% dos Organismos da Administração Central e 60% das Câmaras Municipais indicaram ter definida uma estratégia para a segurança de informação em 2022.

A **ENISA**, no dia 13 de junho, partilhou o documento *Good Practices for Supply Chain Cybersecurity*, no qual apresenta os resultados de um estudo e algumas recomendações quanto à cibersegurança nas cadeias de abastecimento, tendo em conta as exigências da Diretiva 2022/2555 da UE para as entidades essenciais e importantes. Uma das recomendações é que se adote uma abordagem baseada na gestão de riscos de terceiros, considerando os fornecedores relevantes.



A **ENISA**, no dia 5 de julho, lançou o relatório *Health Threat Landscape*, o primeiro estudo desta organização sobre o quadro de ameaças que afeta o setor da saúde em particular, de modo a disponibilizar uma visão mais profunda sobre esta área e suportar as análises de risco. Entre as várias conclusões, destaca-se a chamada de atenção para a necessidade de combater as vulnerabilidades técnicas nos dispositivos médicos, cada vez mais conectados à Internet.

O **Observatório de Cibersegurança do CNCS**, no dia 13 de julho, publicou o *Estudo Sobre a Comunidade de Competências em Cibersegurança*, onde disponibiliza informação sobre a atual comunidade de competências em cibersegurança no país, nomeadamente os conhecimentos, atividades, processos, tecnologias e investigações. Conclui-se que, embora haja algum dinamismo na investigação em cibersegurança, esta ainda se converte pouco em patentes e produtos.

A **Europol**, no dia 17 de julho, publicou o *Internet Organised Crime Threat Assessment (IOCTA) 2023*, através do qual faz uma análise das tendências no cibercrime na UE. Esta edição salienta a importância da guerra na Ucrânia na configuração das ameaças no ciberespaço de interesse da UE, nomeadamente no aumento dos ataques de DDoS realizados por grupos pró-Rússia motivados politicamente e no uso deste tema como narrativa para a realização de fraudes *online*.

A **Equipa Europa** (Team Europe), no dia 5 de agosto, venceu pela segunda vez consecutiva o International Cybersecurity Challenge, que se encontra na sua segunda edição. Este ano o evento decorreu nos EUA, em San Diego, colocando frente-a-frente equipas dos vários continentes em resposta a desafios de cibersegurança. Em segundo lugar ficou a equipa da Oceânia e em terceiro a da Ásia. A Equipa Europa destacou-se nos desafios de Capture the Flag.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança