

Estratégia Nacional de Segurança do Ciberespaço 2019-2023

Relatório de avaliação da execução
2019

Conselho Superior de Segurança do Ciberespaço

Março 2020

1. Sumário Executivo

Para a elaboração deste relatório anual, determinado pela alínea d) do n.º 1 do Artigo 6.º da Lei n.º 46/2018 de 13 de agosto, contribuíram dois exercícios realizados pelo Centro Nacional de Cibersegurança: o exercício de coordenação da elaboração e acompanhamento da execução do plano de ação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, conforme determina o n.º 3 da Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho; e o exercício de consolidação e análise dos resultados obtidos por via do acompanhamento da execução anteriormente referido.

Neste relatório referente à execução em 2019 do plano de ação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 mostra-se que no seu primeiro ano de implementação foram identificadas 206 atividades desenvolvidas, contando com o envolvimento de 32 organismos da Administração Pública correspondentes a 14 áreas de governação e às duas Regiões autónomas, e dois da sociedade civil. Constatou-se que 85% dessas atividades atingiram ou superaram as metas inicialmente definidas.

Concomitantemente à análise vertical dos resultados à luz da estrutura dos eixos de intervenção definida pela própria Estratégia de Segurança do Ciberespaço, foi realizada uma outra análise, podendo a mesma considerar-se transversal do documento estratégico, à luz da natureza de cada uma das atividades desenvolvidas. Esta segunda análise permitiu apurar que, no âmbito deste documento estratégico,

- As atividades com uma natureza estrutural e legislativa, representam cerca de 3% das atividades desenvolvidas, tendo sido atingidas ou superadas cerca de 67% das metas estabelecidas;
- As atividades com uma natureza de capacitação humana representam cerca de 33% das atividades desenvolvidas, tendo sido atingidas ou superadas cerca de 86% das metas estabelecidas;
- As atividades com uma natureza de capacitação organizacional e tecnológica representam cerca de 32% das atividades desenvolvidas, tendo sido atingidas ou superadas cerca de 86% das metas estabelecidas;

- As atividades de natureza relacionada com o conhecimento e partilha de informação representam cerca de 14% das atividades desenvolvidas, tendo sido atingidas ou superadas cerca de 83% das metas estabelecidas; e
- As atividades com uma natureza de cooperação representam cerca de 17% das atividades desenvolvidas, tendo sido atingidas ou superadas cerca de 83% das metas estabelecidas.

2. Enquadramento

A primeira Estratégia Nacional de Segurança do Ciberespaço foi aprovada pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, e visou o aprofundamento da segurança das redes e dos sistemas de informação, bem como potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos e das entidades públicas e privadas. Aquela Estratégia definiu um prazo de três anos para sua revisão. Em 2017, foi constituído um grupo de projeto, denominado Conselho Superior de Segurança do Ciberespaço (Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto), que tinha como um dos seus objetivos propor essa revisão e elaborar a nova Estratégia Nacional de Segurança do Ciberespaço (ENSC). No âmbito deste grupo de projeto foi elaborado um anteprojecto de ENSC que constituiu a base da nova ENSC que foi aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho.

Com a publicação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, em anexo à Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, é atribuída ao Centro Nacional de Cibersegurança a coordenação da elaboração e monitorização de um plano de ação que reúna os diferentes contributos de organismos públicos e privados que contribuam para os objetivos estratégicos aí definidos.

Com vista ao cumprimento dessa atribuição, foi proposto ao Conselho Superior de Segurança do Ciberespaço pelo Centro Nacional de Cibersegurança uma gestão do ciclo de vida da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 estabelecendo a recolha anual de atividades a inscrever no plano de ação em períodos bianuais. Este exercício anual visa, assim, construir as bases que permitam que seja dado, igualmente, cumprimento à alínea *d*) do número 1 do Artigo 6.º da Lei n.º 46/2018, de 13 de agosto, que atribui competência ao Conselho Superior de Segurança do Ciberespaço para a elaboração anual, ou sempre que necessário, do relatório de avaliação da execução da Estratégia Nacional de Segurança do Ciberespaço.



Figura 1 – Gestão do ciclo de vida da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

A primeira etapa deste ciclo de vida da Estratégia Nacional de Segurança do Ciberespaço 2019-2020 consistiu na interação com todos os organismos da Administração Pública com vista ao levantamento das atividades a desenvolver no biénio 2019-2020 com relevância para a persecução dos objetivos que o documento estratégico pretende alcançar. Estas atividades, contabilizadas em 372 e com a distribuição de metas de acordo com a seguinte tabela, constituíram a base do plano de ação 2019-2020 aprovado por Sua Excelência a Senhora Ministra de Estado e da Presidência.

| | Metas a atingir em 2019 | Metas a atingir em 2019 e 2020 (continuidade) | Metas a atingir em 2020 | Metas a atingir em anos seguintes |
|---------------------|-------------------------|---|-------------------------|-----------------------------------|
| Eixo 1 ¹ | 2 | 10 | 10 | 2 |
| Eixo 2 | 7 | 73 | 63 | 4 |
| Eixo 3 | 25 | 13 | 50 | 5 |
| Eixo 4 | 1 | 10 | 18 | 4 |
| Eixo 5 | 2 | 9 | 15 | 1 |
| Eixo 6 | 1 | 36 | 9 | 2 |

Tabela 1 – Distribuição por eixo das metas definidas para as atividades inscritas no plano de ação para o biénio 2019-2020

¹ 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.

Verifica-se uma maior ambição por parte dos organismos na concretização de atividades em 2020, com 316 atividades a desenvolver, em relação a 2019, com 189 atividades a desenvolver. Uma ambição que representa um incremento de cerca de 67% de atividades a desenvolver em relação a 2019. Foram ainda inscritas 18 atividades que, iniciando o seu período de execução em 2019 ou 2020, têm a sua concretização definida para anos seguintes.

Dos múltiplos aspetos positivos identificados no exercício de construção do plano de ação, para além da cooperação verificada entre os organismos, podem destacar-se a inclusão de atividades pela Região Autónoma dos Açores e pela Região Autónoma da Madeira, uma aposta em atividades que procuram a valorização e capacitação de profissionais da Administração Pública, seja ao nível de utilizadores das tecnologias, como de técnicos com responsabilidades na implementação, gestão e segurança dos sistemas de informação e infraestruturas. Destacam-se ainda atividades que preveem a atenção muito especial que merecem as questões da Cidadania Digital e Cibersegurança dirigidas aos jovens e professores, assim como o interesse na operacionalização de equipas de resposta a incidentes no ciberespaço e a sua integração na Rede Nacional de CSIRTs, na participação ativa em exercícios de Cibersegurança e Ciberdefesa e no reforço dos instrumentos de cooperação, nacional e internacional, entre organismos e comunidades para dotar os organismos de instrumentos e capacidade para responder às ameaças no ciberespaço.

Compete ao Conselho Superior de Segurança do Ciberespaço a produção de um relatório anual com a execução da Estratégia. O apoio logístico e administrativo na elaboração desse relatório, foi prestado pelo Centro Nacional de Cibersegurança, conforme determinado pelo Despacho n.º 1195/2018, de 2 de fevereiro, que aprova o Regulamento Interno do Conselho Superior de Segurança do Ciberespaço.

3. Metodologia

Um dos objetivos intrínsecos ao primeiro exercício de recolha de contributos para a construção do plano de ação para o biénio 2019-2020 foi o de sedimentar experiência e consolidar os instrumentos de recolha e o desenho de critérios orientadores, promovendo, para esse propósito, o contacto e a participação de todos os organismos da Administração Pública. O instrumento adotado foi o de uma tabela onde esses organismos pudessem partilhar informações sobre as atividades a desenvolver, o período de execução dessas atividades, qual ou quais as entidades responsáveis pela sua execução, respetiva unidade de medida, bem como as metas de execução estabelecidas para o biénio em consulta. Para esse efeito, a metodologia de recolha adotada passou pela solicitação de contributos através das Secretarias-Gerais das várias áreas governativas, dado o entendimento de estas disporem, de uma forma geral, de um maior alcance e possibilidade de chegar a todos os organismos da Administração Pública nas respetivas áreas governativas.

