Estratégia Nacional de Segurança do Ciberespaço 2019-2023

6 de junho de 2019

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

ÍNDICE

REOLUÇÃO DE CONSELHO DE MINISTROS N.º 92/2019 2

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019-2023 6

1- VALORES, DEFINIÇÕES E PRINCÍPIOS 7
2- ANÁLISE DA ENVOLVENTE 8
3- VISÃO 11
4- OBJETIVOS ESTRATÉGICOS 11
5- EIXOS 11
6 - AVALIAÇÃO E REVISÃO DA ESTRATÉGIA 23

Resolução de Conselho de Ministros N.º 92/2019

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Resolução do Conselho de Ministros n.º 92/2019

A Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, aprovou a primeira Estratégia Nacional de Segurança do Ciberespaço, visando aprofundar a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço, por parte de todos os cidadãos e das entidades públicas e privadas. Face ao rápido desenvolvimento intrínseco ao ciberespaço e, consequentemente, à crescente evolução das ameaças, das vulnerabilidades, dos processos e das infraestruturas, bem como dos modelos económicos, sociais e culturais que assentam na sua utilização, ficou definido que a referida estratégia seria objeto de revisão num prazo de três anos.

Através da Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto, foi constituído um grupo de projeto, denominado Conselho Superior de Segurança do Ciberespaço, que teve como um dos seus objetivos propor a revisão e elaborar a nova Estratégia Nacional de Segurança do Ciberespaço (ENSC). No âmbito deste grupo de projeto, foi elaborado um anteprojeto que constituiu a base da nova ENSC que agora se aprova.

Por seu turno, a Lei n.º 46/2018, de 13 de agosto, veio estabelecer o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União. Através dessa lei, foi instituído o Conselho Superior de Segurança do Ciberespaço, enquanto órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço.

O Conselho Superior de Segurança do Ciberespaço tem como competências, nomeadamente, verificar a implementação da ENSC, através do acompanhamento e avaliação da respetiva execução, devendo, ademais, ser ouvido, nos termos do n.º 2 do artigo 4.º da Lei n.º 46/2018, de 13 de agosto, no âmbito do processo de aprovação da ENSC.

O projeto de ENSC 2019-2023 foi objeto de parecer favorável do Conselho Superior de Segurança do Ciberespaço, nos termos da alínea c) do n.º 1 do artigo 6.º da Lei n.º 46/2018, de 13 de agosto.

Assim, tendo em consideração a evolução digital ocorrida desde a aprovação da ENSC de 2015, estão reunidas as condições para aprovar a ENSC 2019-2023, enquanto instrumento estruturante para a capacitação nacional neste âmbito, definindo o enquadramento, os

objetivos e as linhas de ação do Estado em matéria de segurança do ciberespaço, de acordo com o interesse nacional.

A ENSC 2019-2023 assenta em três objetivos estratégicos: maximizar a resiliência, promover a inovação e gerar e garantir recursos. As implicações e necessidades associadas a cada um dos objetivos estratégicos permitem definir uma orientação geral e específica, traduzida em seis eixos de intervenção, que enformam linhas de ação concretas destinadas a reforçar o potencial estratégico nacional no ciberespaço.

A consecução da ENSC 2019-2023 permitirá tornar Portugal um país mais seguro e próspero, através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade.

Determina-se ainda a elaboração, no prazo de 120 dias, de um Plano de Ação da ENSC 2019-2023, que se afigura um instrumento essencial de acompanhamento e avaliação da respetiva execução e que deve ser articulado com a Estratégia Nacional de Combate ao Terrorismo, designadamente contemplando medidas de proteção contra as respetivas ameaças à segurança do ciberespaço, com a Estratégia TIC 2020 - Estratégia para a Transformação Digital na Administração Pública, bem como com a Estratégia de Inovação Tecnológica e Empresarial para Portugal 2018-2030.

Assim:

Ao abrigo do n.º 2 do artigo 4.º da Lei n.º 46/2018, de 13 de agosto, e nos termos das alíneas d), f) e g) do artigo 199.º e da alínea a) do n.º 1 do artigo 200.º da Constituição, o Conselho de Ministros resolve:

1 - Aprovar a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, que consta do anexo à presente resolução e da qual constitui parte integrante.

2 - Determinar a elaboração de um Plano de Ação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, a aprovar no prazo de cento e vinte dias após a entrada em vigor da presente resolução.

3 - Cometer ao Centro Nacional de Cibersegurança, enquanto Autoridade Nacional de Cibersegurança, a coordenação da elaboração, o acompanhamento da execução e a revisão do Plano de Ação referido no número anterior, em articulação e estreita cooperação com todas as entidades com responsabilidade no âmbito da segurança do ciberespaço.

4 - Determinar que o coordenador do Centro Nacional de Cibersegurança deve auscultar o Conselho Superior de Segurança do Ciberespaço sobre o Plano de Ação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 previamente à respetiva aprovação pelo membro do Governo responsável pela área da cibersegurança.

5 - Determinar que a assunção de compromissos para a execução da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 depende da existência de fundos disponíveis por parte das entidades públicas competentes.

