Por determinação de Sua Excelência o Presidente da A.R.,

1. À 1.ª Comissão;
2. c/c aos GPs, DURPs e Deputada não inscrita;
3. Acusar a receção e informar encaminhamento.

11.05.2020

REPÚBLICA PORTUGUESA

GABINETE DO SECRETÁRIO DE ESTADO DOS ASSUNTOS PARLAMENTARES

Exma. Senhora
Chefe do Gabinete de Sua Excelência o
Presidente da Assembleia da República
Dra. Maria José Ribeiro

SUA REFERÊNCIA	SUA COMUNICAÇÃO DE	NOSSA REFERÊNCIA	DATA
		Nº: 1625 ENT.: 2383 PROC. Nº:	11/05/2020

ASSUNTO: Relatório de avaliação da execução da Estratégia Nacional de Segurança do Ciberespaço relativo ao ano de 2019

Encarrega-me o Secretário de Estado dos Assuntos Parlamentares de junto enviar a V. Exa. cópia do ofício n.º 139/MPCM/2020, datado de 11 de maio, do Gabinete da Senhora Ministra de Estado e da Presidência e respetivo anexo, nos termos do disposto no artigo 6.º, n.º 2 da Lei n.º 46/2018, de 13 de agosto.

Com os melhores cumprimentos,

A Chefe do Gabinete

Catarina Gamboa

Dê-se conhecimento aos Deputados.
20.5.28

Assembleia da República
Gabinete do Presidente

N.º de Entrada: 655570
Classificação: 06.02.03
Data: 11.05.2020

ASSEMBLEIA DA REPÚBLICA
Divisão de Apoio às Comissões
CACDLG
N.º Único 655570
Entrada/Saída nº 394 Data: 12/05/2020

Gabinete do Secretário de Estado dos Assuntos Parlamentares
Palácio de São Bento, 1249-068 Lisboa, PORTUGAL
TEL + 351 213 920 500/06 FAX +351 213 920 515 EMAIL gabinete.seap@pm.gov.pt www.portugal.gov.pt

REPÚBLICA PORTUGUESA

GABINETE DA MINISTRA DE ESTADO E DA PRESIDÊNCIA

Exma. Senhora
Chefe do Gabinete do
Secretário de Estado dos Assuntos
Parlamentares
Palácio de São Bento (AR)

SUA REFERÊNCIA	SUA COMUNICAÇÃO DE	NOSSA REFERÊNCIA	DATA
		Nº: 139/MPCM/2020	11/05/2020

Assunto: Entrega à Assembleia da República do Relatório de Avaliação da Execução da Estratégia Nacional de Segurança no Ciberespaço relativo ao ano de 2019

Nos termos do artigo 6.º, n.º 2, da lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, encarrega-me a Senhora Ministra de Estado e da Presidência de enviar a V. Exa. o Relatório de Avaliação da Execução da Estratégia Nacional de Segurança do Ciberespaço relativo ao ano de 2019, para efeitos de entrega à Assembleia da República.

Mais informamos que o relatório foi aprovado pelo Conselho Superior de Segurança no Ciberespaço, no dia 8 de maio de 2020.

Com os melhores cumprimentos,

O Chefe do Gabinete

Miguel Rodrigues Cabrita

Anexo: o referido

Gabinete da Ministra de Estado e da Presidência
Rua Prof. Gomes Teixeira, 2 8º 1399-022 Lisboa, PORTUGAL
TEL + 351 213 927 600 EMAIL gabinete.mpcm@mpcm.gov.pt www.portugal.gov.pt

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. Constata-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 anteprojeto 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 temos 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.

Eixos da Estratégia Nacional de Segurança do Ciberespaço	**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.

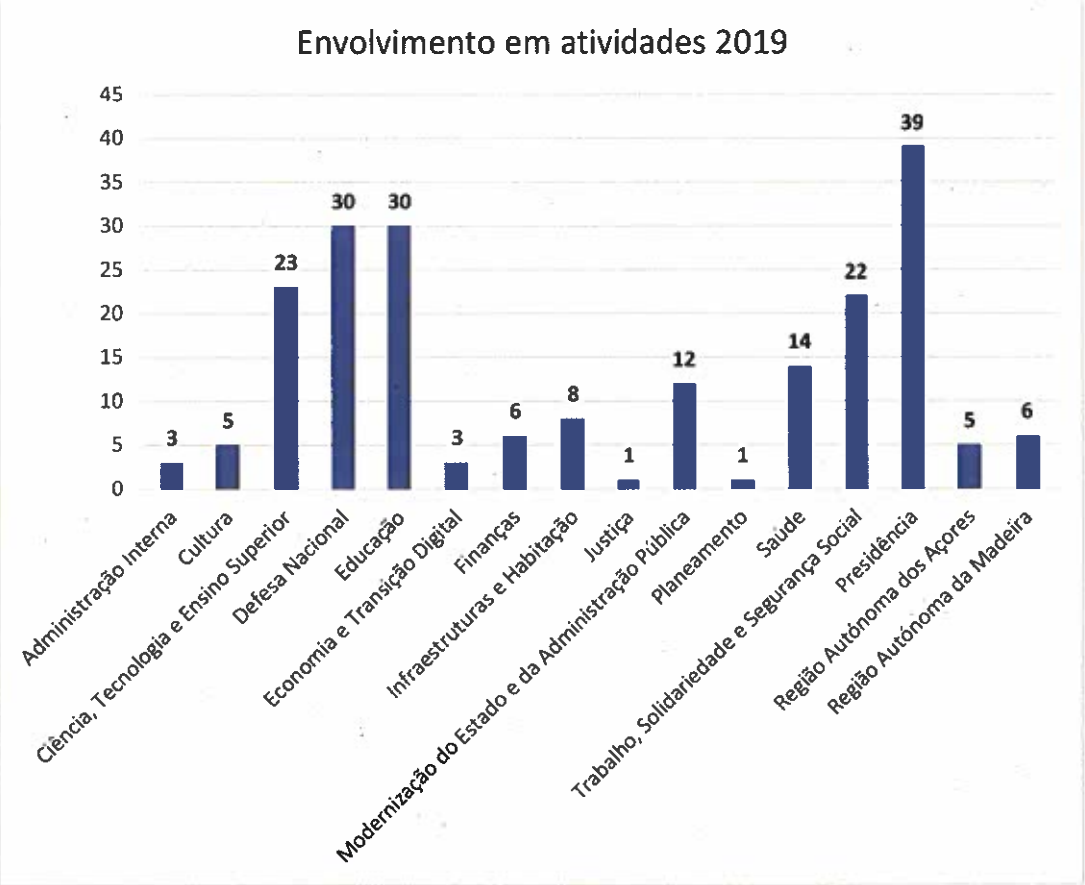

Gráfico 1 – Envolvimento das Áreas de Governo e Regiões Autónomas nas atividades desenvolvidas em 2019

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).

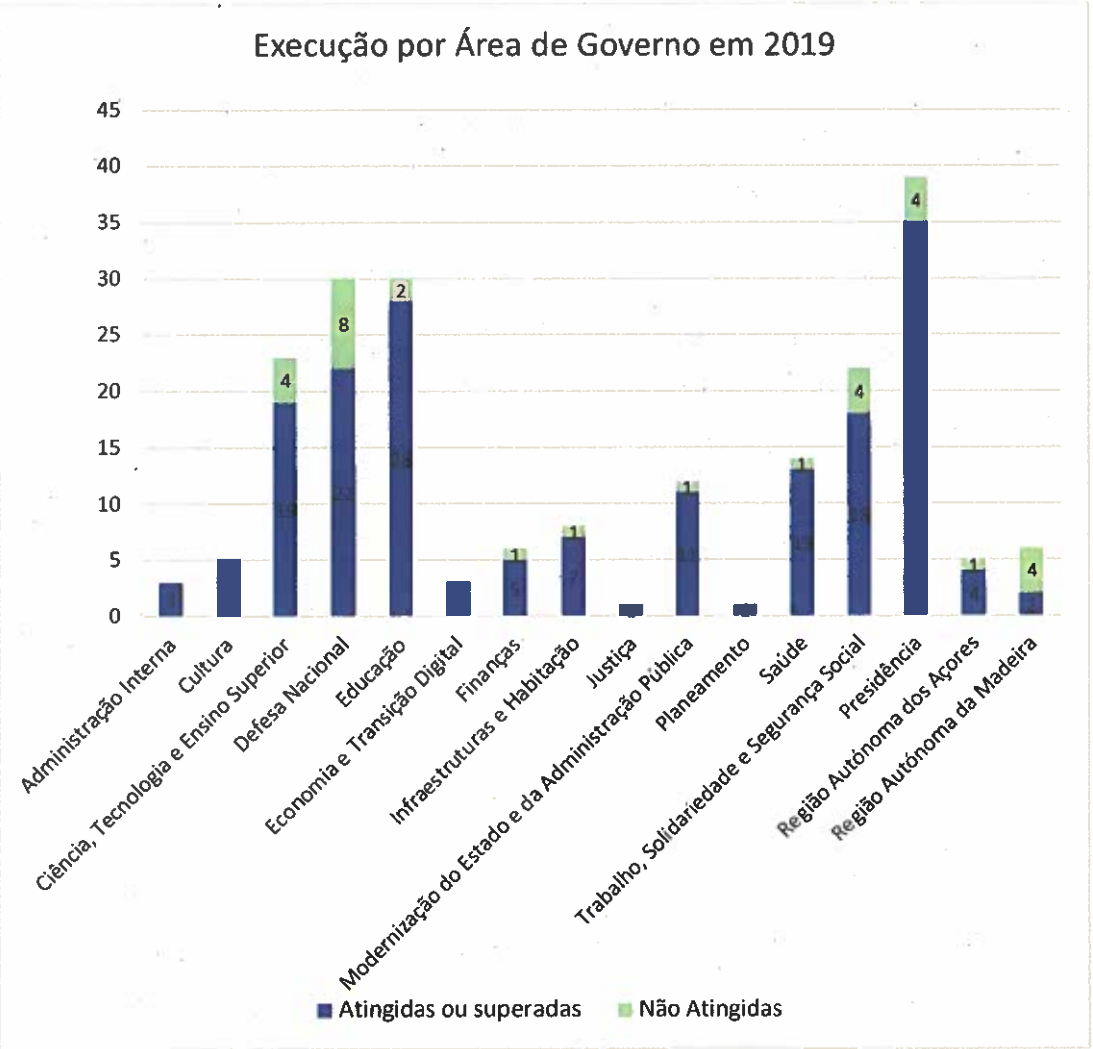

Gráfico 2 – Metas atingidas ou superadas e metas não atingidas por Área de Governo e Regiões Autónomas em 2019

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

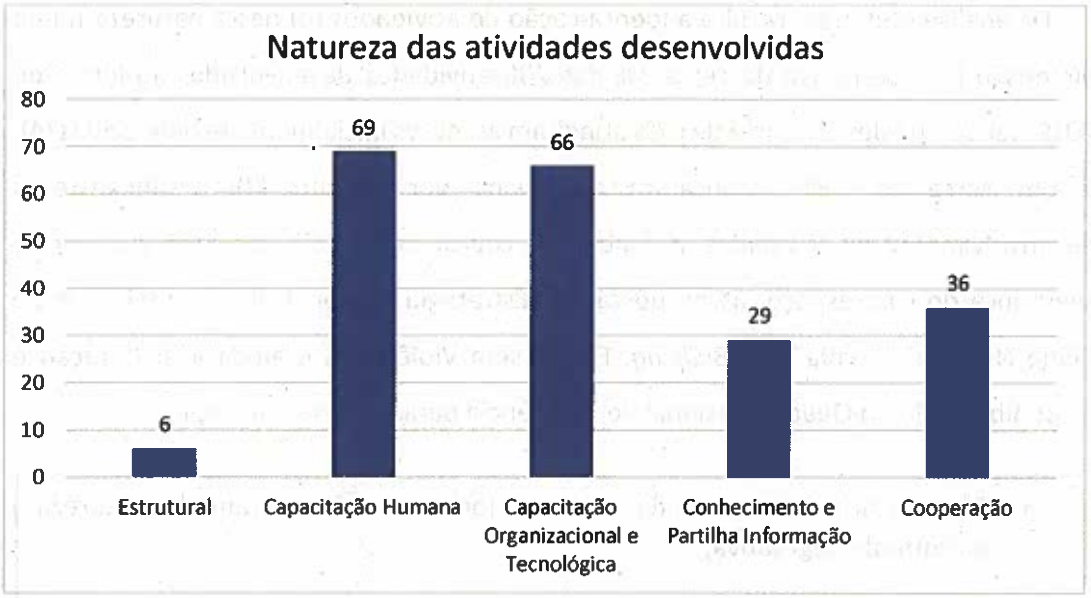

Gráfico 3 – Natureza das atividades desenvolvidas em 2019 no âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

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 caráter 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 CTF[2] 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.