Posteriormente, o tratamento da informação recolhida incluiu a realização de reuniões setoriais ou individuais, sempre que possível de forma presencial, com os organismos que participaram neste exercício, tendo por objetivo a prestação de esclarecimentos e apoio no preenchimento das atividades em termos do seu enquadramento na Estratégia Nacional de Segurança do Ciberespaço 2019-2023, em especial no que respeita às Linhas de Ação para as quais concorrem, na linguagem utilizada e na tentativa de harmonização de indicadores.

Entre janeiro e fevereiro de 2020 procedeu-se ao levantamento, junto dos vários organismos com atividades inscritas no plano de ação para o biénio 2019-2020 e com metas definidas para 2019, do estado de execução dessas atividades e dos indicadores atingidos.

Neste enquadramento, a apresentação da análise da execução do plano de ação relativo ao ano 2019 da Estratégia Nacional de Segurança do Ciberespaço neste relatório será dividida em duas partes:

Na primeira parte, é apresentada uma análise quantitativa dos resultados com a estrutura estabelecida pela Estratégia Nacional de Segurança do Ciberespaço, isto é, dos eixos de intervenção que orientam a sua implementação.

Na segunda parte, é apresentada uma análise considerando a natureza das várias atividades com o objetivo de proporcionar uma melhor interpretação dos contributos e do foco dos organismos na persecução dos objetivos estratégicos definidos pela Estratégia Nacional de Segurança do Ciberespaço.

Em termos da linguagem utilizada neste relatório, sempre que for utilizada a expressão “atividade desenvolvida”, ou o seu plural, deve entender-se como uma atividade que implicou algum tipo de ação por parte do organismo responsável, mesmo que não tenha sido concretizada na sua plenitude. No caso em que se verifique que o resultado da atividade não tenha atingido a sua meta ou que esta tenha sido superada, utilizar-se-á a expressão “com desvio”, ou o seu plural, sendo que esta poderá ser complementada com as expressões “por defeito”, quando se verificar a primeira situação, isto é, quando o resultado do desenvolvimento da atividade não atingiu completa ou parcialmente a sua meta, e “por excesso”, quando se verificar a segunda situação, isto é, quando o resultado do desenvolvimento da atividade superou a sua meta ou o quando o resultado do desenvolvimento da atividade foi antecipado em relação ao período de execução inicialmente identificado.

Nas referências a resultados observados, a preferência de apresentação recai sobre a sua expressão em percentagem sendo que, quando não expressos no texto, os seus valores absolutos serão apresentados entre parênteses curvos (n).

4. Análise da execução

4.1 Uma abordagem global

Os resultados da análise efetuada agora apresentados têm por base uma abordagem que considerou a matriz definida pela própria Estratégia Nacional de Segurança do Ciberespaço, que estabelece seis eixos de intervenção como orientação para a persecução dos objetivos estratégicos que se propõe alcançar.

| | |
|---|--|
| <i>Eixos da Estratégia Nacional de Segurança do Ciberespaço</i> | 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 |

Tabela 2 – Eixos de intervenção da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

No ano 2019 observou-se o desenvolvimento de atividades com a participação de organismos referentes a 14 áreas governativas, a saber, Economia e Transição Digital (1), Presidência (5), Finanças (2), Defesa Nacional (3), Administração Interna (5), Justiça (1), Modernização do Estado e da Administração Pública (1), Planeamento (1), Cultura (1), Ciência, Tecnologia e Ensino Superior (2), Educação (1), Trabalho, Solidariedade e Segurança Social (3), Saúde (1) e Infraestruturas e Habitação (1). Concomitantemente, verificaram-se atividades desenvolvidas por organismos da Região Autónoma dos Açores (1) e da Região Autónoma da Madeira (3).

Na sua grande maioria, o desenvolvimento destas foi registado com uma única entidade responsável pelo seu desenvolvimento, excetuando as atividades

desenvolvidas conjuntamente pela área da Ciência, Tecnologia e Ensino Superior e a Associação Portuguesa de Apoio à Vítima (1), pela área da Presidência e a Associação DNS.PT (1), uma atividade com o envolvimento conjunto de cinco organismos da área da Administração Interna, e ainda uma outra atividade com o envolvimento das áreas da Presidência, da Defesa Nacional e da Justiça.

Os dados apurados mostram que em 2019 foram desenvolvidas 206 atividades, o que representa um acréscimo de 17 atividades em relação às 189 inicialmente previstas, demonstrando que alguns dos organismos anteciparam para 2019 o desenvolvimento de atividades com metas que haviam sido definidas para o ano 2020 e/ou subsequentes.

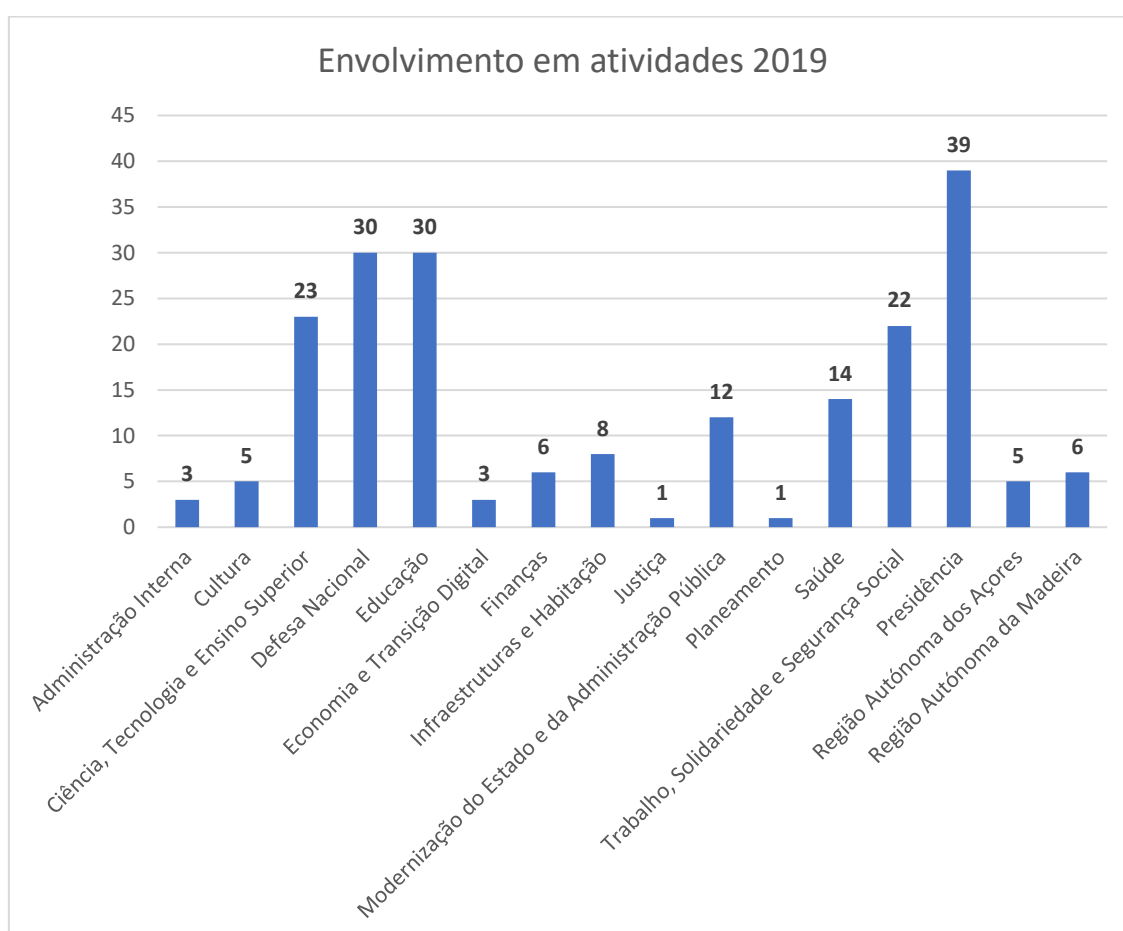


Gráfico 1 – Envolvimento das Áreas de Governo e Regiões Autónomas nas atividades desenvolvidas em 2019

Em termos absolutos, das 189 atividades programadas para 2019, 138 atingiram as metas inicialmente definidas representando, assim, um grau de execução de cerca de 73%, tendo-se verificado 68 atividades com desvios. Nestas últimas, identificam-se *i*) atividades com desvios por defeito (31), isto é, atividades que não foram implementadas

na sua totalidade ou que foram implementadas parcialmente, justificadas pelo calendário eleitoral verificado em 2019, por “condicionantes de ordem interna e alheios” aos organismos, por “constrangimentos de ordem orçamental em matéria de aquisição de serviços” ou mesmo pelo facto de a sua implementação ter dependências de outros organismos, algumas vezes internacionais; e, em maior número, *ii*) atividades com desvios por excesso (37) em resultado da antecipação da sua implementação (17) em relação ao período de execução previsto ou por terem sido superadas as metas das atividades inicialmente previstas (20).