6 - Determinar a revisão, com periodicidade anual ou sempre que necessário, do Plano de Ação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023.

7 - Revogar a Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho.

8 - Determinar que a presente resolução entra em vigor no dia seguinte ao da sua publicação.

Presidência do Conselho de Ministros, 23 de maio de 2019. - O Primeiro-Ministro, António Luís Santos da Costa.

Estratégia Nacional de Segurança do Ciberespaço

2019-2023

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

1- Valores, definições e princípios

A Estratégia Nacional de Segurança do Ciberespaço 2019-2023, doravante designada por Estratégia, funda-se no compromisso de aprofundar a segurança das redes e sistemas de informação, como forma de garantir a proteção e defesa do ciberespaço de interesse nacional e potenciar uma utilização livre, segura e eficiente do mesmo por parte de todos os cidadãos, das empresas e das demais entidades públicas e privadas.

Para uma eficaz apreensão da presente Estratégia, afigura-se necessária a explanação de alguns dos conceitos mais relevantes neste âmbito, permitindo concomitantemente a constituição de uma base conceptual que possa ser utilizada por todos.

Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.

Cibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.

Ciberdefesa consiste na atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço.

Por cibercrime entendem-se os factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa.

Uma vez apresentada a base conceptual, cumpre mencionar que a presente Estratégia assenta no direito vigente que regula as relações internacionais soberanas, designadamente na Carta das Nações Unidas e no Direito Internacional Humanitário, e bem assim nas convenções internacionais que regulam a proteção pelos Estados dos direitos e liberdades fundamentais, nomeadamente a Declaração Universal e o Pacto dos Direitos Civis e Políticos, e no direito europeu correspondente, como a Convenção Europeia dos Direitos Humanos e a Carta dos Direitos Fundamentais da União Europeia. Assenta ainda nos princípios gerais da soberania do Estado, na proteção da liberdade de expressão, dos dados pessoais e da privacidade, nas linhas gerais da Estratégia da União Europeia para a Cibersegurança, bem como na política de ciberdefesa da Organização do Tratado do Atlântico Norte e nos compromissos assumidos tendo

em vista a resiliência e a capacidade de resposta rápida e efetiva a ciberataques. Assim, a presente Estratégia alicerça-se nos seguintes princípios:

Princípio da subsidiariedade:

Portugal afirma o seu forte compromisso com a segurança do ciberespaço. Considerando que grande parte das infraestruturas tecnológicas que compõem o ciberespaço é detida por entidades do setor privado, cabe a estas a responsabilidade primária pela sua proteção. Esta responsabilidade inicia-se no próprio indivíduo, pela forma responsável como utiliza o ciberespaço, e termina no Estado, enquanto garante da soberania e dos princípios constitucionais.

Princípio da complementaridade:

A segurança do ciberespaço é uma responsabilidade partilhada entre os diferentes atores, sejam eles públicos ou privados, coletivos ou individuais. Uma abordagem inclusiva, alargada e integradora da segurança do ciberespaço exige diferentes responsabilidades e capacidades, para benefício do interesse comum.

A interdependência das infraestruturas tecnológicas, e a consequente probabilidade de propagação dos impactos resultantes de incidentes, requer uma atuação complementar e confiável, assente na consciência do dever de cooperação reforçado entre as estruturas e entidades nacionais, atentas às referidas dependências por forma a maximizar a proteção e a resiliência digital.

Princípio da proporcionalidade:

A segurança do ciberespaço resulta também de um exercício complexo, verificável e contínuo, de avaliação dos riscos associados ao ecossistema digital. Em consequência, a adequação e a alocação de recursos deve ser proporcional aos riscos identificados e à execução das linhas de ação constantes da presente Estratégia.

2- Análise da envolvente

Quando a primeira Estratégia Nacional de Segurança do Ciberespaço foi aprovada, em 2015, a emergência tecnológica e o seu impacto na nossa sociedade já eram evidentes.

A tendência para um crescente aumento da dependência das tecnologias de informação e de comunicação e o surgimento de novos fenómenos com impacto direto no desenvolvimento

social trouxeram, de igual modo, em sociedades conectadas como a nossa, oportunidades significativas para aqueles que pretendem comprometer as nossas redes e sistemas de informação com intuitos potencialmente perniciosos para o bem-estar da sociedade portuguesa.

Num ambiente estratégico, em que o panorama geopolítico se apresenta em constante mutação, as ameaças no ciberespaço de interesse nacional provêm de diversos agentes e assumem diferentes tipologias e motivações.

As ameaças com origem em agentes estatais, das quais avultam os riscos crescentes de extensão aos conflitos armados, decorrem da motivação política, militar e económica com que estes intervenientes procuram, a coberto do anonimato conferido pelo ciberespaço, alcançar os seus objetivos estratégicos por meio de operações de ciberespionagem, de ações de ingerência e de desinformação em ambiente digital, incluindo ações de cibersabotagem destinadas a atingir infraestruturas críticas e a provocar a disrupção de serviços essenciais para o regular funcionamento da sociedade.