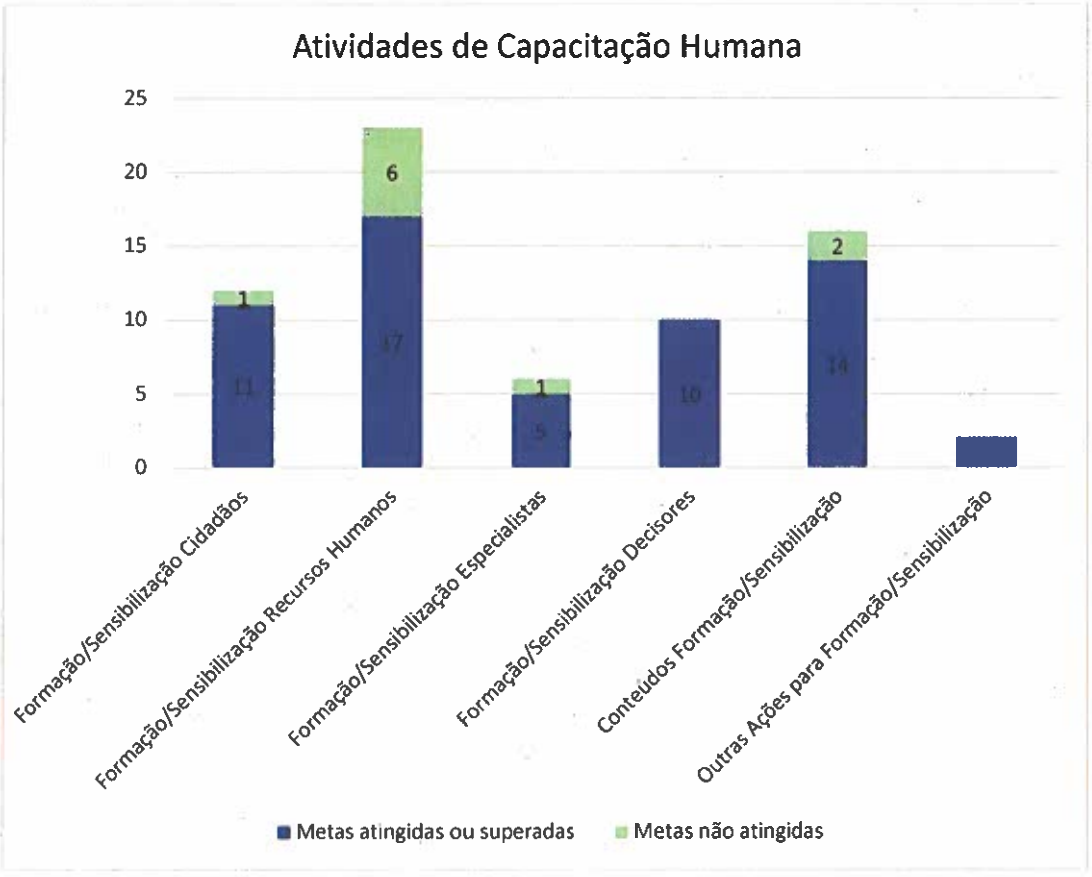

Gráfico 4 – Atividades de Capacitação Humana desenvolvidas em 2019 no âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

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 estes 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 cibersefesa 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 Segurança[5] 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.

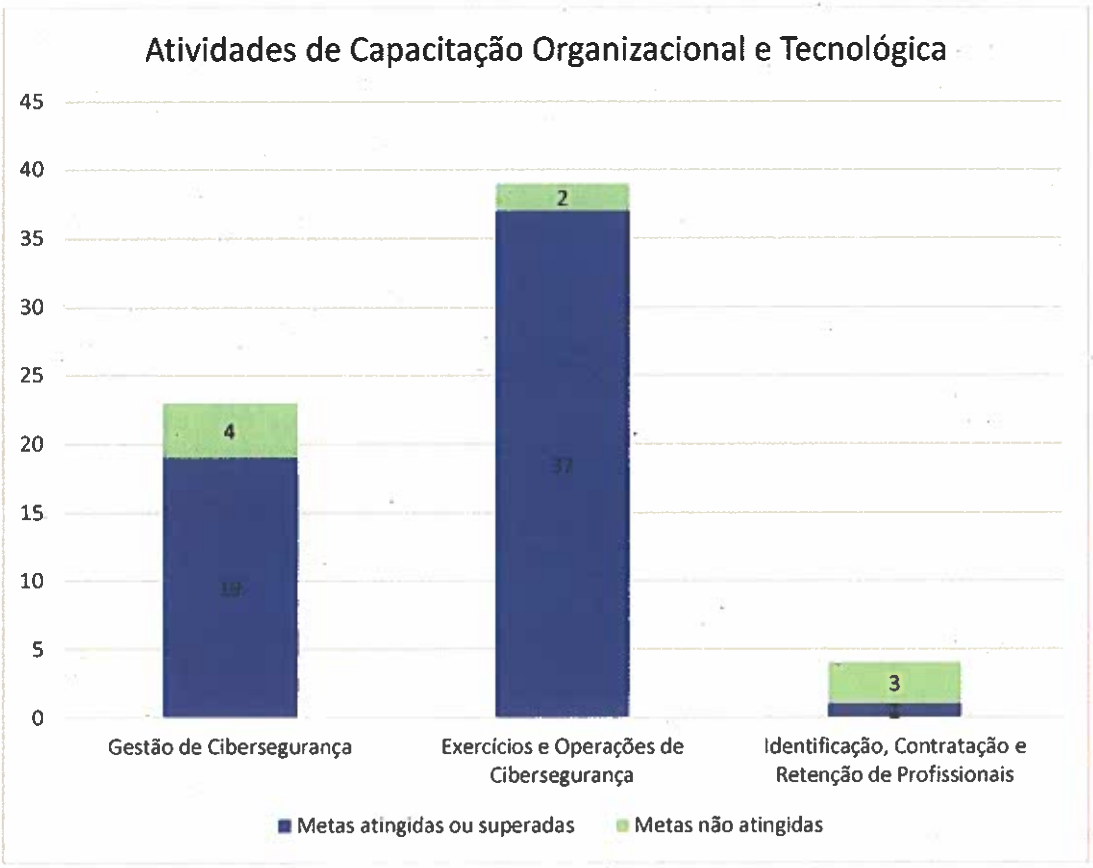

Gráfico 5 – Atividades de Capacitação Organizacional e Tecnológica desenvolvidas em 2019 no âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

- 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 caráter mais transversal, de participações na qualidade de formador ou docente, ou produção de documentação que, não tendo um caráter 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 Informação[6]. 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%.

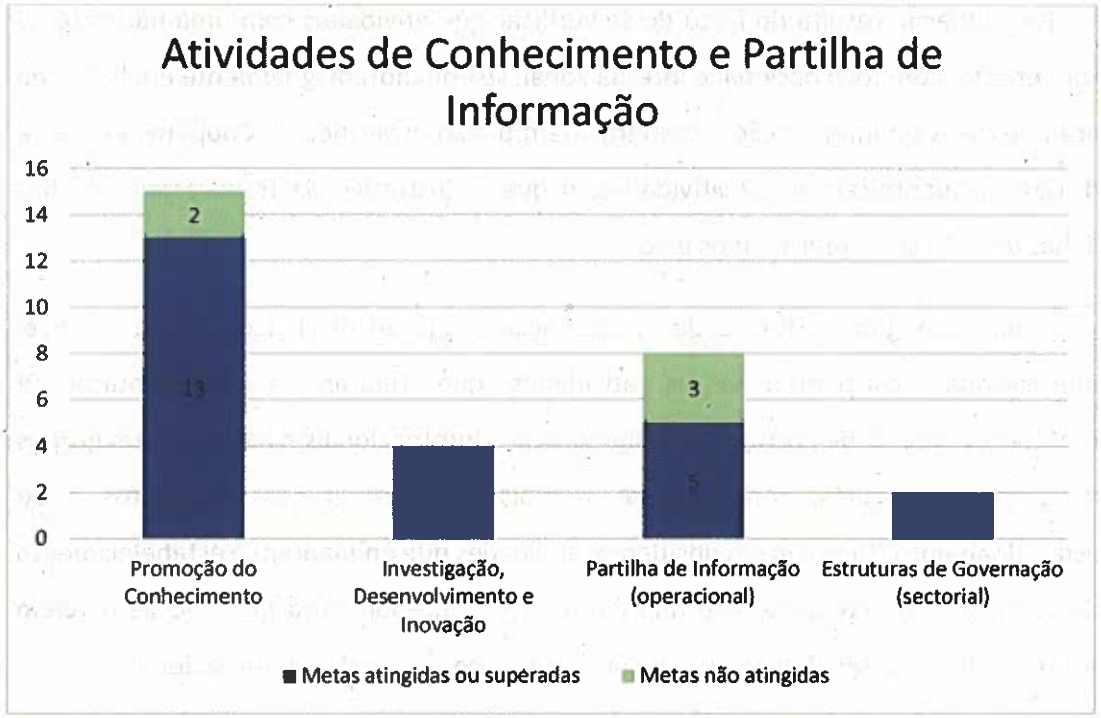

Gráfico 6 – Atividades de Conhecimento e Partilha de Informação desenvolvidas em 2019 no âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

- **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.

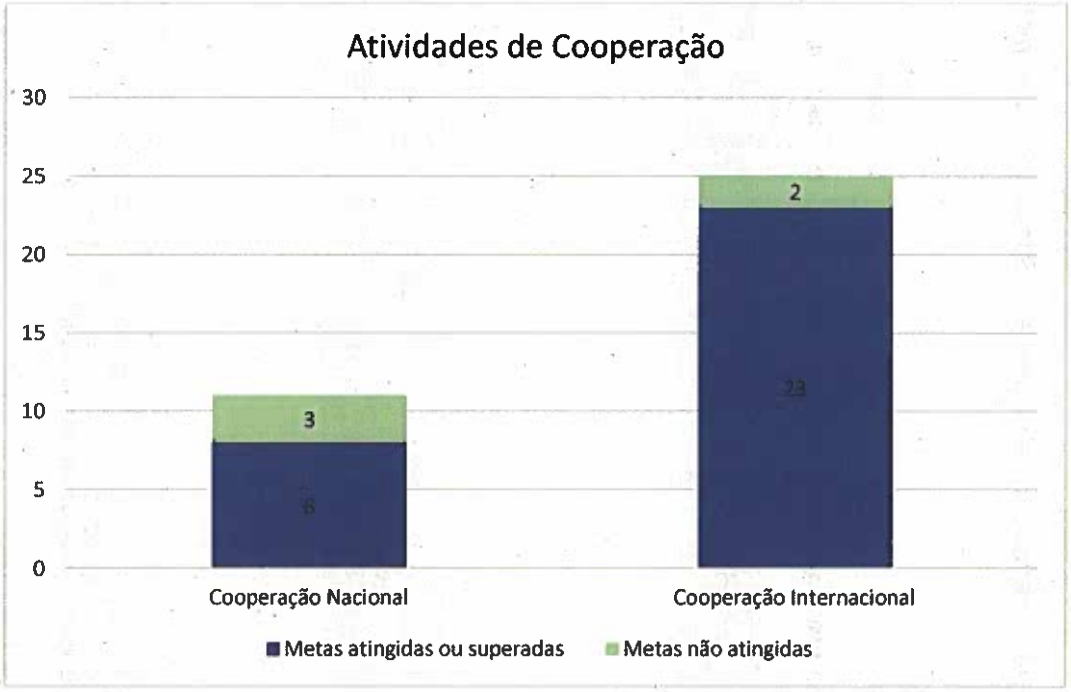

Gráfico 7 – Atividades de Cooperação desenvolvidas em 2019 no âmbito da Estratégia Nacional de Segurança do Ciberespaço 2019-2023

- 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											
Capacitação Humano	Formação/Sensibilização Cidadãos				3	7	1							1					
	Formação/Sensibilização Recursos Humanos				13	4	6												
	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			
	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.