Tabela 3 – Quadro de atividades previstas e desenvolvidas em 2019 por estado de concretização

| | Atividades programadas | Atividades desenvolvidas | Metas atingidas ou superadas | Metas não superadas |
|--------------|-------------------------------|---------------------------------|-------------------------------------|----------------------------|
| Eixo 1 | 12 | 13 | 8 | 5 |
| Eixo 2 | 80 | 87 | 72 | 15 |
| Eixo 3 | 38 | 42 | 36 | 6 |
| Eixo 4 | 11 | 11 | 9 | 2 |
| Eixo 5 | 11 | 12 | 11 | 1 |
| Eixo 6 | 37 | 41 | 39 | 2 |
| Total | 189 | 206 | 175 | 31 |

Tabela 4 – Quadro de atividades previstas e desenvolvidas em 2019 por estado de concretização

Assim, se, de todas as atividades desenvolvidas, se considerarem as que atingiram as suas metas iniciais e as que superaram ou anteciparam essas metas, verifica-se, então, uma execução de cerca de 85% (175/206).

Numa perspetiva de áreas governativas, no computo das atividades desenvolvidas, os dados coligidos mostram que a percentagem das metas atingidas ou superadas ultrapassou os 80%: Economia e Transição Digital 100% (3), Presidência do Conselho de Ministros 90% (35), Finanças 83% (5), Defesa Nacional 73% (22), Administração Interna 100% (3), Justiça 100% (1), Modernização do Estado e da Administração Pública 92% (11), Planeamento 100% (1), Cultura 100% (5), Ciência, Tecnologia e Ensino Superior 83% (19), Educação 93% (28), Trabalho, Solidariedade e Segurança Social 82% (18), Saúde 93% (13) e Infraestruturas e Habitação 88% (7). Relativamente às Regiões Autónomas, verificara-se que 80% (4) das atividades desenvolvidas pelos organismos da Região Autónoma dos Açores atingiram ou superaram as metas estabelecidas e na Região Autónoma da Madeira este valor foi de 33% (2).

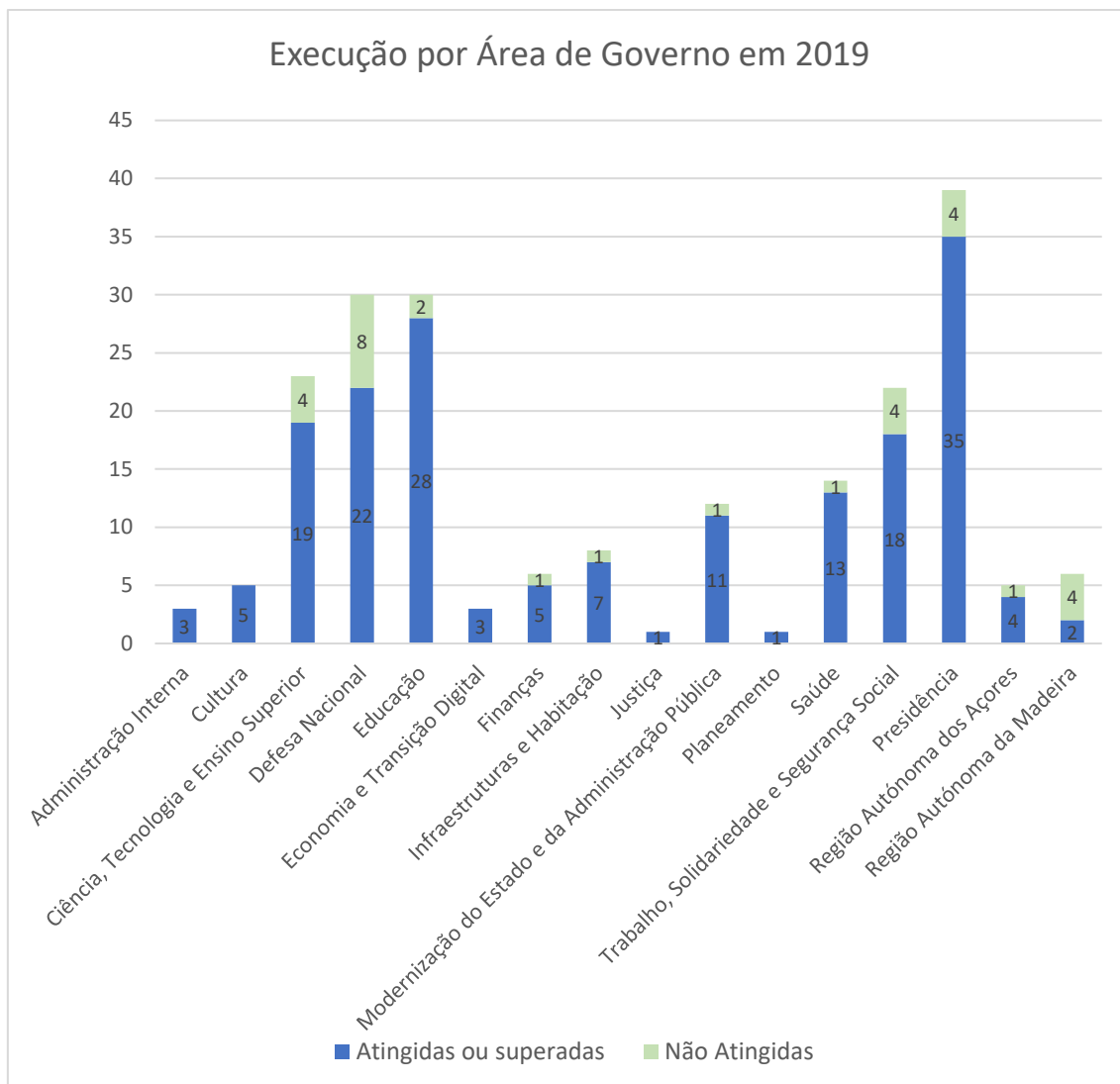


Gráfico 2 – Metas atingidas ou superadas e metas não atingidas por Área de Governo e Regiões Autónomas em 2019

Para o quadro anterior, contribuiu a antecipação, para 2019, de atividades cujas metas haviam sido estabelecidas para 2020, e/ou anos subsequentes, pelas áreas da Economia e Transição Digital (2), Finanças (3), Defesa Nacional (2), Administração Interna (1), Cultura (2), Ciência, Tecnologia e Ensino Superior (1), Trabalho, Solidariedade e Segurança Social (2) e Saúde (4).

- 85% das atividades desenvolvidas atingiram, superaram ou anteciparam as metas inicialmente definidas;
 - As atividades cujas metas foram superadas ou antecipadas (37) representam cerca de 18% das 206 atividades desenvolvidas;
- 15% das atividades desenvolvidas (31) não atingiram as metas inicialmente definidas.

4.2 Uma abordagem por natureza da atividade

Ao longo do exercício de recolha e consolidação dos contributos para o plano de ação da Estratégia Nacional de Segurança do Ciberespaço, verificou-se que algumas das atividades inscritas apresentavam objetivos transversais em termos de linhas de ação, e muitas vezes em termos dos eixos de intervenção. Nesse sentido, concluiu-se a necessidade de identificar a natureza dessas atividades inscritas por forma a conseguir-se, não só estabelecer uma matriz com os eixos de intervenção e os objetivos estratégicos, como contribuir para uma interpretação dos objetivos que as atividades pretendem atingir e, dessa forma, contribuir para uma base de conhecimento de comunicação da execução da Estratégia Nacional de Segurança do Ciberespaço.