Por outro lado, as ameaças provenientes de agentes não estatais são frequentemente de origem criminosa, de móbil pecuniário, embora também se verifiquem ações com motivação política e ideológica, bem como outras para denegrir imagens institucionais e diminuir a reputação dos alvos.

Explorando de forma maciça a utilização de malware (ou «código malicioso»), as ferramentas de anonimização de identidade e o caráter transnacional do ciberespaço, as estruturas organizadas do cibercrime estão cada vez mais presentes no panorama criminal, não só de forma direta mas também colocando as suas capacidades técnicas ao serviço de estruturas criminosas tradicionais.

Também os alvos tradicionais do cibercrime têm vindo a expandir-se com a massificação dos métodos de ransomware e de meios de pagamento que permitem transações financeiras em aparente anonimato. De igual modo, o incremento de dispositivos conectados na Internet, conhecidos por Internet-of-Things, poderá contribuir para um aumento dos vetores de ataque à disposição das estruturas organizadas do cibercrime.

No que diz respeito ao terrorismo e respetivas atividades de suporte, alguns dos mais frequentes e visíveis usos ofensivos das tecnologias de informação e comunicação por organizações e indivíduos associados ao terrorismo incluem, designadamente, ações visando a alteração não

autorizada de conteúdos de sítios na Internet nacionais e a exfiltração e divulgação pública de informação ou de dados pessoais sem consentimento do respetivo titular com aquele propósito.

Finalmente e ainda que os fenómenos da radicalização e mobilização ativas não se restrinjam à vertente online, cumpre referir o impacto dos serviços e redes sociais e das plataformas de comunicação instantânea sobre aqueles fenómenos e ainda, de forma geral, sobre o fenómeno da distribuição de propaganda ou conteúdos apologéticos das principais organizações terroristas. Com efeito, os serviços online de comunicação permitem um contacto quase permanente entre radicalizados e radicalizadores, independentemente da geografia, bem como a disseminação e saturação de conteúdos propagandísticos e radicalizantes nos referidos serviços e plataformas.

Relativamente ao ativismo no ciberespaço (hacktivismo), fenómeno com aparente motivação política ou ao serviço de uma causa, que se traduz, na generalidade dos casos, na aplicação de métodos de disrupção de sistemas, de exfiltração e de divulgação pública massiva de dados de indivíduos, persiste um potencial adormecido de agentes de ameaça com as capacidades especializadas adequadas à execução de atos de grande disrupção de redes e sistemas de informação.

A multiplicação de recursos de aprendizagem disponíveis e de ferramentas de fácil utilização tem incrementado o número dos ataques dolosos contra redes e sistemas de informação por parte dos mais diversos atores. Muitos dos agentes de ameaça supramencionados encontram no ciberespaço palco de atuação, facilitado por um conjunto de vulnerabilidades de que este padece.

A identificação destas vulnerabilidades, associada à fraca cultura de cibersegurança e de consciência das responsabilidades individuais neste domínio, bem como à insuficiente maturidade digital para atender às necessidades de segurança, patentes tanto no setor público como no setor privado, apresentam-se como as principais fragilidades que urge resolver.

A par desta realidade, a dificuldade de capacitação, manutenção e captação de recursos humanos e financeiros que permitam o acompanhamento da rápida evolução tecnológica e o concomitante impacto na vida em sociedade representa uma vulnerabilidade nacional adicional, que exige um forte investimento para ser colmatada, modelos de colaboração inovadores em rede e um incremento da investigação, desenvolvimento e inovação.

Impõe-se ainda o reforço da articulação ao nível da coordenação e da cooperação estratégica e operacional de entidades nacionais envolvidas na segurança do ciberespaço por forma a salvaguardar uma eficiente e eficaz gestão nacional de crises.

3- Visão

A presente Estratégia estabelece a seguinte visão para 2023:

Que Portugal seja um país seguro e próspero através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade.

4- Objetivos Estratégicos

Objetivo estratégico 1 - Maximizar a resiliência:

Fortalecer e garantir a resiliência digital nacional potenciando a inclusão e a colaboração em rede de forma a salvaguardar a segurança do ciberespaço de interesse nacional face às ameaças que possam comprometer ou provocar a disrupção das redes e sistemas de informação essenciais à sociedade.

Objetivo estratégico 2 - Promover a inovação:

Fomentar e potenciar a capacidade nacional de inovação afirmando o ciberespaço como um domínio de desenvolvimento económico, social, cultural e de prosperidade.

Objetivo estratégico 3 - Gerar e garantir recursos:

Contribuir para obter e garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço.

5- Eixos

As implicações e necessidades associadas a cada um dos objetivos estratégicos permitem definir uma orientação geral e específica, traduzida em seis eixos de intervenção, que enformam linhas

de ação concretas destinadas a reforçar o potencial estratégico nacional no ciberespaço através do incremento da sua segurança, a saber:

Eixo 1 - Estrutura de segurança do ciberespaço;

Eixo 2 - Prevenção, educação e sensibilização;

Eixo 3 - Proteção do ciberespaço e das infraestruturas;

Eixo 4 - Resposta às ameaças e combate ao cibercrime;

Eixo 5 - Investigação, desenvolvimento e inovação;

Eixo 6 - Cooperação nacional e internacional.