Eixo 1 — Estrutura de segurança do ciberespaço															
EnLA#	Linhas de Ação	EnLAMAD#	Domínio	Obj Estr.	Atividades a desenvolver	Período execução		Entidade responsável	Indicador	Meta (bianual)		Resultados			Obs.
						Início	Fim			2019	2020	2019	Desvio 2019	2020	
E1LA1	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;	E1LA1AD2	EL - DAENR	OE1	Realizar reuniões de coordenação político-estratégica para a segurança do ciberespaço	01/01/2019	31/12/2023	CSSC	Nº de reuniões	4	4	1	Com Desvio		Por razões de agenda e calendário legislativo só se realizou uma reunião do CSSC
		E1LA1AD3	EL - DAENR	OE1	Elaborar relatório anual de avaliação de avaliação da execução da ENSC	01/01/2019	31/12/2023	CSSC	Elaborado/não Elaborado	Elaborado	Elaborado	Elaborado	Executada		Elaborado relatório de execução da ENSC 2015-2018
E1LA2	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;	E1LA2AD1	C - CI	OE1	Participar como autoridade nacional competente e ponto de contacto único nacional para a segurança das redes e dos sistemas de informação no âmbito da Diretiva (EU) 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 da informação em toda a União	01/01/2019	31/12/2023	PCM/CNCS	Participa/não Participa	Participa	Participa	Participa	Executada		
E1LA3	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;	E1LA3AD1	EL - DAENR	OE1	Elaborar proposta de Estratégia Nacional de Ciberdefesa.	01/01/2019	31/12/2019	MDN/EMGFA/CCD	Elaborado/não Elaborado	Elaborado		Elaborado	Executada		- Documento de proposta de estratégia Nacional de Ciberdefesa elaborado e aprovado em CCEM. - Documento enviado pelo GABCEMGFA ao GABMDN
		E1LA3AD4	C - CI	OE1	Participar como líder em iniciativas internacionais na área da ciberdefesa.	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de iniciativas	2	1	2	Executada		- Liderança da área de treino de Ciberdefesa no exercício NATO CWIX20 - Liderança do projeto Smart Defense MN CD E&T
		E1LA3AD5	COT - ICRP	OE3	Prover os recursos humanos adequados às necessidades estruturais da capacidade de Ciberdefesa.	01/01/2019	31/12/2021	MDN/EMGFA/CCD	Nº de Recursos Humanos total	30	60	24	Com Desvio		- À data de 31-12-2019 o CCD conta com um efetivo de 24 elementos dos três Ramos das FFAA
E1LA4	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;	E1LA4AD1	C - CN	OE1	Participação do Serviço Regional de Proteção Civil num exercício anual de cibersegurança	01/01/2019	31/12/2020	RAM - GR/VP, RAM - GR/SRS, RAM - GR/SRPC	Participa/não Participa	Participa	Participa	Participa	Executada		

E1LA6	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;	E1LA6AD1	C - CI	OE1	Estabelecer protocolos de colaboração e interações com as Forças Armadas e outras entidades internacionais	01/01/2019	31/12/2023	MDN/SG	Nº de protocolos	2	3	1	Com Desvio	
		E1LA6AD2	CPI - PC	OE1	Realizar workshops com vista à troca de experiência MAI e COSI (Centro de Operações de Segurança da Informação)	01/01/2019	31/12/2020	MAI/SG	Nº entidades participantes	1	3	1	Executada	
E1LA11	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;	E1LA11AD1	C - CN	OE1	Estabelecer novos âmbitos de colaboração e interação no protocolo estabelecido entre o Centro Nacional de Cibersegurança e o RCTS CERT	01/01/2019	31/12/2019	MCTES/FCT	Estabelecido/não Estabelecido	Estabelecido		Não Estabelecido	Com Desvio	
E1LA12	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;	E1LA12AD1	CPI - PC	OE1	Realização encontros no âmbito do fórum "Rede Académica CSIRT"	01/01/2019	31/12/2020	MCTES/FCT	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	
		E1LA12AD2	CPI - EG	OE1	Concretizar o papel e os objetivos da estrutura de comando e controlo de riscos de cibersegurança na Saúde	01/01/2019	31/12/2020	MS/SPMS	Concretizado/não Concretizado		Concretizado	Concretizado	Com Desvio	[CONCRETIZADO] Neste âmbito começou-se a fazer algum trabalho em 2019, esperando-se que seja concretizado em pleno em 2020 com a consolidação da equipa interna SPMS (Estrutura governativa e CSIRT SPMS). Em 2019 a SPMS emanou orientações para que todo o universo de entidades MS/SNS adotasse uma estrutura governativa de segurança da informação/cibersegurança - Comité de Risco e Segurança da Informação (CRSI). Estas estruturas visam, através de constituição de uma estrutura multidisciplinar com a participação de um elemento do CA/CD garantir a aplicação das boas práticas pelas diversas estruturas internas, assim como definir e gerir o risco e iniciativas associadas a segurança da informação na organização.

E1LA13	Incrementar a interoperabilidade no seio das estruturas, designadamente através do desenvolvimento e aprofundamento da taxonomia e dos procedimentos existentes;	E1LA13AD1	C- CN	OE1	Participar em grupos de trabalho estratégicos e técnicos na temática de cibersegurança	01/01/2019	31/12/2023	MDN/SG	Nº reuniões participadas	14	20	12	Com Desvio

Eixo 2 — Prevenção, educação e sensibilização															
EnLAS	Linhas de Ação	EnLASAD#	Domínio	Obj Estr.	Atividades a desenvolver	Período execução		Entidade responsável	Indicador	Meta (bianual)		Resultados			Obs.
						Início	Fim			2019	2020	2019	Desvio 2019	2020	
E2LA1	Reforçar os meios de recolha e processamento de informação e as capacidades de análise;	E2LA1AD1	CPI - PI	OE1	Melhorar a qualidade da informação tratada pelo SIEM do CEGER (reduzindo falsos positivos, agregando LOGS de forma mais eficaz, reduzindo o tempo de análise das ameaças), incluindo a informação partilhada com o GNS/CNCS para o Quadro Situacional Agregado de Cibersegurança, no âmbito do Projeto PANORAMA.	01/01/2019	31/12/2019	PCM/CEGER	Nº de sistemas com melhorias implementadas	1	1	1	Executada		Durante o ano de 2019, para além do trabalho diário de análise e identificação de falsos positivos, foram efetuadas no SIEM do CEGER diversas melhorias tal como: - Revisão de log sources; - Melhoria da qualida da informação de alguns logs (introdução/eliminação de campos); - Criação de dashboards personalizados para monitorização mais eficaz e permanente. Relativamente ao Quadro Situacional Agregado de Cibersegurança, procedeu-se à: - Instalação e configuração do IntelMQ para recolha e envio de informação do CEGER; - Definição e configuração do CMDB do CEGER no Quadro Situacional.
		E2LA1AD2	CPI - PI	OE1	Alargar o número de fontes de informação para o PANORAMA	01/01/2019	31/12/2023	PCM/CNCS	Nº total de fontes de informação	70	80	84	Com Desvio		
E2LA4	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»,	E2LA4AD1	CPI - PC	OE1	Participar como formador e/ou orador em ações de formação, palestras e sessões de esclarecimento interno e externo, favorecendo o aumento da partilha de conhecimentos e a consciencialização da sociedade.	01/01/2019	31/12/2023	MDN/SG	Nº de participações	10	14	6	Com Desvio		
E2LA5	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;	E2LA5AD1	CH - CFS	OE1	Disponibilizar website no âmbito da comemoração do Dia da Internet Mais Segura onde as escolas georreferenciam as suas atividades	01/01/2019	31/12/2023	ME/DGE	Disponibilizado /não Disponibilizado	Disponibilizado	Disponibilizado	Disponibilizado	Executada		400 registos de escolas/Agrupamentos fizeram o registo na página da campanha Dia da Internet Mais Segura 2019 nas Escolas do Centro de Sensibilização SeguraNet, da responsabilidade da DGE. 250 sessões de sensibilização foram promovidas nas Escolas pelos 10 Centros de Competência TIC, embaixadores DGE e embaixadores SeguraNet(nas regiões autónomas da Madeira e Açores), alcançando cerca de 15 000 participantes entre alunos, pais, professores, assistentes operacionais, entre outros
		E2LA5AD2	CH - FSC	OE1	Realizar sessões de sensibilização de cidadania digital nas escolas	01/01/2019	31/12/2023	ME/DGE	Nº de sessões de sensibilização	200	200	250	Com Desvio		
		E2LA5AD4	CH - FSC	OE1	Organizar sessões sensibilização sobre segurança digital no Dia da Defesa Nacional	01/01/2019	31/12/2023	ME/DGE	Nº de sessões de sensibilização	100	100	0	Com Desvio		Como indicador complementar, em momento de reporte pode indicar também "Nº de pessoas alcançadas"

	E2LASAD5	CH - FSC	OE1	Organizar concurso "Desafios SeguraNet" destinado a alunos, do 1.º, 2.º, 3.º Ciclos, pais e professores com o objetivo de sensibilizar para as questões da cidadnia digital e de educação para os média, incluindo cibersegurança.	01/01/2019	31/12/2020	ME/DGE	Nº de pessoas alcançadas	40000	40000	45000	Com Desvio	
	E2LASAD6	CH - OAFS	OE1	Propor junto da comunidade escolar a organização de ações de sensibilização com recurso a Líderes Digitais (incluindo ações de sensibilização, recursos multimédia e comunicação social local, atividades pedagógicas, etc.)	01/01/2019	31/12/2020	ME/DGE	Proposto/não Proposto	Proposto	Proposto	Proposto	Executada	900 Líderes Digitais dinamizaram inicitivas de sensibilização alcançando cerca de 25 000 participantes.
	E2LASAD7	CH - CFS	OE1	Divulgar as linhas de apoio "Alerta" e "Internet segura" junto da comunidade escolar	01/01/2019	31/12/2023	ME/DGE	Divulgado/não Divulgado	Divulgado	Divulgado	Divulgado	Executada	
	E2LASAD8	CH - FSC	OE1	Envolver jovens na participação em forums internacionais no âmbito da Cidadnia Digital, incluindo a cibersegurança.	01/01/2019	31/12/2023	ME/DGE	Nº de jovens envolvidos	3	3	3	Executada	
	E2LASAD9	CH - FSC	OE1	Disseminar a iniciativa Selo de Segurança Digital (eSafety Label) da União Europeia junto das escolas, incluindo o apoio ao preenchimento do questionário e sensibilização para o cumprimento de requisitos necessários para a sua obtenção.	01/01/2019	31/12/2023	ME/DGE	Disseminado/não Disseminado	Disseminado	Disseminado	Disseminado	Executada	Como indicador complementar, em momento de reporte pode indicar também "Nº de selos obtidos"
	E2LASAD10	CH - CFS	OE1	Desenvolver recursos educativos digitais para a promoção da cidadania digital nas escolas	01/01/2019	31/12/2023	ME/DGE	Desenvolvido/não Desenvolvido	Desenvolvido	Desenvolvido	Desenvolvido	Executada	Como indicador complementar, em momento de reporte pode indicar também "Nº de recursos desenvolvidos"
	E2LASAD11	CH - CFS	OE1	Disponibilizar jogo de tabuleiro sobre cidadania digital por todos os estabelecimentos do 1.º ciclo do ensino básico	01/01/2019	31/12/2019	ME/DGE	Disponibilizado /não Disponibilizado	Disponibilizado		não Disponibilizado	Com Desvio	
	E2LASAD14	CH - CFS	OE1	Disponibilizar website no âmbito da comemoração do Mês da Cibersegurança onde as escolas georreferenciam as suas atividades	01/01/2019	31/12/2023	ME/DGE	Disponibilizado /não Disponibilizado	Disponibilizado	Disponibilizado	Disponibilizado	Executada	Registaram-se na campanha 400 Escolas/Agrupamentos.
	E2LASAD15	CH - CFS	OE1	Disseminar junto das Escolas Portuguesas no estrangeiro atividades de Cidadania Digital e de Educação para os Media promovidas pela Direção-Geral da Educação	01/01/2019	31/12/2023	ME/DGE	Disseminado/não Disseminado	Disseminado	Disseminado	Disseminado	Executada	Encontram-se a colaborar nas iniciativas a Escola Portuguesa de Moçambique, Escola Portuguesa de Macau, Escola Portuguesa de São Tomé e Príncipe.
	E2LASAD16	CH - CFS	OE1	Participar como expositor em eventos de larga escala promovendo a componente de cibersegurança e cidadania digital	01/01/2019	31/12/2023	ME/DGE	Participa/não Participa	Participa	Participa	Participa	Executada	Participou no evento Altominho Digital Minds, Arco de Valdevez. Em três eventos de ribeira de encarnação.
	E2LASAD17	CH - CFS	OE1	Planear, Desenvolver e Implementar a atividade "Dia da Internet Mais Segura"/"Safer Internet Day", a nível nacional	01/01/2019	31/12/2021	Centro Internet Segura | MCTES/FCT	Implementado/ não Implementado	Implementado	Implementado	Implementado	Executada	Como indicador complementar, em momento de reporte pode indicar também o "Nº de sessões de sensibilização" e o "Nº de pessoas alcançadas"
	E2LASAD18	CH - FSC	OE1	Organizar e/ou colaborar na concretização de iniciativas de sensibilização dirigidas à Comunidades de Língua Portuguesa para uma utilização segura e responsável das tecnologias digitais	01/01/2019	31/12/2021	Centro Internet Segura | MCTES/FCT	Nº de iniciativas	1	2	1	Executada	Participação na Bienal de Jovens Criadores que teve lugar em Angola de 25 a 26 de julho, em parceria com o IPDJ.
	E2LASAD19	CH - CFS	OE1	Produzir novos recursos e conteúdos de sensibilização para uma utilização segura e responsável das tecnologias digitais	01/01/2019	31/12/2021	Centro Internet Segura | MCTES/FCT	Produzido/não Produzido	Produzido	Produzido	Produzido	Executada	Como indicador complementar, em momento de reporte pode indicar também "Nº de novos recursos e conteúdos produzidos"
	E2LASAD20	CH - FSC	OE1	Organizar ações de sensibilização (Roadshows) para uma utilização segura e responsável das tecnologias digitais dirigida a jovens excluídos, jovens universitários e seniores	01/01/2019	31/12/2021	Centro Internet Segura | MCTES/FCT	Nº de sessões de sensibilização	3	6	4	Com Desvio	Tendo em consideração o publico-alvo foram realizadas sessões de sensibilização dirigidas a públicos excluídos, Professores, Pais e Jovens
	E2LASAD21	CH - CFS	OE1	Assegurar a Divulgação da Linha Internet Segura, através da realização de campanhas promocionais.	01/01/2019	31/12/2021	Centro Internet Segura | MCTES/FCT, APAV	Divulgado/Não Divulgado	Divulgado	Divulgado	Divulgado	Executada	