Para esse efeito, tomando como referência as atividades inscritas no plano de ação para o biénio 2019-2020, da análise e interpretação das atividades a desenvolver foi possível identificar a sua natureza, respeitando o “espírito” subjacente à sua inscrição pelo organismo, enquadrada nos objetivos que pretendem atingir.

Na seguinte tabela identificam-se a natureza e foco das atividades:

| Natureza | Foco |
|---|--|
| <i>Estrutural</i> | Decisão/Avaliação Estratégica Nacional e Regional |
| <i>Capacitação Humana</i> | Formação/Sensibilização Cidadãos |
| | Formação/Sensibilização Recursos Humanos |
| | Formação/Sensibilização Especialistas |
| | Formação/Sensibilização Decisores |
| | Conteúdos Formação/Sensibilização |
| | Outras Ações para Formação/Sensibilização |
| | <i>Capacitação Organizacional e Tecnológica</i> |
| | Exercícios e Operações de Cibersegurança |
| | Identificação, Contratação e Retenção de Profissionais |
| <i>Conhecimento e Partilha Informação</i> | Promoção do Conhecimento |
| | Investigação, Desenvolvimento e Inovação |
| | Partilha de Informação (operacional) |
| | Estruturas de Governação (sectorial) |
| <i>Cooperação</i> | Cooperação Nacional |
| | Cooperação Internacional |

Tabela 5 – Identificação da natureza e do foco das atividades da Estratégia Nacional de Segurança do Ciberespaço

Neste exercício, e com base na análise os resultados comunicados, verifica-se que a o maior número de atividades desenvolvidas pelos organismos são essencialmente dirigidas para a capacitação humana, representando cerca de 33% (69), e para a capacitação organizacional e tecnológica de organismos, com cerca de 32% (66). A vertente de cooperação, representando cerca de 17% (36) das atividades desenvolvidas, é também uma propriedade da cibersegurança que mereceu alguma atenção por parte dos organismos.

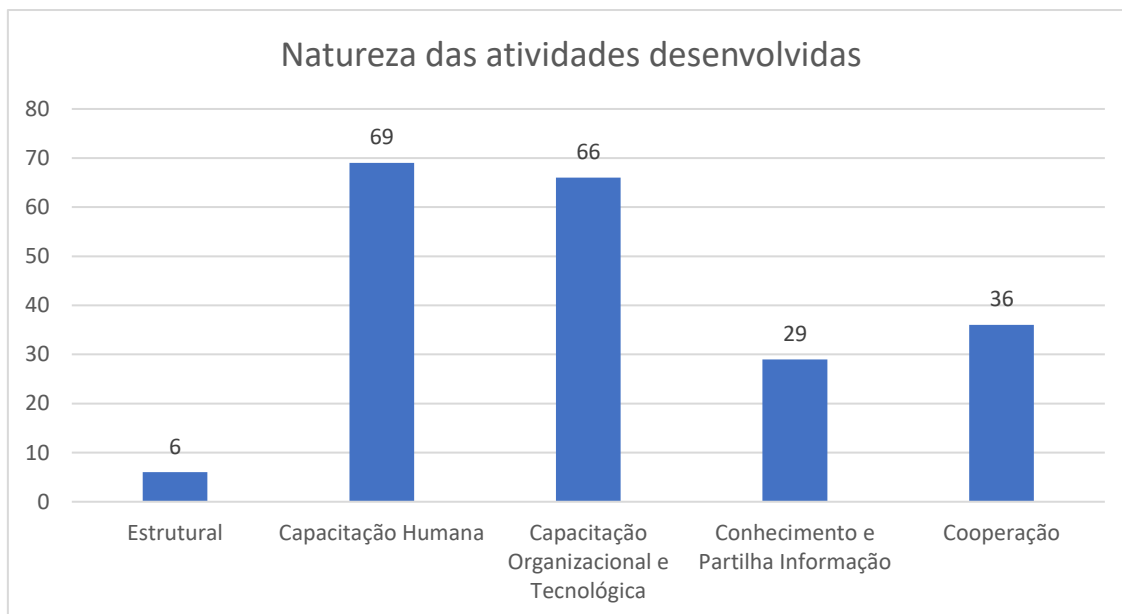


Gráfico 3 – Natureza das atividades desenvolvidas em 2019 no âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

Em seguida apresenta-se uma análise em mais detalhe em cada uma destas vertentes, com o enquadramento prévio que se considera pertinente.

4.2.1 Atividades Estruturais

Enquadram-se neste âmbito as atividades cuja natureza contribua para o contexto estrutural e legislativo em matéria de cibersegurança, bem como para a decisão e avaliação estratégica de enquadramento Nacional e Regional. Consideram-se atividades de carácter legislativo ou estratégico, como serão os casos da adoção de estratégias nacionais ou regionais, da adoção de legislação ou doutrinas, da implementação de estruturas orgânicas, ou da proposta ou adoção de iniciativas que alterem enquadramentos no âmbito das políticas públicas (como por exemplo a alteração de programas nacionais de ensino, a definição de quadros de referência, etc.).

Da análise efetuada, resulta a identificação de atividades (6) desta natureza numa dimensão representativa de cerca 3% das 206 atividades desenvolvidas ao longo de 2019, sendo que destas, cerca de 67% atingiram as metas inicialmente estabelecidas (4), e em cerca de 33% verificaram-se desvios por defeito (2). Verificou-se o desenvolvimento de atividades no âmbito da coordenação político-estratégica para a segurança do ciberespaço, as propostas de Estratégia Nacional de Ciberdefesa e do Plano Nacional "Escola sem *Bullying*. Escola sem Violência", e ainda a elaboração e disponibilização do Quadro Nacional de Referência para a Cibersegurança.

- 3% das atividades desenvolvidas ao longo de 2019 foram de natureza estrutural e legislativa;
- 67% das atividades de natureza estrutural atingiram as metas inicialmente estabelecidas;
- 33% das atividades de natureza estrutural não foram atingidas.

4.2.2 Atividades de Capacitação Humana

Para a “Capacitação Humana” identificam-se todas as atividades cujos objetivos contribuam para a formação de cidadãos, de profissionais das organizações, de especialistas e de decisores. Por norma, as atividades que concorrem para este objetivo apresentam indicadores quantitativos (tendencialmente “n.º de pessoas alcançadas”). No que respeita à capacitação de especialistas, consideraram-se igualmente atividades que incluam a realização de CTF² ou *hackatons*³.

Identificam-se também atividades que pretendem disponibilizar conteúdos de formação ou sensibilização sob a forma de plataformas, aplicações, websites, publicações, conteúdos para comunicação ou campanhas de disseminação (cujo público a alcançar não corresponda a um universo controlável ou mensurável). Consideram-se

² Competições designadas por *Capture The Flag* com o objetivo de desafiar os participantes a resolver desafios de segurança.

³ Eventos dirigidos a programadores informáticos onde os participantes são desafiados a encontrar/desenvolver soluções e projetos, de forma individual ou colaborativa, habitualmente relacionados com inovação.

ainda outras atividades na área da formação e sensibilização que não se enquadrem nas atividades anteriores. Nestas, entre outras, podem enquadrar-se atividades como propostas de ações ou planos de formação que não assumam um caráter estrutural ou legislativo, isto é, que não assumam uma capacidade de estabelecer alterações programáticas nas áreas do ensino formal (seja de âmbito nacional ou regional). Aqui, consideram-se atividades efetuadas junto de comunidades ou associações e cujo público a alcançar não seja passível de ser controlado ou medido pela entidade proponente.

Resulta da análise efetuada que as atividades que contribuíram para a capacitação de pessoas (69), assentaram, na sua generalidade, na realização de ações com o objetivo de sensibilizar e formar pessoas na temática da cibersegurança e da literacia digital, presencialmente e com recurso a plataformas digitais para o ensino e formação à distância. Estas atividades representam cerca de um terço (33%), do total das atividades desenvolvidas em 2019. Destas, cerca de 55% (38) foram atingidas de acordo com as metas inicialmente estabelecidas, sendo que nas restantes atividades, em cerca de 45% (31) verificaram-se desvios por defeito (10) e por excesso (21).