Eixo 1 – Estrutura de segurança do ciberespaço:

A complexidade e a abrangência dos desafios da segurança do ciberespaço requerem uma liderança e governação forte e transversal, uma coordenação operacional ágil, célere e eficaz, uma capacidade de resposta e salvaguarda dos interesses nacionais e, acima de tudo, uma envolvência de recursos, conhecimentos e competências. Assim, no âmbito deste eixo devem ser adotadas as seguintes linhas de ação:

Sedimentar a estrutura nacional constante da Lei n.º 46/2018, de 13 de agosto, consolidando o Conselho Superior de Segurança do Ciberespaço como órgão específico de consulta do Primeiro-Ministro que assegure a coordenação político-estratégica para a segurança do ciberespaço, com representantes de todas as partes interessadas, que garanta uma abordagem transversal e inclusiva relativamente às políticas e iniciativas desenvolvidas pelas diversas entidades com responsabilidades neste âmbito;

Robustecer o Centro Nacional de Cibersegurança como Autoridade Nacional de Cibersegurança e, por inerência, como ponto de contacto único nacional para efeitos de cooperação internacional em matéria de cibersegurança, sem prejuízo das atribuições legais cometidas a outras entidades, nomeadamente, ao Ministério Público e à Polícia Judiciária, relativas a cooperação internacional em matéria penal, às Forças Armadas em matéria de ciberdefesa, ao Secretário-Geral do Sistema de Informações da República Portuguesa relativamente à produção de informações de segurança nacional, nas suas vertentes externa e interna e ao Secretário-Geral do Sistema de Segurança Interna relativamente ao Ponto Único de Contacto em matéria de cooperação policial internacional e às situações de alerta e resposta rápidas às ameaças à segurança interna;

Reforçar a capacidade de ciberdefesa nacional tendo em vista maximizar a resiliência das Forças Armadas para fazer face a incidentes ou ciberataques significativos que afetem os interesses e a soberania nacionais, devendo ser utilizados todos os meios para responder a ciberataques, incluindo a capacidade ofensiva no ciberespaço, sendo fundamental uma estreita ligação e coordenação com os diversos atores relevantes em casos de incidentes;

Reforçar a capacidade de cibersegurança nacional tendo em vista maximizar a resiliência das Forças e Serviços de Segurança, proteção e socorro, para fazer face a incidentes ou ciberataques significativos, no âmbito das respetivas atribuições, sendo fundamental uma estreita ligação e coordenação com os diversos atores relevantes em casos de incidentes;

Aprofundar o emprego dual das capacidades de ciberdefesa, no âmbito das operações militares e da cibersegurança nacional, desenvolvendo e consolidando um sistema de partilha de informação aos vários níveis e patamares de decisão;

Promover uma maior articulação e coordenação das entidades relevantes nas áreas da segurança do ciberespaço, nomeadamente, através da criação de sinergias com as entidades que integram o Sistema de Segurança Interna, bem como com as autoridades e reguladores sobre os setores relevantes, tais como o setor das comunicações eletrónicas e os setores relativos aos serviços essenciais;

Atualizar as estruturas do Ministério Público através da criação de estruturas especializadas de resposta a solicitações emergentes decorrentes da prática de crimes em ambiente digital, de forma a garantir eficácia na obtenção de elementos de prova e de forma a estar habilitado a satisfazer eventuais exigências de cooperação internacional em matéria penal;

Reforçar as capacidades da Polícia Judiciária através do robustecimento das suas estruturas e das suas capacidades humanas e técnicas para a investigação e o combate ao cibercrime, fomentando os recursos humanos afetados a esta área e a sua capacidade de execução de medidas de obtenção de prova com recurso a meios técnicos, bem como a resposta às exigências de cooperação policial internacional;

Robustecer o Serviço de Informações de Segurança, no âmbito da sua competência exclusiva para a produção de informações destinadas a garantir a segurança interna e necessárias a prevenir a sabotagem, o terrorismo, a espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido, bem como o Serviço de Informações Estratégicas de Defesa, no âmbito da sua competência exclusiva para a produção de informações que contribuam para a salvaguarda da independência nacional, dos

interesses nacionais e da segurança externa do Estado Português, sem prejuízo das atividades de informações levadas a cabo pelas Forças Armadas necessárias ao cumprimento das suas missões específicas e à garantia da segurança militar, para que os respetivos meios humanos e técnicos de pesquisa e análise possam ter a imagem clara das capacidades e intenções dos vetores de ameaça que, a cada momento, sejam identificados, reforçando paralelamente a cooperação internacional e consolidando a proximidade com os atores nacionais neste domínio;

Aplicar a legislação complementar ao regime jurídico de segurança do ciberespaço assegurando um enquadramento legal claro para todos, designadamente, em relação aos requisitos de segurança a cumprir, aos limiares para determinar o impacto de um incidente e aos requisitos de notificação de incidentes;