		E2LA5AD22	CH - FSC	OE1	Criar curso de e-learning dirigido ao cidadão comum	01/01/2019	31/12/2023	PCM/CNCS	Nº de pessoas alcançadas	6000	6000	18546	Com Desvio	Dos 30430 inscritos, só estão considerados os formandos que extrairam o certificado de conclusão do curso
		E2LA5AD23	CH - CFS	OE1	Implementar website de sensibilização para o combate à desinformação (fake news)	01/01/2019	31/12/2023	MC/LUSA	Implementado/ não Implementado			Implementado	Com Desvio	(meta: 2023)
		E2LA5AD24	CH - FSC	OE1	Organizar eventos com o objetivo de sensibilizar a sociedade civil para o combate à desinformação (fake news)	01/01/2019	31/12/2023	MC/LUSA	Organizado/nã o Organizado			Organizado	Com Desvio	Como indicador complementar, em momento de reporte por indicar "Nº de pessoas alcançadas"
		E2LA5AD25	CH - CFS	OE1	Divulgar o Curso Cidadão Ciberseguro na RAM	01/01/2019	31/12/2020	RAM - GR/VP	Divulgado/não Divulgado	Divulgado	Divulgado	Não divulgado	Com Desvio	
		E2LA5AD26	CH - CFS	OE1	Realizar ações de comunicação interna e externa sobre as ameaças de phishing em geral e, em especial, divulgação à sociedade civil de ameaças específicas nesse domínio e ações a tomar pelos utilizadores	01/01/2020	31/12/2020	MF/AT	Realizado/não Realizado		Realizado	Realizado	Com Desvio	
E2LA6	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;	E2LA6AD1	CH - FSRH	OE1	Realizar ações de formação e awareness aos utilizadores da rede da Defesa	01/01/2019	31/12/2023	MDN/SG	Nº de ações	4	6	4	Executada	
		E2LA6AD3	CH - FSRH	OE1	Realizar ações de sensibilização através de programa de capacitação adequado a todo o universo do MS/SNS para profissionais da área da Saúde	01/01/2019	31/12/2023	MS/SPMS	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Durante 2019 as atividades concretizadas neste âmbito foram: - Disponibilização e respetiva gestão e acompanhamento do Curso online do Cidadão Ciberseguro a 57 entidades do MS/SNS com mais de 160 000 inscritos. - Dinamização de 2 Sessões para Comités de Risco e Segurança da Informação do MS/SNS para orientações sobre as responsabilidades e partilha de experiências após 6 meses da criação destas Estruturas Internas. Ainda no contexto de formação e ações de sensibilização sobre cibersegurança para profissionais da área da saúde, foram estabelecidos 2 protocolos pela SPMS (Ordem dos Farmacêuticos; e Universidade da Beira Interior (UBI) e as unidades de saúde hospitalares envolvidas na formação de médicos da Faculdade de Ciências da Saúde (FCS-UBI))
		E2LA6AD4	CH - FSC	OE1	Organizar sessões do programa de sensibilização em Cibersegurança para o cidadão comum e colaboradores de organizações dos setores público e privado	01/01/2019	31/12/2023	PCM/CNCS	Nº de pessoas alcançadas	2000	2000	8538	Com Desvio	Nº de sessões: 117 Considera formandos do CGC Não considera formação de dechores

		E2LA6AD7	CH - FSRH	OE1	Disponibilizar cursos de formação e ações desensibilização para colaboradores da AMA e de outras entidades da Administração Pública para conceitos, políticas e procedimentos de segurança de informação e literacia digital	01/01/2019	31/12/2020	MMEAP/AMA	Disponibilizado /não Disponibilizado	Disponibilizado	Disponibilizado	Disponibilizado	Executada	2 edições do curso online sobre segurança de informação. 1ª: edição para colaboradores internos: 233 colaboradores terminaram o curso de um total de 272; 2ª edição para colaboradores externos que se encontram a trabalhar na AMA: 25 conaboradores terminaram o curso de um total de 55 Cursos Literacia Digital: 1. Criação de Macros em Excel: 12 2. Mail Merge - Comunicação em Série: 7 Curso online sobre segurança da informação para todos os colaboradores internos e externos. Apresentação de sessão partilha AMA sobre Segurança na Internet 2 Cursos de literacia Digital para colaborador. s da AMA (Introdução à Criação de Macros em Excel e Mail Merge - Comunicação em Série)
E2LA7	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;	E2LA7AD1	CH - FSRH	OE1	Realizar ações de formação para professores com o objetivo de sensibilizar para a aplicação das orientações curriculares TIC para o primeiro ciclo que preconiza a obrigatoriedade da dinamização de atividades de cidadania digital.	01/01/2019	31/12/2023	ME/DGE	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Foram realizadas 72 formações alcançando 1400 participantes.
		E2LA7AD2	CH - FSRH	OE1	Realizar ações de formação para professores de informática para a aplicação das aprendizagens essenciais da disciplina TIC (5.º, 6.º, 7.º 8.º e 9.º anos) que preconiza a obrigatoriedade da dinamização de atividades de cidadania digital.	01/01/2019	31/12/2023	ME/DGE	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Foram dinamizadas 100 Ações de Curta Duração envolvendo cerca de 1000 professores.
		E2LA7AD3	CH - FSRH	OE1	Realizar ações de formação para professores para a aplicação na área da Cidadania e Desenvolvimento das questões de cidadania digital, cibersegurança e educação para os média (nos domínios Média; Segurança, Defesa e Paz; Saúde; Sexualidade; Prevenção Rodoviária e Direitos Humanos).	01/01/2019	31/12/2023	ME/DGE	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Foi realizada uma formação em Vila Franca de Xira que envolveu 30 professores.
		E2LA7AD4	CH - FSRH	OE1	Realizar ações de formação para professores no âmbito do projeto eTwinning (parcerias/colaboração entre escolas na União Europeia) que englobam questões relacionadas com Cidadania Digital, com objetivo da atribuição do selo de escola eTwinning que requer da escola candidata o cumprimento de um conjunto de iniciativas de sensibilização em segurança digital.	01/01/2019	31/12/2023	ME/DGE	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Realizado. Foram dinamizados 5 encontros regionais envolvendo 400 professores.
		E2LA7AD5	EL - DAENR	OE1	Elaborar proposta do Plano Nacional "Escola sem Bullying. Escola sem Violência" com a colaboração de diversas entidades da área governativa da Educação.	01/01/2019	31/12/2019	ME/DGE	Elaborado/não Elaborado	Elaborado		Elaborado	Executada	Elaborado. Encontram-se envolvidas neste plano mais de 100 Agrupamentos de Escolas.
E2LA8	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;	E2LA8AD2	CH - OAFS	OE1	Propor junto dos Centros de Formação de Associação de Escolas a organização de ações de formação no âmbito da Cidadania Digital	01/01/2019	31/12/2023	ME/DGE	Proposto/não Proposto	Proposto	Proposto	Proposto	Executada	Não dispomos informação do número de professores alcançados nestas formações
		E2LA8AD3	CH - FSRH	OE1	Realizar ações de formação para professores no âmbito da literacia para os média em colaboração com o Sindicato dos Jornalistas	01/01/2019	31/12/2023	ME/DGE	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Tendo sido envolvidos 40 professores.

		E2LA8AD4	CH - FSRH	OE1	Organizar o Encontro Nacional de Educação para os Média destinado a professores, com o objetivo de sensibilizar para a literacia mediática.	01/01/2019	31/12/2023	ME/DGE	Organizado/não Organizado	Organizado	Organizado	Organizado	Executada	Contando com 100 participantes entre alunos, professores e outros agentes educativos
		E2LA8AD5	CH - FSRH	OE1	Organizar o Encontro Nacional "Cidadania Digital nas Escolas" promovido pelo Centro de Sensibilização SeguraNet (DGE) destinado a professores, com o objetivo de sensibilizar para este domínio e reconhecimento de mérito de escolas.	01/01/2019	31/12/2023	ME/DGE	Organizado/não Organizado	Organizado	Organizado	Organizado	Executada	Contando com 200 participantes entre alunos, professores e outros agentes educativos
		E2LA8AD7	CH - CFS	OE1	Disseminar materiais e conteúdos de sensibilização para a cibersegurança a profissionais da área da Saúde e utentes	01/01/2019	31/12/2023	MS/SPMS	Disseminado/não Disseminado	Disseminado	Disseminado	Disseminado	Executada	Esta iniciativa será sempre de carácter contínuo. . Em 2019 foram disponibilizados pelos diversos canais vários materiais e conteúdos aos profissionais da área da Saúde associados às ações de sensibilização realizadas como Dicas sobre Cibersegurança. Foi também criado o Manual de Cibersegurança para Enfermeiros a disseminar em massa em 2020, juntamente com a criação e disponibilização de outros documentos associados a outras classes profissionais. . Orientado ao Utente, foram disseminadas, pelo menos, 2 boas práticas e campanhas diretamente relacionadas com o tema, através do Portal SNS/Área do Cidadão, referenciando a importância de uma autenticação robusta e segura através da Chave Móvel Digital e a promoção do Curso do Cidadão Ciberseguro. [+ de 1 450 000 cidadãos] . No contexto SPMS foram realizadas 2 simulações de phishing e lançado um Programa de Awareness e Sensibilização para a Cibersegurança na SPMS dirigido aos 851 colaboradores, tendo por base um processo de gamificação composto por vários desafios mensais [Taxa de participação de 80%]
		E2LA8AD8	CH - FSC	OE1	Realizar sessões de sensibilização junto de jovens em idade escolar	01/01/2019	31/12/2023	PCM/CNCS	Nº de pessoas alcançadas	1000	1000	2986	Com Desvio	
E2LA9	Incentivar a identificação de jovens com alto potencial para a área da cibersegurança e promover a sua integração atempada em contexto profissional;	E2LA9AD1	CPI - PC	OE3	Realizar estágios profissionais e académicos de alunos de escolas secundárias em cursos técnicos em contexto laboral	01/01/2019	31/12/2023	MDN/SG	Nº de estagiários	3	4	3	Executada	
		E2LA9AD2	COT - ICRP	OE3	Organizar CTFs dirigidos a jovens	01/01/2019	01/12/2020	MCTES/FCT	Nº de CTFs	1	1	0	Com Desvio	Como indicador complementar, em momento de reporte pode indicar também "Nº de pessoas alcançadas"
		E2LA9AD3	COT - ICRP	OE3	Organizar CTFs dirigidos a jovens	01/01/2019	31/12/2023	PCM/CNCS	Nº de CTFs	1	1	1	Executada	48 jovens participantes
E2LA12	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;	E2LA12AD1	CH - FSD	OE3	Frequentar ações de formação no âmbito da cibersegurança ao nível de decisão	01/01/2019	31/12/2023	MDN/SG	Nº de ações	4	10	4	Executada	
		E2LA12AD3	CH - FSD	OE3	Realizar ação de sensibilização para decisores sobre procedimentos a adoptar no que concerne à recolha, tratamento e conservação de dados pessoais e responsabilidades inerentes	01/10/2019	01/11/2019	MTSSS/CPL	Nº de pessoas alcançadas	35		35	Executada	