As atividades desenvolvidas com esta natureza destinaram-se a vários público-alvo:

- a) a cidadãos em geral, representado cerca de 6% do total dessas atividades desenvolvidas;
- b) a recursos humanos, de âmbito geral, nos organismos, representando cerca de 11% do total dessas atividades desenvolvidas;
- c) a especialistas em áreas de tecnologia e cibersegurança, representando cerca de 3% do total dessas atividades desenvolvidas; e
- d) decisores, públicos e privados, representando cerca de 5% do total dessas atividades desenvolvidas.

Ainda deste âmbito, cerca de 9% do total dessas atividades foram focadas no desenho e produção de conteúdos de formação e sensibilização para estas temáticas.

Verifica-se, portanto, que cerca de 86% das atividades com uma natureza de capacitação humana atingiu ou superou as metas inicialmente estabelecidas.

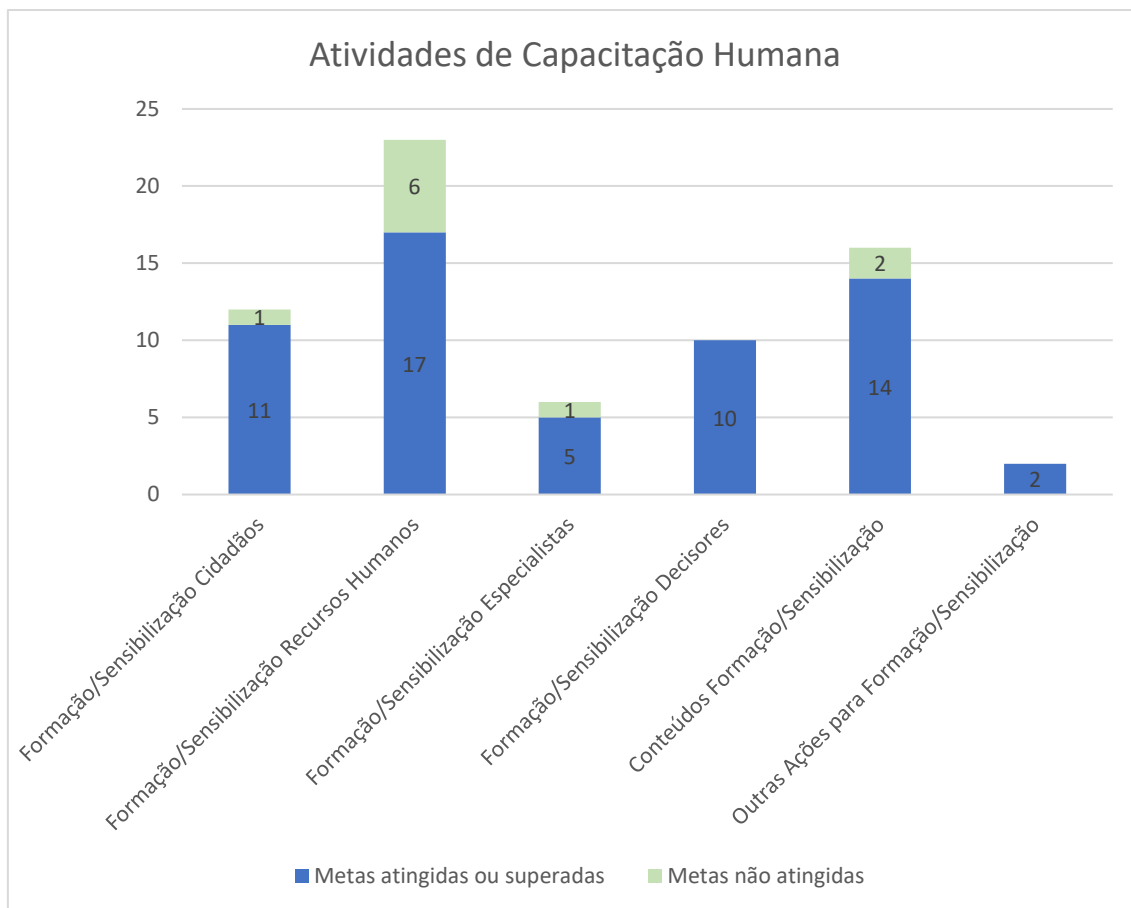


Gráfico 4 – Atividades de Capacitação Humana desenvolvidas em 2019 no âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

De todos os organismos que desenvolveram atividades no âmbito da Estratégia Nacional de Segurança do Ciberespaço, cerca de 63% dos organismos (20) desenvolveu atividades de natureza de capacitação humana. Dos resultados obtidos, constata-se que pelo menos 275 654 pessoas terão tido conhecimento destas iniciativas, tendo delas beneficiado, através da concretização de ações de sensibilização e formação, 135 364 pessoas. Deste universo, 67% das pessoas (91 159) encontravam-se em ambiente escolar, em que cerca de 3 000 serão professores, e cerca de 13% (17 021) estavam em ambiente profissional, sendo a maior fatia (93%), pertencente aos colaboradores não especializados nas áreas da tecnologia (TI) e cibersegurança (15 787). Algumas atividades tiveram o seu foco na sociedade de forma geral, estimando-se um alcance de cerca de pelo menos 27 184 pessoas, representando aproximadamente 10% do universo de pessoas alcançadas.

Capacitação Humana - Formação/Sensibilização

| | | | | | |
|-----------------------|--|--------|--------|--------|-----|
| Universo Escolar | Alunos e Professores ⁴ | 88 289 | 32,03% | 91 159 | 67% |
| | Professores | 2 870 | 1,04% | | |
| Universo profissional | Colaboradores não especializados em TI ou cibersegurança | 15 787 | 5,73% | 17 021 | 13% |
| | Colaboradores especializados em TI ou cibersegurança | 140 | 0,05% | | |
| | Decisores (públicos e privados) | 1 094 | 0,40% | | |
| Sociedade | Cidadãos | 27 184 | 9,86% | | |

Tabela 6 – Distribuição de pessoas alcançadas por ações de sensibilização e formação

De salientar que as atividades desenvolvidas em ambiente escolar se limitaram ao ensino básico e secundário.

- 33% do total das atividades desenvolvidas em 2019 tiveram uma natureza de capacitação humana;
- 86% das atividades de capacitação humana atingiu ou superou as metas inicialmente estabelecidas;
- 14% das atividades de capacitação humana não atingiu as metas estabelecidas;
- 135 364 pessoas beneficiaram de ações de sensibilização e formação.

4.2.3 Atividades de Capacitação Organizacional e Tecnológica

As atividades com uma natureza de “Capacitação Organizacional e Tecnológica” contribuem para o reforço das organizações, tendo sido identificados três focos de atuação:

- i. um que agrega atividades de gestão de cibersegurança, focadas no desenho e adoção de normas e políticas organizacionais, incluindo a vertente de conformidade, que contribuam para uma cultura de cibersegurança;

⁴ Em sede de apresentação de resultados, constata-se que a maior parte das ações de sensibilização ocorreu em ambiente escolar alcançando simultaneamente alunos e professores, e eventualmente pessoal não docente, sendo que os organismos responsáveis pela sua implementação não apresentaram a sua segregação em termos do tipo de participante.

- ii. um outro para atividades que compreendam a participação em exercícios de cibersegurança e ciberdefesa, bem como a implementação de soluções ou ferramentas (de forma isolada de processos de gestão de risco e conformidade com normas adotadas) que contribuam para a cultura de cibersegurança nas organizações, como serão os casos de implementação, desenvolvimento ou aquisição de produtos, aplicações ou equipamentos, bem como a realização de auditorias ou testes de penetração (sejam estas campanhas de *phishing* dentro das organizações para avaliar o grau de falha ou de identificação e análise de vulnerabilidades, etc.); e
- iii. ainda um terceiro que prevê atividades que pretendam identificar potenciais profissionais na área da cibersegurança ou com vista à contratação ou retenção de recursos humanos com elevado nível de qualificação neste campo (aqui podem considerar-se discriminações positivas em matéria de remuneração, etc.).