Capacitar o «CERT.PT» como a equipa de resposta a incidentes de segurança informática nacional, de forma a assegurar o exercício de coordenação operacional na resposta a incidentes, nomeadamente, em articulação com as equipas de resposta a incidentes de segurança informática existentes e todas as demais estruturas nacionais pertinentes, considerando que a notificação de incidentes permite melhorar o conhecimento situacional do ciberespaço de interesse nacional e facilitar a partilha de informação em benefício de todos;

Reforçar o papel das comunidades das equipas de resposta a incidentes de segurança informática como plataforma de excelência para a resposta operacional coordenada e a partilha de boas práticas e de informação relativa a incidentes;

Incrementar a interoperabilidade no seio das estruturas, designadamente através do desenvolvimento e aprofundamento da taxonomia e dos procedimentos existentes;

Desenvolver, no âmbito da atuação internacional, a ciberdiplomacia como a disciplina da ação externa do Estado que visa promover, nomeadamente, a aplicação do direito internacional vigente ao ciberespaço a fim de garantir a respetiva estabilidade, a governação transparente e partilhada da sua utilização universal e a criação eficiente de capacidades normativas, designadamente no seio da Comunidade dos Países de Língua Portuguesa.

Eixo 2 – Prevenção, educação e sensibilização:

No âmbito da prevenção, importa salvaguardar o papel fundamental da partilha de informação na avaliação precoce da ameaça. A incerteza permanente, relativa às diferentes ameaças de natureza difusa, contornos indefinidos e em permanente mutação e evolução que impendem sobre a segurança do ciberespaço de interesse nacional exigem capacidade nacional para detetar e conhecer atempadamente os indicadores que possam estar associados a ameaças

potenciais e em curso. Neste sentido, é fulcral desenvolver a capacidade de obter, de forma automatizada, sistematizada e coerente, conhecimento desses indicadores. O conhecimento homogéneo e criterioso de indicadores de ameaça permitirá assim a todo o ecossistema nacional da segurança do ciberespaço o conhecimento prévio adequado à produção de medidas de antecipação da ameaça e de segurança contra impactos não desejados.

Concomitantemente, a segurança do ciberespaço depende da promoção de uma cultura de segurança, enquadrada pelos princípios da ética, que proporcione a todos o conhecimento, a consciência e a confiança necessários para a utilização das redes e sistemas de informação, reduzindo a exposição aos riscos do ciberespaço. Neste contexto, é fundamental informar, sensibilizar e consciencializar não só as entidades públicas, mas, também as empresas e a sociedade civil. Por outro lado, é fundamental que o país se dote de recursos humanos qualificados para lidar com os complexos desafios da segurança do ciberespaço.

A garantia da segurança das infraestruturas tecnológicas, das redes e sistemas de informação depende da capacidade de os utilizadores finais adotarem medidas que previnam os riscos a que se encontram expostos. Assim, a sensibilização permanente constitui um fator essencial para a prevenção da segurança do ciberespaço.

Desta forma, no âmbito da prevenção, educação e sensibilização devem ser adotadas as seguintes linhas de ação:

Reforçar os meios de recolha e processamento de informação e as capacidades de análise;

Conhecer os agentes de ameaça, as suas intenções e capacidades e avaliar os potenciais impactos gerados pela sua atividade;

Antecipar a emergência, evolução e mutação das ameaças, possibilitando a adoção atempada de ações que acrescentem resiliência;

Criar uma sociedade mais resiliente, estimulando nos cidadãos o desenvolvimento de competências digitais, sem prejuízo de outros programas nacionais de índole congénere como é o caso, designadamente, do programa «Iniciativa Nacional Competências Digitais e.2030 - INCoDe.2030»;

Criar instrumentos e reforçar as medidas de sensibilização da sociedade civil para o uso seguro e responsável das tecnologias digitais, dando particular importância à capacitação e conhecimento obtidos por crianças, adolescentes, população sénior e outros grupos de risco;

Promover programas de capacitação em cibersegurança, robustos e transversais a todas as organizações e ao cidadão comum, permitindo que os utilizadores entendam as suas responsabilidades, usando e protegendo adequadamente as informações e os recursos que lhes são confiados;

Reforçar as competências e conhecimentos em segurança do ciberespaço na educação, incluindo estas temáticas na estrutura curricular dos ensinos básico, secundário e superior e na formação contínua de professores;

Promover a educação e literacia digital enquanto condição basilar para a confiança e utilização dos recursos digitais de uma forma consciente, informada e responsável das novas tecnologias pelas novas gerações e os grupos especialmente vulneráveis;

Incentivar a identificação de jovens com alto potencial para a área da cibersegurança e promover a sua integração atempada em contexto profissional;

Promover a formação técnica avançada em segurança do ciberespaço no ensino superior universitário e politécnico, de modo a suprir as necessidades nacionais de profissionais do sector;

Valorizar a inclusão do comportamento consciente e responsável da utilização da tecnologia enquanto parte integrante e transversal da formação académica e profissional corrente;

Promover formação especializada e sensibilizar os decisores, gestores públicos e operadores de infraestruturas críticas e de entidades que fornecem serviços essenciais à sociedade, numa ótica de consciencialização e prevenção para a necessidade de salvaguardar os interesses e informação crítica nacional;