		E2LA12AD4	CH - FSD	OE3	Realizar seminários no âmbito do Programa de Capacitação de PME em Cibersegurança com o objetivo de informar os gestores e quadros das PME portuguesas sobre os riscos de um ciberataque e das suas consequências, na esfera do Memorando de Entendimento celebrado em 2018 entre o IAPMEI, I.P. e a Cisco International Limited.	01/01/2019	31/12/2020	METD/IAPMEI	Nº de pessoas alcançadas	75	75	149	Com Desvio	
		E2LA12AD5	CH - FSD	OE1	Realizar iniciativas conjuntas de sensibilização em Cibersegurança, dirigidas ao tecido empresarial, com o Centro Nacional de Cibersegurança.	01/01/2019	31/12/2020	METD/IAPMEI	Realizado/não Realizado		Realizado	Realizado	Com Desvio	Cooperação no Evento C-Days 2019.Sessão DGAE sobre resultados com a participação do CNCS
		E2LA12AD6	CH - FSD	OE1	Divulgar cursos gratuitos sobre cibersegurança, para empresários, através dos canais de comunicação do IAPMEI.	01/01/2019	31/12/2020	METD/IAPMEI	Divulgado/não Divulgado		Divulgado	Divulgado	Com Desvio	Divulgação e promoção do Curso Online de introdução à Cibersegurança da Cisco.
		E2LA12AD9	CH - FSD	OE3	Realizar ações de formação e sensibilização dirigida à estrutura diretiva da Saúde	01/01/2019	31/12/2023	MS/SPMS	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Entre Dezembro e Fevereiro 2020, foram promovidas as 10 Semanas de Cibersegurança, tendo uma das iniciativas sido uma Formação em Cibersegurança na Saúde para Altos Dirigentes, cujo público alvo foram elementos do Conselho de Administração e Conselho Diretivo. (82 participantes)
		E2LA12AD10	CH - FSD	OE3	Criar programa de sensibilização em Cibersegurança para decisores	01/01/2019	31/12/2023	PCM/CNCS	Nº de pessoas alcançadas	100	500	734	Com Desvio	Nº de sessões: 13
		E2LA12AD11	CH - FSD	OE3	Realizar ações de formação dirigida a dirigentes superiores e intermédios na área da sensibilização para as necessidades de cibersegurança	04/01/2020	30/9/2020	MCTES/DGES	Nº de pessoas alcançadas		7	7	Com Desvio	Realização de ação de sensibilização aos dirigentes por parte do CNCS
		E2LA12AD13	CH - FSD	OE3	Realizar ações de sensibilização dirigida a dirigentes superiores e intermédios para as necessidades de cibersegurança, no âmbito de programas internos de consciencialização de cibersegurança.	01/01/2019	31/12/2023	MIH/IP	Nº de pessoas alcançadas	100	200	122	Com Desvio	
		E2LA12AD14	CH - FSD	OE3	Realizar ações de formação dirigida a dirigentes superiores e intermédios na área da Cidadania Digital e da sensibilização para as necessidades de cibersegurança	01/01/2019	31/12/2023	ME/DGE	Nº de pessoas alcançadas	15	15	15	Executada	
E2LA13	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;	E2LA13AD1	CPI - PC	OE1	Organizar a Conferência Anual de Cibersegurança C-DAYS	01/01/2019	31/12/20123	PCM/CNCS	Organizado/não Organizado	Organizado	Organizado	Organizado	Executada	
		E2LA13AD2	CH - FSE	OE3	Participar em ações de formação/workshops com a equipa do Departamento de Segurança e Certificação Eletrónica nas áreas da cibersegurança e da certificação eletrónica.	01/01/2019	31/12/2020	PCM/CEGER	Nº de pessoas alcançadas	4	4	4	Executada	Foram diversos os temas abrangidos (Metodologias de investigação Científica/Lei do Cibercrime/Análise Forense Digital e Prova do Cibercrime/TRANSITS I/MASTERCLASS ISO 27001:2013, entre outros).
		E2LA13AD3	CH - FSE	OE3	Frequentar ações de formação no âmbito da cibersegurança aos nível técnico	01/01/2019	31/12/2023	MDN/SG	Nº de ações	8	12	4	Com Desvio	
		E2LA13AD4	CPI - PC	OE1	Participar em conferências de forma a consolidar conhecimento com outras entidades.	01/01/2019	31/12/2023	MDN/IASFA	Nº de pessoas alcançadas	1	2	1	Executada	
		E2LA13AD6	CH - FSE	OE3	Realizar ações de sensibilização para técnicos de informática do GRA no âmbito da cibersegurança	01/01/2019	31/12/2023	RAA - GR	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Nº de pessoas alcançadas: 50 profissionais
		E2LA13AD15	CH - FSRH	OE1	Realizar ações de sensibilização de carácter voluntário na temática de cibersegurança e segurança da informação a organismos do MTSSS	01/01/2019	31/12/2019	MTSSS/II	Nº de pessoas alcançadas	2000		.2500	Com Desvio	
		E2LA13AD19	CH - FSRH	OE1	Realizar ações de formação em cibersegurança para colaboradores	10/01/2019	31/12/2019	MCTES/DGES	Nº de pessoas alcançadas	80		60	Com Desvio	Promoção do curso Cidadão CiberSeguro em conjunto com o CNCS
		E2LA13AD27	CH - FSRH	OE1	Realizar ações de Sensibilização para a Cibersegurança para a Administração Pública Regional	01/01/2019	31/12/2020	RAM - GR/VP	Nº de pessoas alcançadas	600	5000	72	Com Desvio	

	E2LA13AD30	CH - FSE	OE3	Realizar formações técnicas de cibersegurança para as equipas técnicas das entidades de Saúde	01/01/2020	31/12/2023	MS/SPMS	Nº de pessoas alcançadas		50	82	Com Desvio	No âmbito das 10 Semanas de Cibersegurança, foram promovidas 3 edições de formação em Gestão de Segurança da Informação para os Responsáveis de Segurança e Diretores TIC do MS/SNS. (80 participantes) Além disso, a SPMS dinamizou 2 sessões técnicas sobre tratamento e resposta a incidentes de cibersegurança para os Responsáveis de Notificações Obrigatória de Incidentes (RNO) do universo MS/SNS. (52 Participantes)
	E2LA13AD31	CH - FSRH	OE1	Realizar ações de sensibilização para a cibersegurança	01/01/2019	31/12/2020	MCTES/FCT	Nº de pessoas alcançadas	50	50	60	Com Desvio	
	E2LA13AD32	CH - FSRH	OE3	Realizar ações de formação a colaboradores do CNCS	01/01/2019	31/12/2023	PCM/CNCS	Nº de pessoas alcançadas	15	22	25	Com Desvio	
	E2LA13AD33	CH - FSRH	OE1	Realizar ações de sensibilização interna sobre cibersegurança para colaboradores da LUSA	01/01/2019	31/12/2023	MC/LUSA	Nº de pessoas alcançadas	50	50	50	Executada	
	E2LA13AD36	CH - FSRH	OE1	Realizar ações de sensibilização para os colaboradores da eSPap com recurso ao "Curso Cidadão Ciberseguro" disponibilizado pelo CNCS	01/01/2019	31/12/2020	MF/eSPap	Nº de pessoas alcançadas	150	150	15	Com Desvio	Apenas foi possível efetuar 15 para técnicos. Iremos em 2020 dar formação integral a todos os colaboradores através do curso da plataforma do INA.
	E2LA13AD40	CH - FSRH	OE1	Realizar ações de sensibilização dirigida a colaboradores sobre cibersegurança, no âmbito de programas internos de consciencialização de cibersegurança.	01/01/2019	31/12/2023	MIH/IP	Nº de pessoas alcançadas	800	800	570	Com Desvio	
	E2LA13AD41	CH - CFS	OE1	Produzir recursos e conteúdos de sensibilização para uma utilização segura e responsável das tecnologias digitais pelos colaborados do Grupo IP.	01/01/2019	31/12/2023	MIH/IP	Produzido/não Produzido	Produzido	Produzido	Produzido	Executada	Publicação de guias de boas práticas, divulgação de apresentações e notícias em newsletter
	E2LA13AD44	CH - FSRH	OE1	Disponibilizar ações de sensibilização aos colaboradores da ADC com recurso ao "Curso Cidadão Ciberseguro" disponibilizado pelo CNCS	01/01/2019	31/12/2020	MP/ADC	Nº de pessoas alcançadas	10	40	215	Com Desvio	As ações de ensibilização forma dirigiadas internamente a todos os colaboradores da AD&C, através de canais internos (intranet e newsletters)
	E2LA13AD45	CH - FSRH	OE1	Realizar ações de formação para os colaboradores da DGE focadas na Cidadania Digital e na área da cibersegurança	01/01/2019	31/12/2023	ME/DGE	Nº de pessoas alcançadas	20	20	20	Executada	
	E2LA13AD46	CH - FSE	OE3	Realizar ações de sensibilização para técnicos de informática da DGE no âmbito da cibersegurança	01/01/2019	31/12/2023	ME/DGE	Nº de pessoas alcançadas	4	4	4	Executada	
	E2LA13AD47	CH - FSRH	OE1	Realizar ações de formação para todos os colaboradores do ACM no âmbito da cibersegurança e boas práticas informáticas	01/01/2019	31/12/2020	PCM/ACM	Nº de pessoas alcançadas	40	100	0	Com Desvio	Atendendo a que a definição da proposta e contributo do ACM,IP no âmbito desta estratégia foi concluída no último trimestre de 2019 e face a condicionantes de ordem interna e alheios ao Organismo, não foi possível assegurar a concretização das 40 ações pensadas para 2019, sendo que se assume o compromisso de concretização, em 2020, do total de 140 ações de formação no âmbito da Cibersegurança e Boas práticas, que já se encontram previstas em sede de Plano de Formação 2020, aprovado pelo Conselho Diretivo deste Instituto.

E2LA16	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;	E2LA16AD1	COT - EOC	OE1	Organizar exercícios e simulacros abrangendo todo o ecossistema da Saúde	01/01/2019	31/12/2023	MS/SPMS	Organizado/não Organizado	Organizado	Organizado	Organizado	Executada	A SPMS simulou com uma entidade de saúde a falência dos serviços centrais do Registo Nacional de Utentes (RNU), com impacto em serviços centrais como a prescrição de Exames Sem Papel e a Prescrição Médica Eletrónica. Além disso, internamente foram realizados 2 exercícios em sala de forma a simular a continuidade de serviço no caso de falência de sistemas clínicos hospitalares e de cuidados de saúde primários como o SONHO e SINUS.
		E2LA16AD2	COT - EOC	OE1	Organizar exercício anual de Cibersegurança	01/01/2019	31/12/2023	PCM/CNCS	Organizado/não Organizado	Organizado	Organizado	Organizado	Executada	
		E2LA16AD3	COT - EOC	OE1	Organização de exercícios regulares de planeamento, preparação e resposta às crises nacionais de cibersegurança com foco no âmbito do Grupo IP.	01/01/2019	31/12/2023	MIH/IP	Organizado/não Organizado	Organizado	Organizado	Organizado	Executada	Campanhas de phishing e participação em exercícios de cibersegurança
E2LA17	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;	E2LA17AD1	C - CN	OE3	Estabelecer protocolos de cooperação com entidades externas para a formação dos elementos afetos à capacidade de ciberdefesa.	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de protocolos	1	1	0	Com Desvio	- Desenvolvidos contactos com as entidades do G4 para a realização conjunta de ações de formação na área da análise forense. Estabelecidos os TOR
		E2LA17AD2	CH - FSRH	OE1	Realizar ações de sensibilização de campanhas de phishing nas redes e sistemas de informação das FFAA e Defesa	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de pessoas alcançadas	15000	20000	10000	Com Desvio	- Desenvolvidas campanhas de sensibilização para ataques de Phishing durante os exercícios Cyberdex e CiberPerseu com aproximadamente 10,000 pessoas alcançadas
		E2LA17AD4	CPI - PC	OE3	Dinamizar o intercâmbio de RH na área da educação e sensibilização.	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de intercâmbios	2	2	0	Com Desvio	- Face à apresentação tardia dos elementos de reforça da capacidade, não foi possível desenvolver os contactos necessários para estes intercâmbios em 2019