Na análise realizada, as atividades que se consideram ter uma natureza de capacitação organizacional e tecnológica dos organismos, representam cerca de 32% (66) do total das atividades desenvolvidas em 2019, com o envolvimento de 72% (23) do universo de organismos que participaram na implementação do plano de ação da Estratégia Nacional de Segurança do Ciberespaço. Estas atividades focaram-se

- a) no reforço da gestão da cibersegurança dos organismos, como são a definição e implementações de políticas internas de segurança de sistemas e informação, de planos de continuidade de negócio e planos estratégicos, a obtenção de certificações de acordo com normas internacionais, ou a identificação de ativos críticos para os organismos;
- b) na organização e participação em exercícios, nacionais e internacionais, de cibersegurança e ciberdefesa e realização de operações de cibersegurança como a implementação de novas soluções tecnológicas para a deteção e mitigação de ameaças, a instalação de Centros de Operações de Segurança⁵ ou realização de auditorias e testes de verificação de vulnerabilidades; e

⁵ Security Operations Center (SOC).

- c) na identificação, contratação e retenção de profissionais especializados em cibersegurança.

Nesta vertente, verificou-se que cerca de 73% (48) das metas atingiram os valores inicialmente definidos, tendo-se identificado desvios em cerca de 27% (18) das atividades, sendo este número dividido em partes iguais entre desvios por defeito e desvios por excesso.

A contabilização destes dados mostra, por isso, que cerca de 86% das atividades dirigidas à capacitação organizacional e tecnológica atingiu ou superou as metas inicialmente estabelecidas.

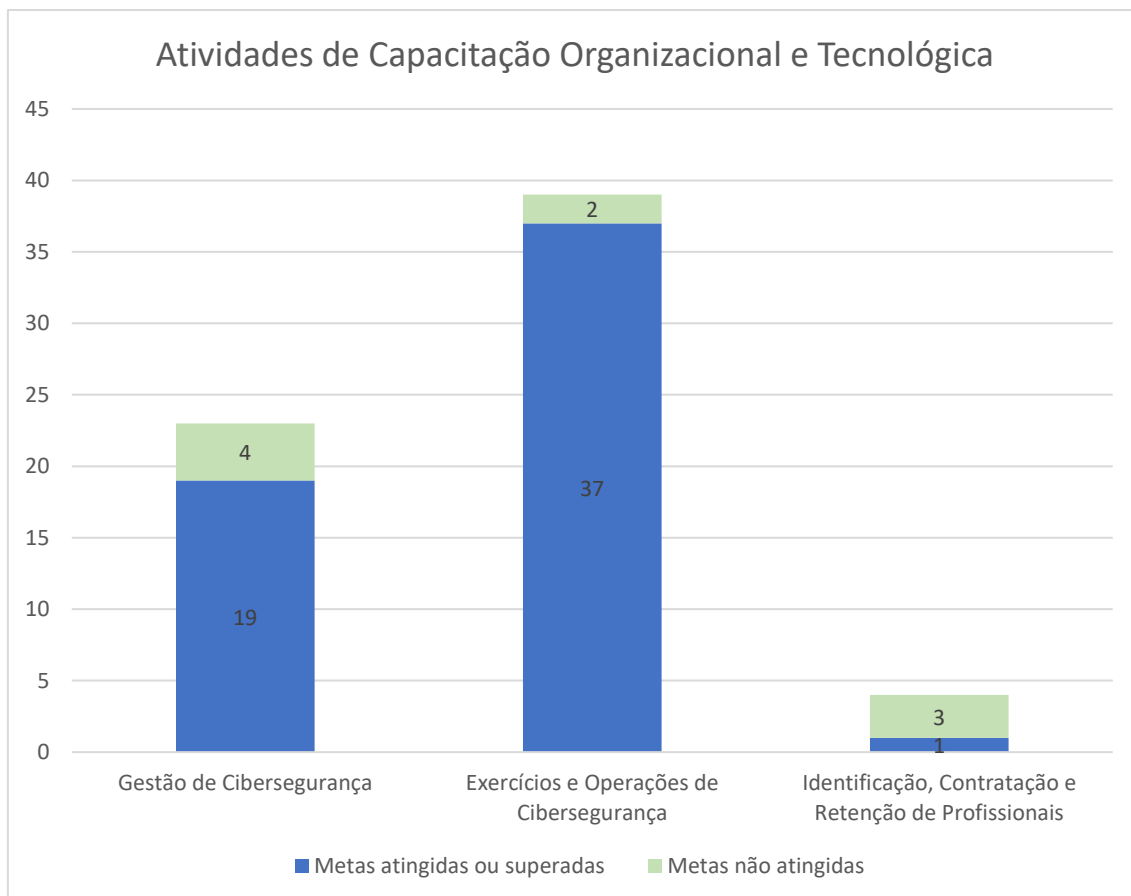


Gráfico 5 – Atividades de Capacitação Organizacional e Tecnológica desenvolvidas em 2019 no âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

- 32% do total das atividades desenvolvidas em 2019 tiveram uma natureza de capacitação organizacional e tecnológica;
- 86% das atividades de capacitação organizacional e tecnológica atingiu ou superou as metas inicialmente estabelecidas;
- 14% das atividades de capacitação organizacional e tecnológica não atingiu as metas estabelecidas.

4.2.4 Atividades de Conhecimento e Partilha Informação

Com uma natureza de “Conhecimento e Partilha Informação” identificam-se atividades que se focam na promoção do conhecimento numa lógica de partilha e disseminação entre múltiplos atores, a Investigação, Desenvolvimento e Inovação, a partilha de informação com uma perspetiva operacional – distinta da partilha de

conhecimento – e a criação e operacionalização de estruturas de governação em matéria de cibersegurança numa lógica sectorial.

Com o primeiro foco, a promoção do conhecimento, admitem-se as atividades como a realização e/ou participação em eventos (conferências, seminários, *workshops*) de carácter mais transversal, de participações na qualidade de formador ou docente, ou produção de documentação que, não tendo um carácter de se constituir como produção científica, permita o entendimento de panoramas e enquadramentos.

Focadas na Investigação, Desenvolvimento e Inovação (I&D&I), distinguem-se aquelas atividades que visam fomentar o financiamento ou participação de projetos de I&D&I, nacionais e internacionais, ou ainda a produção de conhecimento científico em cibersegurança e acomodação de estágios que visem alargar o âmbito e o campo de investigação nesta matéria.

O foco na partilha de informação tem privilegiado os aspetos de cariz operacional, seja entre organizações, multilateral ou bilateralmente, com vista a identificação de riscos e ameaças de âmbito nacional e/ou regional, ou o estabelecimento, por exemplo, de Centros de Análise e Partilha de Informação⁶. No entanto, identifica-se o surgimento de novas estruturas de governação da Cibersegurança de âmbito setorial ou abrangendo as entidades de uma de área de governação.

Observou-se que, no conjunto das atividades com uma natureza relacionada com o conhecimento e partilha de informação, representando cerca de 14% (29) do total desenvolvido em 2019, foram promovidas atividades com um foco na

- d) incremento do conhecimento (15), enquadrando-se atividades como o intercâmbio de recursos humanos na área da educação e sensibilização, a realização de estágios profissionais, a produção de relatórios sobre o nível de exposição nacional a vulnerabilidades específicas, ou ainda a disseminação de iniciativas nacionais e internacionais dirigidas a comunidades específicas e participação em eventos temáticos;

⁶ Information Sharing and Analysis Center (ISAC)

- e) Investigação, Desenvolvimento e Inovação (4), enquadrando-se atividades como a definição de indicadores, a produzir de forma sistemática, que permitam a caracterização do estado da cibersegurança em Portugal, o estabelecimento de ações de reconhecimento científico em cibersegurança ou a participação em projetos de I&D&I no âmbito da cibersegurança e ciberdefesa;
- f) partilha de informação numa perspetiva operacional (8), enquadrando-se atividades como a implementação de Centros de Análise e Partilha de Informação, a automatização da partilha de informação em cibersegurança entre organismos, a implementação de plataformas de partilha de informação de indicadores de compromisso ou a produção de níveis de alerta; e
- g) implementação de estruturas de governação setoriais (2), isto é, estruturas de comando e controlo de riscos de cibersegurança em áreas de governação.