Valorizar os profissionais no âmbito da segurança do ciberespaço, ampliando o número de especialistas, qualificando profissionais e envolvendo os diversos atores de toda a sociedade;

Garantir um nível elevado da qualidade dos cursos de formação e de requalificação em cibersegurança, obtido através da certificação deste quadro de referência;

Criar mecanismos de retenção em entidades nacionais de recursos humanos qualificados no âmbito da segurança do ciberespaço;

Organizar e realizar exercícios que permitam avaliar o grau de preparação e a maturidade das diversas entidades para lidar com incidentes com impacto relevante, potenciando sinergias. Adicionalmente participar em exercícios de âmbito internacional;

Tirar proveito das estruturas de ensino e formação militares e policiais nacionais e internacionais, aproveitando em particular a oportunidade da edificação em Portugal de estruturas específicas de ensino da Organização do Tratado do Atlântico Norte e da União Europeia e iniciativas associadas, para o aprofundamento do conhecimento relacionado com o ciberespaço e contribuindo para a sensibilização e prevenção na sua utilização;

Promover programas de sensibilização específicos junto das instituições públicas e privadas, que robusteçam a vertente comportamental de segurança em ambiente digital, com base na partilha de conhecimento especializado sobre os agentes da ameaça e seus modos de atuação; Sensibilizar as entidades nacionais para as respetivas vulnerabilidades específicas, passíveis de serem infiltradas, exploradas ou subvertidas no campo digital por agentes de ameaça diversos.

Eixo 3 – Proteção do ciberespaço:

A segurança do ciberespaço é parte integrante da segurança nacional e é essencial para o regular funcionamento do Estado, para o desenvolvimento económico e a inovação, bem como para a confiança dos cidadãos no mercado digital e no ciberespaço. Assim, para o presente eixo devem ser adotadas as seguintes linhas de ação:

Identificar e consolidar o conhecimento das infraestruturas críticas de informação, acompanhando a profunda alteração e dinâmica do quadro legal nacional e internacional da segurança do ciberespaço;

Promover o contínuo desenvolvimento das capacidades e maturidade das entidades nacionais na prevenção, deteção, resposta e recuperação perante cenários adversos à segurança do ciberespaço que possam produzir impactos nas suas redes e sistemas de informação e ecossistema que as caracteriza, consolidando a confiança mútua, a partilha de informação e conhecimento, e a cooperação célere e eficaz;

Promover estruturas de cooperação nacional e setorial de proteção do ciberespaço, inclusive do setor público ao nível central, regional e local, e também do setor privado, incluindo as pequenas e médias empresas, para a partilha de informação e de promoção da colaboração mútua na proteção de interesses comuns;

Garantir a aplicação de mecanismos e incentivos que permitam o desenvolvimento de quadros de referência nacionais e internacionais de gestão da segurança do ciberespaço e a sua adoção pelas entidades nacionais com responsabilidades sobre as infraestruturas críticas e serviços essenciais;

Maximizar a segurança e a defesa das redes e sistemas de informação das Forças Armadas e da Defesa Nacional tendo em vista a manutenção da capacidade de operação no ciberespaço através da capacidade de ciberdefesa defensiva.

Eixo 4 – Resposta às ameaças e combate ao cibercrime:

No domínio da resposta pós-incidente, dada as características dos ciberataques, para além das autoridades judiciárias e das entidades que integram o Sistema de Segurança Interna, têm intervenção outras entidades que, por força das suas atribuições, detenham informação, própria ou resultante da cooperação nacional e internacional, relevante para a atribuição da autoria ou que coadjuve a própria investigação criminal.

A segurança nacional do ciberespaço alicerça-se igualmente na sua capacidade de edificação de mecanismos de dissuasão. A realização de tal desiderato passa pela capacitação das entidades responsáveis pela segurança do ciberespaço de mecanismos defensivos e de resposta de modo a que qualquer atuação ilícita contra o ciberespaço de interesse nacional seja merecedora de uma ação apropriada.

Assim, a imprescindível existência de mecanismos de identificação, análise, avaliação e de disrupção da ameaça tornam imperativa a necessidade de reforço de meios de identificação de ameaça e de resposta apropriada, por meio do robustecimento das estruturas nacionais de segurança do ciberespaço.

Por outro lado, o ciberespaço proporcionou a criação quer de novos padrões de comportamento e ação humana em benefício da sociedade, quer de novas tipologias de ameaça e de crimes que necessitam de uma resposta atempada, coerente, participada e colaborativa, onde importa proteger os bens jurídicos legalmente consagrados e os direitos dos cidadãos. Complementarmente, para além de ter aberto o espaço para a prática de novos tipos de crimes, deu também origem a um ambiente propício para que se desenvolvam crimes antigos com novos métodos e ações ofensivas de grande envergadura lesivas do interesse nacional.