E2LA18	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;	E2LA18AD1	CH - FSRH	OE1	Realizar uma campanha anual de sensibilização para as temáticas do âmbito da cibersegurança (segurança de passwords, dados pessoais, trabalho remoto, correio eletrónico, entre outros...) a todos os utilizadores da Rede Informática do Governo.	01/01/2019	31/12/2010	PCM/CEGER	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	O CEGER promoveu uma campanha de awareness em 2019, que consistiu em dois simulacros de campanhas de phishing (um para assessment inicial e outro após a campanha de sensibilização para aferir eventual evolução). A campanha de sensibilização, que envolveu 2387 utilizadores, consistiu na divulgação semanal de 8 pequenos vídeos (1 conteúdo por semana), abordando os temas seguintes: a) Segurança de Passwords; b) Segurança em Dispositivo USB; c) Segurança na Internet; d) Introdução ao Regulamento Geral de Proteção de Dados (RGPD); e) RGPD - Dados sensíveis; f) Segurança no E-mail; g) Segurança no Posto de Trabalho; h) Segurança no Trabalho Remoto.
		E2LA18AD2	EL - DAENR	OE1	Propor temáticas para formação específica em Cibersegurança e Ciberdefesa, para funcionários públicos gerais e específica para a carreira informática, ao CEFAPA- Centro de Formação da Administração Pública dos Açores	01/01/2019	31/12/2019	RAA - GR	Proposto/não Proposto	Proposto		não Proposto	Com Desvio	Transitado para 2020, para que a proposta possa, caso seite pela entidade, fazer parte do Catálogo de formação do CEFAPA de 2021
		E2LA18AD3	CPI - PC	OE1	Realizar eventos direcionados para público específico, designados por CiberTalks do GRA, nomeadamente: juristas, gestores, informáticos, entre outros.	01/01/2019	31/12/2023	RAA - GR	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Nº de pessoas alcançadas: 150
		E2LA18AD4	CPI - PC	OE1	Realizar campanhas de phishing em instituições do Ensino Superior (a pedido destas), colmatadas com posterior sessão de sensibilização.	01/01/2019	31/12/2020	MCTES/FCT	Nº de campanhas realizadas	2	2	4	Com Desvio	Como indicador complementar, em momento de reporte pode indicar também "Nº de pessoas alcançadas" (em virtude das sessões de sensibilização posteriores)
		E2LA18AD5	CH - CFS	OE1	Divulgar o Curso Cidadão Ciberseguro junto da rede do Ministério das Finanças no âmbito do Plano Setorial do MF CTIC 2020	01/01/2019	31/12/2020	MF/eSPap	Divulgado/não Divulgado	Divulgado	Divulgado	Divulgado	Executada	
E2LA19	Sensibilizar as entidades nacionais para as respetivas vulnerabilidades específicas, passíveis de serem infiltradas, exploradas ou subvertidas no campo digital por agentes de ameaça diversos.	E2LA19AD1	CPI - PC	OE1	Realizar evento anual sobre Cibersegurança e Ciberdefesa, destinado a instituições da administração pública regional, a empresas públicas e privadas, visando a sensibilização, promoção e partilha de informação.	01/01/2019	31/12/2023	RAA - GR	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Nº de pessoas alcançadas: as mesmas de E2LA18AD3
		E2LA19AD2	COT - GC	OE1	Disponibilizar plataforma que permita verificar o nível de conformidade de um domínio de Internet e de correio eletrónico com os mais recentes standards para a comunicação segura entre sistemas, facilitando a identificação das medidas técnicas necessárias para a sua implementação.	01/01/2019	31/12/2019	PCM/CNCS; Associação DNS.PT	Disponibilizado /não Disponibilizado	Disponibilizado		Disponibilizado	Executada	
		E2LA19AD3	COT - GC	OE3	Produzir recomendações técnicas de cibersegurança	01/01/2019	31/12/2020	PCM/CNCS	Nº de recomendações técnicas	2	4	2	Executada	

Eixo 3 — Proteção do ciberespaço e das infraestruturas															
EnLA#	Linhas de Ação	EnLA#AD#	Domínio	Obj Estr.	Atividades a desenvolver	Período execução		Entidade responsável	Indicador	Meta (Manual)		Resultados			Obs.
						Início	Fim			2019	2020	2019	Desvio 2019	2020	
E3LA1	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;	E3LA1AD1	COT - GC	OE3	Identificar as infraestruturas críticas de informação na esfera da responsabilidade da eSPap	01/01/2019	31/12/2020	MF/eSPap	Identificado/não Identificado		Identificado	Identificado	Com Desvio		
		E3LA1AD3	COT - GC	OE3	Identificar as infraestruturas críticas de informação na esfera da responsabilidade do MAI	01/01/2020	31/12/2020	MAI/SG, MAI/GNR, MAI/PSP, MAI/SEF, MAI/ANEPC	Nº total de entidades	1	5	1	Executada		
E3LA2	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 ciliere e eficaz;	E3LA2AD5	COT - GC	OE1	Realizar ação de verificação de conformidade dos sistemas de informação com a RCM nº 41/2018	01/10/2019	01/12/2019	MTSSS/CPL	Realizado/não Realizado	Realizado		Não Realizado	Com Desvio		A reprogramar para o corrente ano económico devido constrangimenmtos de ordem orçamental em matéria de "aquisição de serviços"
		E3LA2AD6	COT - GC	OE1	Aplicar política de segurança no acesso ao correio eletrónico	01/01/2019	31/12/2019	MTSSS/IEFP	Aplicado/não Aplicado	Aplicado		Aplicado	Executada		
		E3LA2AD7	COT - GC	OE1	Realizar ação de verificação de conformidade dos sistemas de informação com a RCM nº 41/2018	01/01/2019	31/12/2019	MTSSS/IEFP	Realizado/não Realizado	Realizado		Realizado	Executada		
		E3LA2AD8	COT - GC	OE1	Implementar soluções para cumprimento do RGPD e da RCM 41/2018	01/01/2019	31/12/2020	MTSSS/II	Implementado/não Implementado	Implementado	Implementado	Implementado	Executada		
		E3LA2AD9	COT - GC	OE3	Reformular o Sistema Gestão Integrado do II,IP garantindo a conformidade com as normas ISO/IEC 20000 e ISO/IEC 27001.	01/01/2019	31/12/2019	MTSSS/II	Reformulado/não Reformulado	Reformulado		Reformulado	Executada		
		E3LA2AD10	COT - GC	OE1	Realizar auditoria externa de acompanhamento para manutenção das certificações com as normas ISO/IEC 20000 e ISO/IEC 27001.	01/01/2019	31/12/2020	MTSSS/II	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada		
		E3LA2AD12	COT - EOC	OE1	Implementar solução de deteção automática de Vulnerabilidades	01/01/2019	31/12/2019	MTSSS/II	Implementado/não Implementado	Implementado		Implementado	Executada		
		E3LA2AD13	COT - EOC	OE1	Realizar auditoria externa à infraestrutura e aos serviços TI sob a forma de testes de intrusão.	01/01/2019	31/12/2019	MTSSS/II	Realizado/não Realizado	Realizado		Realizado	Executada		
		E3LA2AD14	COT - EOC	OE1	Realizar testes de verificação de vulnerabilidades com recurso a métodos de phishing.	01/01/2019	31/12/2019	MTSSS/II	Realizado/não Realizado	Realizado		Realizado	Executada		
		E3LA2AD16	COT - EOC	OE1	Realizar auditorias trimestrais aos sistemas de informação interna	01/01/2019	31/12/2020	MTSSS/IEFP	Nº de auditorias	1	3	1	Executada		
		E3LA2AD17	COT - EOC	OE1	Realizar auditorias semestrais à rede interna do IEFP e postos de trabalho	01/01/2019	31/12/2020	MTSSS/IEFP	Realizado/não Realizado			Realizado	Com Desvio		
		E3LA2AD24	COT - GC	OE3	Implementar do Plano de Continuidade do Negócio (PCN) do IEFP, IP	01/01/2019	31/12/2020	MTSSS/IEFP	Implementado/não Implementado		Implementado	Implementado	Com Desvio		
		E3LA2AD28	COT - EOC	OE1	Realizar auditoria de segurança sobre os principais padrões técnicos em uso.	01/01/2019	31/12/2019	MTSSS/II	Realizado/não Realizado	Realizado		Realizado	Executada		
		E3LA2AD29	COT - GC	OE1	Rever o PCN com o objetivo de integrar novas aplicações e agilizar os procedimentos de ativação, tirando partido de novas funcionalidades tecnológicas	01/01/2019	31/12/2019	MTSSS/II	Revisto/não Revisto	Revisto		Revisto	Executada		
		E3LA2AD30	COT - GC	OE3	Elaborar o Plano Estratégico de Sistemas de Informação do MTSSS (triénio 2020-2022)	01/01/2019	31/12/2019	MTSSS/II	Elaborado/não Elaborado	Elaborado		não Elaborado	Com Desvio		Em Curso

	E3LA2AD31	COT - GC	OE3	Elaborar o Plano Estratégico de Segurança da Informação do II,IP (triénio 2020-2022)	01/01/2019	31/12/2019	MTSSS/II	Elaborado/não Elaborado	Elaborado		não Elaborado	Com Desvio	Em Curso
	E3LA2AD32	COT - EOC	OE3	Implementar SOC para sistemas de informação geridos pelo II,IP	01/01/2019	31/12/2019	MTSSS/II	Implementado/não Implementado	Implementado		não Implementado	Com Desvio	
	E3LA2AD33	COT - EOC	OE1	Implementar procedimento de acesso à informação, digital e física, assegurando a legitimidade e registo no acesso	01/07/2019	01/12/2020	MTSSS/CPL	Implementado/não Implementado	Implementado	Implementado	Implementado	Executada	Identificados espaços que preservam informação física crítica
	E3LA2AD34	COT - EOC	OE1	Implementar novos mecanismos de prevenção de ameaças	01/01/2019	31/12/2020	MCTES/DGES	Nº de mecanismos	2	2	2	Executada	Nova firewall com atualização automática de ameaças. Novo SIEM com visibilidade melhorada sobre ameaças.
	E3LA2AD42	COT - ICRP	OE1	Afetar especialistas com qualificação em cibersegurança a funções específicas	01/01/2019	31/12/2020	RAM - GR/VP	Nº de especialistas afetados	3	6	1	Com Desvio	
	E3LA2AD45	COT - GC	OE3	Identificar o nível de maturidade das diversas entidades da Saúde ao nível da cibersegurança e segurança da informação	01/01/2019	31/12/2023	MS/SPMS	Identificado/não Identificado	Identificado	Identificado	Identificado	Executada	Esta iniciativa será sempre de carácter contínuo. Apesar de ainda não estarmos a trabalhar num Modelo de Maturidade bem definido, as diversas iniciativas relacionadas com segurança da informação e cibersegurança são monitorizadas quanto à sua adesão por parte do universo de 66 entidades do MS/SNS. Existe um dashboard continuamente atualizado com a participação e adesão das diversas iniciativas de segurança transversais como Governance (CRSI - Aprovação de um Comité de Risco e Segurança da Informação + PSI - Aprovação de Política de Segurança da Informação), Formações, Sessões, Curso do Cidadão Cibersseguro MS/SNS e respostas aos Alerta de Vulnerabilidades enviados via ECOS - Elemento de Coordenação Operacional de Segurança na Saúde.
	E3LA2AD46	COT - GC	OE3	Emitir recomendação de criação de planos de contingência para infraestruturas críticas da Saúde	01/01/2020	31/12/2023	MS/SPMS	Emitido/não Emitido		Emitido	Emitido	Com Desvio	Em 2019 foi emitida pela SPMS uma Circular Normativa com medidas de reforço imediato de cibersegurança para deteção e mitigação de ameaças de ransomware, prevendo medidas de recuperação e proativas de defesa.
	E3LA2AD49	COT - EOC	OE3	Implementar o Centro de Operações de Segurança (SOC) do CNCS	01/01/2019	31/12/2019	PCM/CNCS	Implementado/não Implementado	Implementado		Implementado	Executada	
	E3LA2AD53	COT - EOC	OE1	Realizar testes de verificação de vulnerabilidades com recurso a métodos de phishing.	01/01/2019	31/12/2023	MC/LUSA	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	
	E3LA2AD57	COT - GC	OE1	Atualizar e detalhar processo de reporting operacional e de atuação e resposta a incidentes	01/01/2019	31/12/2019	MMEAP/AMA	Atualizado/não Atualizado	Atualizado		Atualizado	Executada	Processo atualizado
	E3LA2AD58	COT - EOC	OE1	Implementar sistema de monitorização e deteção de tentativas de intrusão	01/01/2018	01/12/2019	MMEAP/AMA	Implementado/não Implementado	Implementado		Implementado	Executada	

	E3LA2AD59	COT - EOC	OE1	Atualizar e evoluir sistema de gestão de aplicações e distribuição de atualizações	01/01/2018	01/12/2019	MMEAP/AMA	Atualizado/não Atualizado	Atualizado		Atualizado	Executada		
	E3LA2AD60	COT - EOC	OE1	Realizar testes periodicos de penetração para verificação da segurança do perimetro exterior da AMA e para aferir vulnerabilidades com a disponibilização ao exterior de novos sistemas	01/01/2018	31/12/2023	MMEAP/AMA	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Foram realizados com periodicidade mensal	
	E3LA2AD62	COT - EOC	OE1	Realizar testes de avaliação ao Plano de Continuidade de Negócio	01/01/2019	01/12/2020	MMEAP/AMA	Realizado/não Realizado	Realizado	Realizado	Realizado	Executada	Realizado teste aos cenários I, II e III. O cenário IV, correspondente à continuidade de negócio em Data Center alternativo só está previsto para 2020	
	E3LA2AD63	COT - GC	OE3	Operacionalizar politicas, processos e procedimentos de acordo com o referencial normativo ISO 27001:2013 transversal a toda a organização	01/01/2019	01/12/2020	MMEAP/AMA	Operacionalizado/não Operacionalizado	Operacionalizado		Operacionalizado	Executada		
	E3LA2AD64	COT - GC	OE3	Obter Certificação ISO 27001:2013 com ambito circunscrito à componente de integração da IAP - Plataforma de Interoperabilidade de AP	01/01/2019	01/12/2020	MMEAP/AMA	Obtido/não Obtido	Obtido		Obtido	Executada	Obtida em 27-12-2019	
	E3LA2AD69	COT - EOC	OE1	Implementar procedimentos de detação e de prevenção de ameaças	01/01/2019	31/12/2019	ME/DGE	Implementado/não Implementado	Implementado		Implementado	Executada	Indicação por email em 26.02.2020	
	E3LA2AD70	COT - GC	OE3	Operacionalizar o Plano Global de Segurança da AT	01/01/2019	31/12/2019	MF/AT	Operacionalizado/não Operacionalizado	Operacionalizado		Operacionalizado	Executada	Atividade de carácter permanente, a ser prosseguida em 2020 e seguintes.	