Neste campo, verificou-se que cerca de 69% (20) das metas estabelecidas foram atingidas, sendo que, nas restantes atividades, cerca de 31% (9), tiveram desvios por defeito (5) e por excesso (4).

Estes dados apontam para uma percentagem de metas atingidas e superadas das atividades orientadas para a criação de conhecimento e partilha de informação na ordem dos 83%.

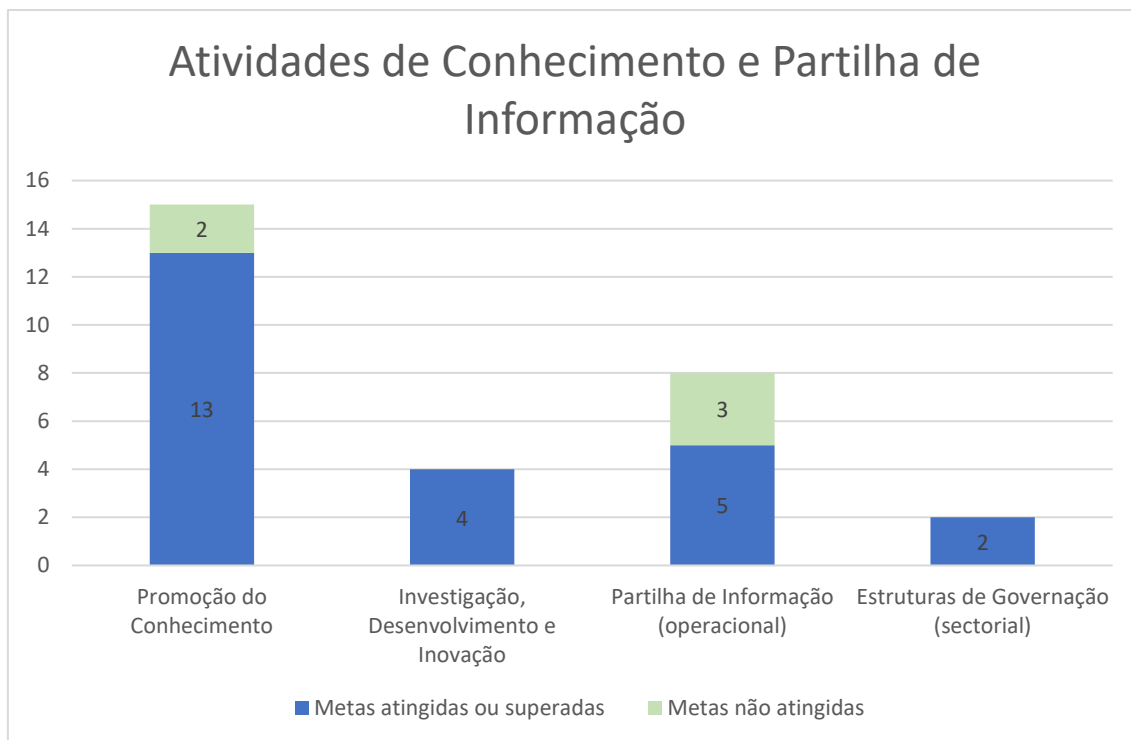


Gráfico 6 – Atividades de Conhecimento e Partilha de Informação desenvolvidas em 2019 no âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

- 14% do total das atividades desenvolvidas em 2019 tiveram uma natureza de relacionada com o conhecimento e partilha de informação;
- 83% das atividades de conhecimento e partilha de informação atingiu ou superou as metas inicialmente estabelecidas;
- 17% das atividades de conhecimento e partilha de informação não atingiu as metas estabelecidas.

4.2.5 Atividades de Cooperação

Deve reiterar-se que, apesar das linhas de ação previstas no eixo Cooperação assumirem uma relevância do ponto de vista do posicionamento de Portugal a nível internacional, as atividades retratadas nesta secção devem ser interpretadas de forma mais abrangente, nomeadamente considerando a sua natureza, e não estritamente à luz desse eixo de intervenção.

Esta situação resulta do facto de se verificar que atividades com uma natureza de cooperação, com foco nacional e internacional, se enquadram igualmente em linhas de ação de eixos de intervenção que extravasam o eixo específico da Cooperação. Nesta disposição identificam-se 12 atividades, o que é ilustrativo da transversalidade das linhas de ação que enformam os eixos.

Assim, com uma natureza de “Cooperação”, seja ao nível nacional ou ao nível internacional, consideram-se as atividades que reflitam a representação e representatividade de Portugal nas Organizações Internacionais e nacionais em grupos de trabalho, comités, conselhos de administração ou grupos de peritos e de aconselhamento. Também se consideram atividades que enquadrem o estabelecimento de protocolos de cooperação e memorandos de entendimento que não se revelem passíveis de ser enquadrados num plano estratégico nacional ou internacional.

Na análise realizada constatou-se que das atividades (36) com uma natureza de cooperação, nacional (11) e internacional (25), o que representa cerca de 17% do total das atividades desenvolvidas em 2019, houve o envolvimento de cerca de 38% (12) dos organismos que participaram na implementação do plano de ação da Estratégia Nacional de Segurança do Ciberespaço. Estas atividades revelam a representação de Portugal em organizações e instituições internacionais como o Conselho da União Europeia e Comissão Europeia, a Agência Europeia para a Cibersegurança (ENISA), grupos de trabalho, ações comuns e parcerias no âmbito da União Europeia, na Organização para a Segurança e Cooperação na Europa (OSCE), a Organização para a Cooperação e Desenvolvimento Económico (OCDE), o Fórum da Governação da Internet no âmbito da Organização das Nações Unidas (ONU), a União Internacional de Telecomunicações, a *Internet Assigned Names and Numbers* (ICANN), a European SchoolNet, a Rede Insafe, a Organização do Tratado do Atlântico Norte (NATO), a *Task Force on Computer Security Incident Response Teams* (TF-CSIRT) e *Forum of Incident Response and Security Teams* (FIRST), entre outros.

Verificou-se que cerca de 78% (28) das metas estabelecidas foram atingidas, sendo que, nas restantes atividades, cerca de 22% (8), se verificaram desvios por defeito (5) e por excesso (3).

Estes indicadores mostram que cerca de 86% das atividades de cooperação atingiram ou superaram as metas inicialmente estabelecidas.

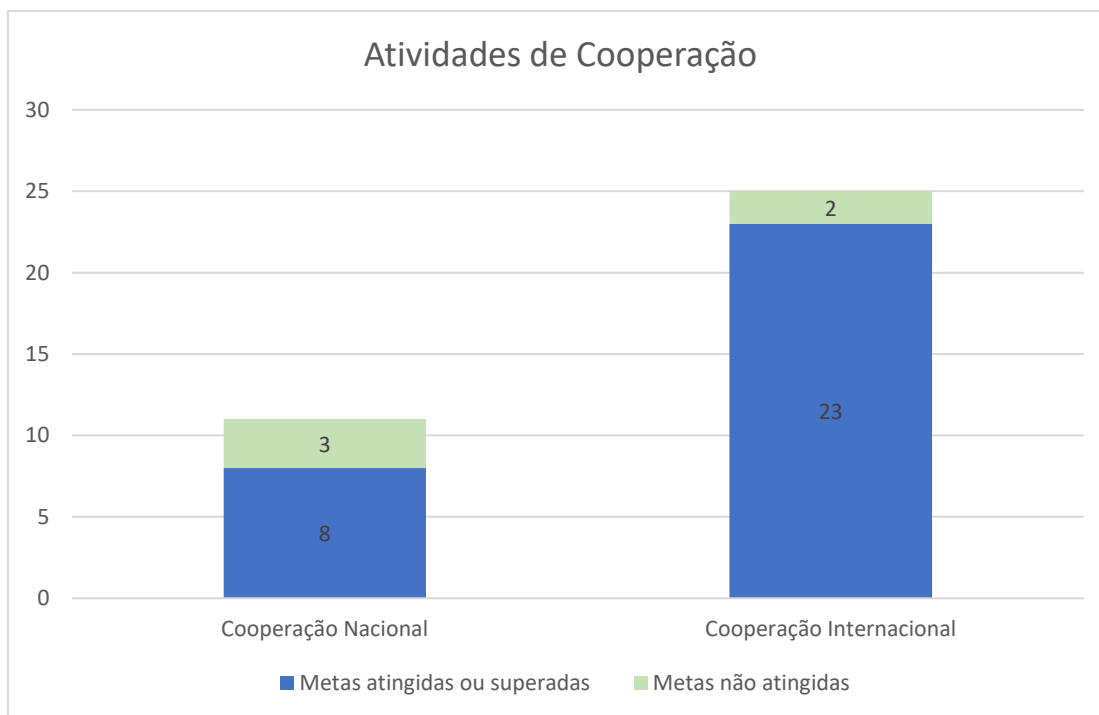


Gráfico 7 – Atividades de Cooperação desenvolvidas em 2019 no âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