Importa, ainda, relevar que as ameaças do ciberespaço se caracterizam pela sua transversalidade, rápida propagação em rede, anonimização e persistência. Face a esta tipologia de ameaça, apenas uma resposta em rede potenciará e tornará resiliente o esforço e capacidade de toda a comunidade envolvida na mitigação dos riscos, minimizando ou impedindo os respetivos impactos e garantindo um elevado nível comum de segurança do ciberespaço de interesse nacional.

Os desafios colocados pela prevenção e investigação destes fenómenos implicam uma observação atenta e permanente, que permita, por um lado, preparar uma atempada evolução da legislação e, por outro, adequar a capacidade das entidades públicas e privadas para responder às ameaças que coloquem em causa a continuidade operacional e o combate ao cibercrime. Da mesma forma, tais desafios exigem que as instituições desenvolvam um permanente esforço de apetrechamento, que as habilite a cumprirem cabalmente as suas missões. Importa, pois, que os sistemas de resposta às ameaças, designadamente, o policial e judiciário, em esforço coordenado, se adaptem às formas de responder às ameaças e investigar os crimes que recorrem às novas tecnologias. Assim, devem ser adotadas as seguintes linhas de ação:

Desenvolver e consolidar a capacidade de ciberdefesa, com vista a assegurar a condução de operações militares no ciberespaço, assegurando a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional;

Adequar, para efeitos de gestão de crises, as capacidades das Forças Armadas, das Forças e Serviços de Segurança e de outras entidades públicas e privadas, tendo em vista impulsionar uma abordagem integrada às ameaças e riscos em matéria de segurança do ciberespaço;

Proceder à avaliação das necessidades de revisão e atualização da legislação. Deste modo, as entidades competentes devem adotar as medidas necessárias que lhes permitam preparar anteprojetos legislativos que se mostrarem necessários, quer na área do direito penal substantivo, quer quanto a instrumentos processuais e de cooperação institucional, policial e judiciária, nacional e internacional;

Avaliar no âmbito da cibercriminalidade a necessidade de ajustamento das normas processuais penais aos desafios globais que a mesma coloca e, em particular quanto a eventual acesso transfronteiriço a dados (prova digital), a eventual cooperação com operadores de comunicações estrangeiros e a agilização de ações de investigação online, incluindo as que possam enquadrar-se no contexto de ações encobertas, nos termos da lei;

Ponderar a atualização do existente enquadramento legal da retenção de dados e o enquadramento legal da apreensão do correio eletrónico e outras comunicações de natureza semelhante;

Reforçar a capacidade de resposta às ameaças, maximizando as sinergias criadas pela cooperação e confiança existentes entre as equipas de resposta a incidentes de segurança

informática, potenciando a criação de novas equipas desta natureza em todas as entidades, públicas e privadas, com responsabilidade pela segurança das redes e sistemas de informação;

Promover, ao nível setorial e do tecido empresarial, a criação de fora de partilha de informação operacional e técnica, de resposta coordenada a incidentes de segurança e de produção de referenciais de segurança específicos, garantindo a ligação destes fora com os seus congéneres internacionais, caso existam, e o alinhamento com os referenciais atinentes;

Consolidar e promover a capacidade nacional de conhecimento das ameaças à segurança do ciberespaço, de forma colaborativa entre as autoridades nacionais com responsabilidade nesta área e com a participação ativa das entidades do setor público e privado, produzindo e partilhando, desta forma, um conhecimento agregado que permita a antecipação dos impactos, a tomada de ações proativas e um melhor conhecimento da ameaça, por todos os envolvidos;

Fomentar e incentivar a participação das equipas de resposta a incidentes de segurança informática nos fora nacionais e internacionais especializados em segurança do ciberespaço, beneficiando da partilha de conhecimento e do reforço da confiança interpares.

Eixo 5 – Investigação, desenvolvimento e inovação:

A criação de capacidades tecnológicas no âmbito da segurança no ciberespaço assume-se como fundamental na presente Estratégia para um desenvolvimento sustentado e para a observação pertinente do futuro. Em consequência, pretende-se fortalecer, apoiar e promover o potencial nacional de investigação, desenvolvimento e inovação de processos e tecnologias de vanguarda para a cibersegurança, com base nas capacidades individuais e coletivas do setor público e privado, da academia e da indústria.

A tarefa de criação destas capacidades tecnológicas cabe em primeira instância ao Sistema Científico e Tecnológico Nacional, incluindo empresas, instituições públicas e instituições privadas, no âmbito dos seus compromissos nacionais e internacionais, assumidos em fora, organizações e sistemas de parcerias em representação de Portugal. Assim, devem ser adotadas as seguintes linhas de ação:

Promover a produção científica, o desenvolvimento e a inovação nos vários domínios da segurança do ciberespaço tendo como objetivo manter e afirmar a independência nacional neste domínio;

Estimular e potenciar através de financiamento adequado as capacidades científicas, técnicas e industriais do país, com especial ênfase nos domínios críticos e nas tecnologias emergentes,

dando prioridade ao desenvolvimento de tecnologias para a cibersegurança e à resposta às necessidades identificadas de inovação;

Apoiar a participação dos intervenientes em investigação, desenvolvimento e inovação em projetos internacionais;