E3LA3	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;	E3LA3AD2	CPI - PI	OE1	Implementar uma Information Sharing and Analisys Center (ISAC) para o setor da Saúde	01/01/2019	31/12/2019	MS/SPMS	Implementado/não Implementado	Implementado		Implementado	Executada	Durante o ano 2019 foi consolidada uma estrutura governativa denominada Grupo de Acompanhamento para a Cibersegurança na Saúde (GACS), que atua nacionalmente como um orgão consultivo multidisciplinar do Conselho Superior de Segurança do Ciberespaço para a área da Saúde. Este Grupo é constituido por 26 entidades de saúde, órgãos de administração pública, privada e social, associações, entre outros, reunindo trimestralmente para debater, refletir e aprender mais sobre cibersegurança, partilhando conhecimento, experiências e iniciativas. (existiram 4 reuniões em 2019) Ainda neste âmbito, foram estabelecidos três grupos de trabalho, presididos por entidades públicas e privadas: • Grupo 1: Prevenção, educação e consciencitização: usuários, profissionais de saúde, profissionais de TIC (relacionados ao eixo 2 da ENSC 2.0) • Grupo 2: Resposta a ameaças e combate ao crime cibernético: CSIRT (Equipe de resposta a incidentes de segurança de computadores) para a saúde (relacionado ao eixo 4 do ENSC) • Grupo 3: Pesquisa, desenvolvimento e inovação: IoT / Dispositivos Médicos em Saúde (relacionados ao Eixo 5 ENSC). Em caso de ameaças, riscos e incidentes, está previsto no regulamento do GACS, que este possa atuar como um ponto de contato para a partilha de informações entre seus membros, garantindo a colaboração operacional em situações de emergência no setor.
		E3LA3AD3	CPI - EG	OE1	Criar um forum de cooperação dentro da área governativa da Saúde	01/01/2019	31/12/2019	MS/SPMS	Criado/não Criado	Criado		Criado	Executada	
		E3LA3AD4	CPI - PI	OE1	Implementar o ISAC Madeira	01/01/2019	31/12/2019	RAM - GR/VP	Implementado/não Implementado	Implementado		não Implementado	Com Desvio	
E3LA4	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;	E3LA4AD1	EL - DAENR	OE3	Elaborar o Quadro Nacional de Referência para a Cibersegurança	01/01/2019	31/12/2020	PCM/CNCS	Elaborado/não Elaborado	Elaborado		Elaborado	Executada	
		E3LA4AD2	COT - GC	OE3	Disponibilizar instrumentos para avaliar os níveis de maturidade das organizações em Cibersegurança	01/01/2019	31/12/2019	PCM/CNCS	Disponibilizado/não Disponibilizado	Disponibilizado		Disponibilizado	Executada	
E3LA5	Maximizar a segurança e a defesa das redes e sistemas de informação das Forças Armadas e da Defesa Nacional tendo em vista a manutenção	E3LA5AD1	CH - FSE	OE3	Participar em ações de formação especifica no âmbito de ciberdefesa	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de pessoas alcançadas	30	30	25	Com Desvio	em 2019 foram realizadas 38 ações de formação, alcançando um total de 25 pessoas

da capacidade de operação no ciberespaço através da capacidade de ciberdefesa defensiva.	ESLASAD2	COT - GC	OE3	Assegurar a evolução tecnológica dos sistemas de informação e das redes da Defesa Nacional.	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de plataformas atualizadas	2	3	2	Executada	- Efetuada uma atualização da plataforma de proteção de perímetro das FFAA com a atualização das NGFW do MDN e EMGFA - Efetuada a atualização da plataforma de monitorização e deteção de ameaças nas FFAA

Eixo 4 – Resposta às ameaças e combate ao cibercrime															
EnLAR	Linhas de Ação	EnLARAD#	Domínio	Obj Estr.	Atividades a desenvolver	Período execução		Entidade responsável	Indicador	Meta (bienal)		Resultados			Obs.
						Início	Fim			2019	2020	2019	Desvio 2019	2020	
E4LA1	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;	E4LA1AD3	COT - EOC	OE1	Participar em exercícios com componente de operações ofensivas	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de exercícios	1	2	1	Executada		- Participação no exercício Locked Shields 19
		E4LA1AD4	COT - EOC	OE1	Organizar exercícios de caráter conjunto com integração da componente de ciberdefesa nos restantes domínios das operações militares.	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de exercícios	1	1	1	Executada		- Participação no exercício LUSITANO19 (equipa de planeamento, controlo da execução e audiência de treino)
E4LA2	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;	E4LA2AD2	CPI - PI	OE1	Alargar a implementação da plataforma de partilha de informação de indicadores de compromisso com entidades externas às FFAA	01/01/2019	31/12/2021	MDN/EMGFA/CCD	Nº de entidades externas	2	2	2	Executada		Concretizada a interligação do sistema de partilha de informação com: - o SIS e - o ComDCiber (Brasil)
E4LA7	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;	E4LA7AD2	CPI - PI	OE1	Criar ISACS em áreas de interesse estratégico	01/01/2019	31/12/2023	PCM/CNCS	Nº de ISACS	3	3	1	Com Desvio		
E4LA8	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;	E4LA8AD4	CPI - PI	OE3	Ligar novas entidades ao PANORAMA	01/01/2019	31/12/2020	PCM/CNCS	Nº de novas entidades	4	10	1	Com Desvio		
		E4LA8AD5	CPI - PI	OE3	Produzir um Nível Único de Alerta Nacional	01/01/2019	31/12/2020	PCM/CNCS, MDN/EMGFA/CCD, MJ/PJ e SIS	Nº de entidades participantes	1	4	1	Executada		Projeto co-financiado CEF-Telecom
		E4LA8AD6	CPI - PC	OE3	Criar um Observatório de Cibersegurança	01/01/2019	31/12/2019	PCM/CNCS	Criado/não Criado	Criado		Criado	Executada		
E4LA9	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.	E4LA9AD1	CPI - PC	OE1	Participar em eventos e seminários que promovam a partilha de conhecimento e informação no âmbito da Cibersegurança, beneficiando dessa partilha e networking.	01/01/2019	31/12/2020	PCM/CEGER	Participa/não Participa	Participa	Participa	Participa	Executada		O Departamento de Segurança e Certificação Eletrónica participou em diversos workshops do X Simpósio sobre Segurança Informática e Cibercrime promovido pela Ubinet/IPBeja.
		E4LA9AD3	C - CI	OE1	Participar em fora internacionais como o TF-CSIRT e First	01/01/2019	31/12/2020	MCTES/FCT	Participa/não Participa	Participa	Participa	Participa	Executada		

	E4LA9AD4	CPI - PC	OE1	Disseminar iniciativas nacionais e internacionais dirigidas à comunidade CSIRT	01/01/2019	31/12/2020	PCM/CNCS	Disseminado/não Disseminado	Disseminado	Disseminado	Disseminado	Executada		
	E4LA9AD7	CPI - PC	OE1	Participação das equipas técnicas da AMA em conferências especificamente dedicadas ao tema CSIRTs	01/01/2019	31/12/2020	MMEAP/AMA	Participa/não Participa	Participa	Participa	Participa	Executada	"Nº de pessoas alcançadas": 2	

Eixo 5 — Investigação, desenvolvimento e inovação															
						Período execução				Meta (bianual)		Resultados			
EnLA#	Linhas de Ação	EnLA#AD#	Domínio	Obj Estr.	Atividades a desenvolver	Início	Fim	Entidade responsável	Indicador	2019	2020	2019	Desvio 2019	2020	Obs.
ESLA1	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;	ESLA1AD4	CPI - I&D&I	OE2	Definir um conjunto de indicadores, a produzir de forma sistemática, referentes a cinco linhas de observação distintas que caracterizam o estado da Cibersegurança em Portugal, no âmbito do Observatório de Cibersegurança	01/01/2019	31/12/2019	PCM/CNCS	Nº de linhas de observação	1	4	6	Com Desvio		Em 2019 definiram-se os indicadores para as 6 linhas de observação previstas no âmbito do Observatório de Cibersegurança, antecipando-se, assim, as metas previstas para os anos seguintes
ESLA2	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;	ESLA2AD3	CPI - I&D&I	OE2	Desenvolver e participar em projetos de I&D na área da cibersegurança.	01/01/2019	31/12/2023	MIH/IP	Nº de projetos	1	1	1	Executada		Candidatura Cef-Telecom Projeto C-Roads
ESLA3	Apoiar a participação dos intervenientes em investigação, desenvolvimento e inovação em projetos internacionais;	ESLA3AD1	C - CN	OE2	Estabelecer protocolos de cooperação com centros de investigação para projetos de cibersegurança em Saúde	01/01/2020	31/12/2023	MS/SPMS	Nº de protocolos		2	1	Com Desvio		A SPMS, EPE e a Hong Kong Hospital Authority (HA), órgão estatal que gere todos os hospitais e instituições de saúde do governo em Hong Kong, estabeleceram uma Declaração de Intenções que prevê uma colaboração assente em boas práticas, por 3 anos, no desenvolvimento conjunto dos respetivos Sistemas Digitais de Saúde. Uma das áreas de colaboração e enfoque desta colaboração é a área de segurança da informação e cibersegurança.
		ESLA3AD2	C - CN	OE2	Estabelecer protocolos para programas e parcerias com parceiros tecnológicos, universidades e especialistas no âmbito da cibersegurança.	02/01/2019	31/12/2023	MIH/IP	Nº de protocolos	1	2	1	Executada		Âmbito Nacional: CNCS e ATEC Âmbito Internacional: CESI
ESLA5	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;	ESLA5AD1	CH - FSC	OE3	Participar em projectos de educação e formação em ciberdefesa de caráter multinacional	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de projetos	1	1	1	Executada		- Participação e Liderança do projeto MN CD E&T
		ESLA5AD2	CPI - I&D&I	OE3	Participar em projetos de I&D-I no âmbito das iniciativas de Smart Defence da NATO	01/01/2020	31/12/2023	MDN/EMGFA/CCD	Nº de projetos	1	1	1	Executada		- Participação no projeto Smart Defense MISP - Malware Information Sharing Platform
		ESLA5AD3	CPI - I&D&I	OE2	Participar em projetos de I&D-I no âmbito da Cooperação Estruturada Permanente da UE	01/01/2020	31/12/2023	MDN/EMGFA/CCD	Nº de projetos	1	1	1	Executada		- Participação no projeto PESCO 6.5 - Cyber Threats and Incident Response Information Sharing Platform (CTIRISP)
ESLA6	Promover o desenvolvimento de produtos, sistemas e serviços secure by design e secure by default;	ESLA6AD2	COT - GC	QE1	Implementar no desenvolvimento de novos sistemas de informação a prática do cumprimento de princípios, boas práticas e normas de segurança.	01/01/2019	31/12/2020	MCTES/DGES	Implementado/não Implementado	Implementado	Implementado	não Implementado	Com Desvio		Em implementação no novo sistema de informação atualmente em desenvolvimento (SIMGES) - data de finalização da implementação e testes: 06/2020
		ESLA6AD7	COT - EOC	QE1	Implementar processos de teste não funcional de forma a garantir o princípio de security-by-desing	01/01/2019	31/12/2019	MTSSS/II	Implementado/não Implementado	Implementado		Implementado	Executada		

ESLA7	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;	ESLA7AD1	C - CI	OE1	Participar no Grupo Europeu para a Certificação da Cibersegurança no âmbito da Comissão Europeia (UE)	01/01/2020	31/12/2023	PCM/CNCS	Participa/não Participa	Participa	Participa	Participa	Executada	
ESLA8	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";	ESLA8AD1	COT - EOC	OE2	Disponibilizar aplicação da Administração Pública "App id.gov.pt"	01/01/2018	31/12/2019	MMEAP/AMA	Disponibilizado/não Disponibilizado	Disponibilizado		Disponibilizado	Executada	A app foi disponibilizada em Janeiro de 2019 com o Cartão de Cidadão, a Carta de Condução e cartão da ADSE. Continua o esforço para a disponibilização de mais cartões na app.
ESLA9	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;	ESLA9AD1	C - CN	OE2	Estabelecer protocolos com o setor privado e académico com vista à disponibilização e utilização da plataforma "Autenticação.gov"	01/01/2019	31/12/2020	MMEAP/AMA	Nº de protocolos	9	10	21	Com Desvio	Existiram várias adesões de Câmaras Munipais que alteraram completamente as estimativas anteriores