- 17% do total das atividades desenvolvidas em 2019 tiveram uma natureza de cooperação nacional e internacional;
- 86% das atividades de cooperação atingiu ou superou as metas inicialmente estabelecidas;
- 14% das atividades de cooperação não atingiu as metas estabelecidas.

A tabela seguinte mostra uma matriz da natureza das atividades desenvolvidas em 2019 distribuídas por eixo de intervenção, assinalando as metas atingidas de acordo com o inicialmente estabelecido (“At”), das metas superadas ou antecipadas (“Sup/Ant”) e das metas que não atingidas (“N/At”).

| 2019 | | Eixo 1 | | | Eixo 2 | | | Eixo 3 | | | Eixo 4 | | | Eixo 5 | | | Eixo 6 | | |
|--|--|--------|-------------|------|--------|-------------|------|--------|-------------|------|--------|-------------|------|--------|-------------|------|--------|-------------|------|
| Natureza | Foco | At | Sup/ Ant | N/At | At | Sup/ Ant | N/At | At | Sup/ Ant | N/At | At | Sup/ Ant | N/At | At | Sup/ Ant | N/At | At | Sup/ Ant | N/At |
| Estrutural | Decisão/Avaliação Estratégica Nacional e Regional | 2 | | 1 | 1 | | 1 | 1 | | | | | | | | | | | |
| | Formação/Sensibilização Cidadãos | | | | 3 | 7 | 1 | | | | | | 1 | | | | | | |
| | Formação/Sensibilização Recursos Humanos | | | | 13 | 4 | 6 | | | | | | | | | | | | |
| Capacitação Humana | Formação/Sensibilização Especialistas | | | | 3 | 1 | 1 | | 1 | | | | | | | | | | |
| | Formação/Sensibilização Decisores | | | | 4 | 6 | | | | | | | | | | | | | |
| | Conteúdos Formação/Sensibilização | | | | 12 | 2 | 2 | | | | | | | | | | | | |
| | Outras Ações para Formação/Sensibilização | | | | 2 | | | | | | | | | | | | | | |
| Capacitação Organizacional e Tecnológica | Gestão de Cibersegurança | | | | 2 | | | 14 | 3 | 3 | | | | | | 1 | | | |
| Organizacional e Tecnológica | Exercícios e Operações de Cibersegurança | | | | 3 | | | 14 | 1 | 1 | 2 | | | 2 | | | 10 | 5 | 1 |
| | Identificação, Contratação e Retenção de Profissionais | | | 1 | 1 | | 1 | | | 1 | | | | | | | | | |
| Conhecimento e Partilha Informação | Promoção do Conhecimento | 2 | | | 5 | 1 | 2 | | | | 4 | | | | | | 1 | | |
| | Investigação, Desenvolvimento e Inovação | | | | | | | | | | | | 3 | 1 | | | | | |
| | Partilha de Informação (operacional) | | | | 1 | 1 | | 1 | | 1 | 2 | | 2 | | | | | | |
| | Estruturas de Governação (sectorial) | | 1 | | | | | 1 | | | | | | | | | | | |
| Cooperação | Cooperação Nacional | 1 | | 2 | | | 1 | | | | | | | 1 | 2 | | 3 | 1 | |
| | Cooperação Internacional | 2 | | 1 | | | | | | | 1 | | | 1 | | | 19 | | 1 |

Tabela 7 – Distribuição da natureza das atividades desenvolvidas pelos eixos de intervenção da Estratégia Nacional de Segurança do Ciberespaço

5. Conclusões

Da análise realizada, resulta um conjunto de observações que poderão constituir, para além de uma visão sobre o grau de execução do plano de ação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 neste seu primeiro ano de vigência, também algumas pistas para trabalho futuro. Desde logo destaca-se o facto de, em 2019, terem sido desenvolvidas (206) mais atividades do que aquelas que estavam inicialmente programadas (189), envolvendo 32 organismos de 14 áreas de governação e ainda dois organismos provenientes da chamada sociedade civil. Os resultados mostram que cerca de 85% (175) das atividades desenvolvidas atingiu ou superou as metas inicialmente estabelecidas e que cerca de 15% (31) não conseguiram atingir as metas que se propunham alcançar.

Se os dados mostram que foi nas atividades de natureza estrutural que se verificou a maior percentagem de desvios (33%), também mostram que nas restantes vertentes a sua execução se manteve acima dos 80%: capacitação humana com 86%, capacitação organizacional e tecnológica com 86%, conhecimento e partilha de informação com 83% e cooperação com 86%.

São as atividades com uma natureza de capacitação humana e de capacitação organizacional e tecnológica que maior peso têm no plano de ação posto em execução durante 2019, com 33% e 32% respetivamente. No entanto, importa destacar que é no âmbito da formação e sensibilização de recursos humanos que se identifica a maior percentagem de metas não atingidas (26%). Verificou-se ainda que, pelos resultados recolhidos, cerca de 275 654 pessoas terão tido conhecimento da existência de ações focadas na formação e sensibilização em cibersegurança. Todavia, apenas 49% (135 364) terão beneficiado, na prática, dessas ações.

No que respeita a atividades com uma natureza de cooperação, releva-se a predominância das focadas na cooperação internacional, representando cerca de 69% do total de atividades de cooperação e 74% das metas atingidas ou superadas destas atividades.

Tendo em conta o horizonte temporal de cinco anos que abrange a execução da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, poder-se-á compreender que em 2019 não tenham sido consideradas atividades em 10 linhas de ação (três no eixo de intervenção 1, três no eixo de intervenção 2, duas no eixo de intervenção 4, uma no eixo de intervenção 5 e uma no eixo de intervenção 6). Este fato será considerado nos momentos de preparação dos planos de ação para biénios subsequentes e respetivos momentos de avaliação. Por outro lado, importa reforçar as atividades dentro de outras linhas de ação com vista a alcançar os objetivos inscritos na Estratégia Nacional de Segurança do Ciberespaço 2019-2023. Importa, assim, procurar fomentar uma maior aposta em atividades que:

- Promovam a utilização dos fundos estruturais e outros instrumentos de financiamento para as diferentes linhas de ação constantes da Estratégia;
- Visem o aumento das competências avançadas em Cibersegurança por via do Ensino Profissional e do Ensino Superior;
- Visem a requalificação e formação especializada do maior número de profissionais possível para responder à evidente falta de recursos qualificados nesta área;
- Visem um incremento da sensibilização de decisores, públicos e privados, para as necessidades de cibersegurança;
- Visem a sensibilização e a formação de cidadãos para a utilização segura e informada dos ambientes digitais, tanto em contextos pessoais como profissionais, para além da Administração Pública;
- Visem a criação de sinergias com o tecido económico, designadamente através das atividades contempladas no Plano de Ação para a Transição Digital, identificando iniciativas que não só sirvam para o setor público, em matéria de oferta e procura, como possam criar sinergias com claras vantagens de interesse público;
- Promovam a resiliência digital em suporte à transformação digital das PMEs;
- Promovam efetivamente a criação de estruturas setoriais de governação da Cibersegurança que assegurem uma visão coerente e alinhada com todos os eixos da ENSC.