Potenciar as sinergias decorrentes da participação nacional nos diversos fora internacionais neste domínio e a presença em território nacional de organismos internacionais que se dediquem à investigação, desenvolvimento e inovação neste âmbito;

Potenciar sinergias nacionais e atender aos esforços cooperativos em curso nas organizações internacionais de que Portugal faz parte integrante, nomeadamente, no âmbito da União Europeia (pooling & sharing), da Organização do Tratado do Atlântico Norte (smart defence) e de iniciativas multinacionais para, em colaboração com as universidades, centros de investigação e a indústria, desenvolver soluções tecnológicas com interesse para duplo uso civil e militar;

Promover o desenvolvimento de produtos, sistemas e serviços secure by design e secure by default;

Participar nos trabalhos das comissões técnicas nacionais e internacionais, para implementar as normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia;

Promover a inovação aliada à cibersegurança no Estado através das tecnologias de informação e comunicação mais eficazes, de acordo com outras estratégias nacionais pertinentes, designadamente, a Estratégia para a Transformação Digital na Administração Pública - Estratégia TIC 2020, bem como, a Estratégia para o desenvolvimento digital "Iniciativa Nacional Competências Digitais e.2030 - INCoDe.2030";

Assegurar a articulação de entidades do setor público e privado, da academia e do tecido empresarial, designadamente, do ecossistema empreendedor e dos clusters, promovendo a inovação tecnológica no País;

Promover a captação de investimento externo em matéria de segurança no ciberespaço.

Eixo 6 – Cooperação nacional e internacional:

Num mundo altamente interligado e interdependente, a segurança do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais e internacionais, alicerçada no desenvolvimento de confiança mútua. Este é um fator primordial para o incremento da resiliência da rede em que todos os cooperantes participam. Em consequência, a presente Estratégia preconiza um dever reforçado de cooperação entre as estruturas e entidades nacionais com responsabilidade nas áreas que contribuem para a segurança do ciberespaço, sejam elas do setor público ou do setor privado. Paralelamente fomenta a ação internacional de Portugal, quer no plano bilateral quer no plano multilateral, de forma a aprofundar a sólida rede de alianças existentes, exercer influência afirmando a sua presença no mundo e capacitando outros através de parcerias estratégicas, nomeadamente, no espaço lusófono, contribuindo assim ativamente para moldar o ecossistema internacional salvaguardando o interesse nacional. Adicionalmente importa caracterizar a participação nacional nas diversas atividades de ciberdefesa no contexto internacional onde Portugal se insere, as quais permitem agregar conhecimento e experiência, possibilitando também a afirmação nacional neste domínio. Deste modo, no âmbito deste eixo devem ser adotadas as seguintes linhas de ação:

Contribuir para a regulação e universalização do ciberespaço promovendo o respeito do direito internacional aplicável, a partilha transparente da sua governação entre todos os atores, a respetiva acessibilidade universal e a disseminação de boas práticas de utilização;

Aprofundar a participação nacional nos órgãos, organismos e agências relevantes, nomeadamente, da Organização das Nações Unidas, da União Europeia e da Organização do Tratado do Atlântico Norte. Deve também aprofundar a participação nacional na Organização para a Segurança e Cooperação na Europa, designadamente, no esforço de redução do risco de tensões entre Estados, no âmbito da segurança do ciberespaço;

Participar nos exercícios de cibersegurança e de ciberdefesa reforçando e aumentando o nível de maturidade para a proteção do ciberespaço, onde a partilha de informação e conhecimento constitui um fator fundamental;

Integrar organismos internacionais de cibersegurança e de ciberdefesa tendo em vista a cooperação internacional e a afirmação de Portugal neste domínio;

Aprofundar a coordenação e cooperação entre as diversas entidades nacionais com responsabilidades na segurança do ciberespaço, tendo em vista uma melhor capacidade de alerta e resposta para fazer face às ameaças;

Aprofundar a articulação entre o Centro Nacional de Cibersegurança e a ANACOM - Autoridade Nacional de Comunicações, bem como entre aquele e as entidades que compõem o Sistema de Certificação Eletrónica do Estado no âmbito das respetivas atribuições;

Desenvolver o quadro internacional da ciberdiplomacia em que Portugal se deverá inserir, identificando iniciativas prioritárias, nomeadamente, as organizações internacionais ou intergovernamentais de intercâmbio de boas práticas a que deverá aderir.

6 - Avaliação e revisão da Estratégia

A presente Estratégia será objeto de avaliação anual pelo Conselho Superior de Segurança do Ciberespaço. Tal avaliação incluirá uma verificação dos objetivos estratégicos e do plano de ação e adequação dos mesmos à evolução das circunstâncias.

Por outro lado, a rápida evolução intrínseca ao ciberespaço exige que a presente Estratégia seja objeto de revisão regular e periódica, considerando-se que, sem prejuízo de processos de revisão extraordinários sempre que as circunstâncias o exijam, aquela deve ocorrer num prazo máximo de cinco anos.

www.cncs.gov.pt
cncs@cncs.gov.pt

Rua da Junqueira 69,
1300-342 Lisboa
+351 210 497 400