Eixo 6 — Cooperação nacional e internacional														
						Período execução				Meta (bienal)		Resultados			Obs.
EnLAM	Linhas de Ação	EnLAMAD#	Domínio	Obj Estr.	Atividades a desenvolver	Início	Fim	Entidade responsável	Indicador	2019	2020	2019	Desvio 2019	2020	
E6LA1	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;	E6LA1AD1	CPI - PC	OE1	Organizar iniciativas e fora de discussão multistakeholder a nível nacional e internacional sobre a temática da Governação da Internet, envolvendo uma multiplicidade de políticas públicas e assuntos técnicos incluindo a gestão do DNS, endereços IP, proteção do consumidor, assim como a capacitação, educação, formação, a sustentabilidade, robustez, segurança e estabilidade da Internet, a garantia da liberdade de expressão e a proteção da privacidade, a promoção do multilinguismo, a criação de um ambiente propício ao desenvolvimento da Internet	01/01/2019	31/12/2023	MCTES/FCT	Nº de iniciativas	1	1	1	Executada		O DSI organizou a oitava edição da iniciativa Portuguesa do Fórum de Governação da Internet, que decorreu na Covilhã, 13 de novembro de 2019. Mais informação em https://www.governacaointernet.pt/2019.html
E6LA2	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;	E6LA2AD1	C - CI	OE1	Participar no GDHP – Global Digital Health Partnership (Workstream Cyber security)	01/01/2019	31/12/2020	MS/SPMS	Participa/não Participa	Participa	Participa	Participa	Executada		Durante o Summit ocorrido em fevereiro 2019 em New Delhi, India foi aprovada a participação da SPMS, enquanto entidade representante da Saúde de Portugal, no GDHP - Global Digital Health Partnership. No âmbito deste grupo, a mesma sempre participou ativamente na Work Stream (WS) dedicada as temáticas de Cibersegurança, cujo objetivo é fortalecer os processos e práticas de proteção de dispositivos, sistemas e redes relacionados à prestação de cuidados médicos, bem como os dados neles contidos de riscos de segurança e ciber-ataques. Ainda antes da formalização da sua participação neste grupo, a SPMS organizou o 1st Cyber Security Workshop em Janeiro 2019, em Lisboa, contando com a participação de 6 países, resultando na produção do "White Paper - Securing digital health". Em Novembro 2019, o Presidente da SPMS foi nomeado Chair deste WS, conjuntamente com Hong Kong, onde participam cerca de 18 países como EUA, Australia, UK, Holanda, Singapura, Coreia do Sul, entre outros. No âmbito da eHaction - Joint Action supporting the eHealth Network, a SPMS participa ativamente, entre outros, no Work Package 7 - Overcoming implementation challenges: Task 7.3 - Data and systems security (Prioritised cybersecurity areas and topics). Este trabalho tem como objetivo facilitar a cooperação e a partilha de informações e boas práticas em cibersegurança em sistemas e serviços de saúde a nível nacional e transfronteiriço, através da criação e adoção de um Guia de Cibersegurança para Prestadores de Cuidados de Saúde.
		E6LA2AD2	C - CI	OE1	Participar na Joint Action supporting the eHealth Network - eHaction o âmbito da União Europeia	01/01/2019	31/12/2020	MS/SPMS	Participa/não Participa	Participa	Participa	Participa	Executada		

	E6LA2AD3	C - CI	OE1	Participar na ENISA's eHealth Security Group, no âmbito da União Europeia	01/01/2019	31/12/2020	MS/SPMS	Participa/não Participa	Participa	Participa	Não Participa	Com Desvio	A ENISA apenas relançou o Grupo de Especialistas em Segurança em Saúde (eHealth Security Group) em fevereiro de 2020. Ainda assim, é importante referenciar que em outubro 2019 foi constituído o European Health Cybersecurity Group (ECHG), como resultado do 1st Cybersecurity Workshop for National Heads of Cybersecurity in Health, ocorrido em Lisboa sob a dinamização da SPMS. Este grupo é constituído por elementos da Comissão Europeia (DG CONNECT, DG SANTE), ENISA e 14 representantes de cibersegurança europeus de Ministérios da Saúde, Serviço Nacional de Saúde e Agências eHealth, com um plano de trabalhos definido a nível estratégico e tático. Em Novembro, este grupo colaborativo e respetivo planeamento de atividades foi formalizado em sede de 16ª reunião da eHealth Network.
	E6LA2AD4	C - CI	OE1	Participar no Horizontal Working Party on Cyber Issues no âmbito do Conselho da União Europeia (UE)	01/01/2019	31/12/2023	PCM/CNCS	Participa/não Participa	Participa	Participa	Participa	Executada	
	E6LA2AD5	C - CI	OE1	Participar no IWG Cyber da Organização para a Segurança e Cooperação na Europa (OSCE)	01/01/2019	31/12/2023	PCM/CNCS	Participa/não Participa	Participa	Participa	Participa	Executada	
	E6LA2AD6	C - CI	OE1	Participar no Working Party on Security in the Digital Economy (SDE) da Organização para a Cooperação e Desenvolvimento Económico (OCDE)	01/01/2019	31/12/2023	PCM/CNCS	Participa/não Participa	Participa	Participa	Participa	Executada	
	E6LA2AD7	C - CI	OE1	Participar no grupo de trabalho European Cybersecurity Month da ENISA	01/01/2019	31/12/2023	PCM/CNCS	Participa/não Participa	Participa	Participa	Participa	Executada	
	E6LA2AD8	C - CI	OE1	Participar no grupo de trabalho European Cybersecurity Exercise da ENISA	01/01/2019	31/12/2023	PCM/CNCS	Participa/não Participa	Participa	Participa	Participa	Executada	
	E6LA2AD9	C - CI	OE1	Participar no Grupo de Alto Nível sobre a Governação da Internet da UE	01/01/2019	31/12/2023	MCTES/FCT	Participa/não Participa	Participa	Participa	Participa	Executada	
	E6LA2AD10	C - CI	OE1	Participar na Comissão Ciência Tecnologia para o Desenvolvimento da ONU	01/01/2019	31/12/2023	MCTES/FCT	Participa/não Participa	Participa	Participa	Participa	Executada	
	E6LA2AD11	C - CI	OE1	Participar no Fórum da Governação da Internet da ONU	01/01/2019	31/12/2023	MCTES/FCT	Participa/não Participa	Participa	Participa	Participa	Executada	Participação no Internet Governance Forum 2019 que decorreu em Berlim de 25 a 29 de novembro com a apresentação de uma comunicação "Filling the Gap on Digital Inclusion Portuguese Safer Internet Centre Best Practices", bem como moderação de uma mesa de trabalho e relatora das conclusões no Workshop "Tackling Hate Speech: A Multi-Stakeholder Responsibility"
	E6LA2AD12	C - CI	OE1	Participar nos grupos de Trabalho sobre a Internet da União Internacional de Telecomunicações	01/01/2019	31/12/2023	MCTES/FCT	Participa/não Participa	Participa	Participa	Participa	Executada	

		E6LA2AD13	C - CI	OE1	Participar na Internet Assigned Names and Numbers (ICANN)	01/01/2019	31/12/2023	MCTES/FCT	Participa/não Participa	Participa	Participa	Participa	Executada	
		E6LA2AD14	C - CI	OE1	Participar nos grupos de trabalho da European SchoolNet que tem como objetivo promover políticas educativas de Cidadania Digital	01/01/2019	31/12/2023	ME/DGE	Participa/não Participa	Participa	Participa	Participa	Executada	Participação nas três reuniões de trabalho nas quais foram abordadas as temáticas: não ao discurso de ódio online; os 10 domínios de Cidadania Digital do Conselho da Europa e políticas educativas (the whole school approach).
		E6LA2AD15	C - CI	OE1	Participar nos grupos de trabalho e projetos desenvolvidos no âmbido da Rede Insafe	01/01/2019	31/12/2023	ME/DGE	Participa/não Participa	Participa	Participa	Participa	Executada	Participação em duas formações presenciais com os 33 países da rede Insafe. Participação nos grupos de trabalho online (Safer Internet Day online meeting; Youth Coordinators online meeting; Awareness online meeting).
		E6LA2AD16	C - CI	OE1	Participar no C-Roads e C-Streets no âmbito do Connecting Europe Facility (CEF) e no 5G-Mobix no âmbito do Horizon 2020.	01/01/2019	31/12/2023	MIH/IP	Participa/não Participa	Participa	Participa	Participa	Executada	
		E6LA3AD1	COT - EOC	OE1	Participar em exercícios de cibersegurança e ciberdefesa	01/01/2019	31/12/2020	PCM/CEGER	Nº de exercícios	1	1	1	Executada	O CEGER participou no exercício CIBER PERSEU 2019, promovido pelo Exército Português.
		E6LA3AD3	COT - EOC	OE1	Participar em exercícios de cibersegurança e ciberdefesa	01/01/2019	31/12/2023	RAA - GR	Participa/não Participa	Participa	Participa	Participa	Executada	
		E6LA3AD4	COT - EOC	OE1	Participar em exercícios de cibersegurança e ciberdefesa	01/01/2019	31/12/2023	PCM/CNCS	Participa/não Participa	Participa	Participa	Participa	Executada	
		E6LA3AD5	COT - EOC	OE1	Realizar exercício de ciberdefesa (CyberDEx) para validação da COI (Capacidade Operacional Inicial) do Centro de Ciberdefesa	01/01/2021	31/12/2021	MDN/EMGFA/CCD	Realizado/não Realizado			Realizado	Com Desvio	- Realizado exercício CyberDEx em OUT19
		E6LA3AD6	COT - EOC	OE1	Realizar exercício de ciberdefesa com abertura a entidades externas às FFAA, na componente de cibersegurança.	01/01/2021	31/12/2021	MDN/EMGFA/CCD	Realizado/não Realizado			Realizado	Com Desvio	- Realizado exercício CySMART no âmbito da iniciativa 5+5 - Realizado Exercício CiberPerseu 19
E6LA3	Participar nos exercícios de cibersegurança e de ciberdefesa reforçando o aumentando o nível de maturidade para a proteção do ciberespaço, onde a partilha de informação e conhecimento constitui um fator fundamental,	E6LA3AD7	COT - EOC	OE1	Participar em exercícios de ciberdefesa de âmbito nacional e internacional	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de exercícios	5	5	5	Executada	- Participação nos exercícios: * NATO Cyber Coalition * NATO CWIX * CCDCOE Locked Shields * ExNCS * Ibero Americano
		E6LA3AD9	COT - EOC	OE1	Participar em exercícios de cibersegurança e ciberdefesa	01/01/2019	31/12/2020	MCTES/FCT	Nº de exercícios	1	1	2	Com Desvio	a equipa do RCTS CERT participou no CiberPerseu Nacional e no International CyberEx
		E6LA3AD10	COT - EOC	OE1	Participar em exercícios de cibersegurança e ciberdefesa	01/01/2020	31/12/2020	MF/AT	Participa/não Participa		Participa	Participa	Com Desvio	
		E6LA3AD11	COT - EOC	OE1	Participar em exercícios anuais de cibersegurança e ciberdefesa	01/01/2019	31/12/2020	RAM - GR/VP	Participa/não Participa	Participa	Participa	Participa	Executada	
		E6LA3AD14	COT - EOC	OE1	Participar em exercícios de cibersegurança e ciberdefesa	01/01/2019	31/12/2023	MC/LUSA	Participa/não Participa	Participa	Participa	Participa	Executada	
		E6LA3AD15	COT - EOC	OE1	Participar em exercícios de cibersegurança e ciberdefesa, nomeadamente o Ciberperseu e ExNCS	01/01/2019	31/12/2023	MAI/SG	Nº de exercícios		2	2	Com Desvio	
		E6LA3AD16	COT - EOC	OE1	Participar em exercícios de cibersegurança, nomeadamente o CiberPerseu 2019	01/01/2019	31/12/2019	MTSSS/MI	Participa/não Participa	Participa		Participa	Executada	
		E6LA3AD17	COT - EOC	OE1	Participar em exercícios de cibersegurança e ciberdefesa	01/01/2019	31/12/2023	MMEAP/AMA	Participa/não Participa	Participa	Participa	Não Participa	Com Desvio	O cumprimento deste objetivo não depende apenas da AMA. Não existiu oportunidade de participação em 2019 nestes exercícios.
		E6LA3AD18	COT - EOC	OE1	Participar em exercícios de cibersegurança e ciberdefesa	01/01/2019	31/12/2023	MIH/IP	Participa/não Participa	Participa	Participa	Participa	Executada	ExNCS e Ciber Perseu

E6LA4	Integrar organismos internacionais de cibersegurança e de ciberdefesa tendo em vista a cooperação internacional e a afirmação de Portugal neste domínio;	E6LA4AD1	C - CI	OE1	Garantir a integração de representação nacional na estrutura de ciberdefesa da NATO.	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de representantes	1	1	1	Executada	- SHAPE - Cyberspace Directorate
		E6LA4AD2	C - CI	OE1	Garantir a integração de representação nacional no CCDCoE	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de representantes	1	1	1	Executada	- Representação nacional com o TCDR Reimão Teixeira.
		E6LA4AD3	C - CI	OE1	Representar Portugal no Management Board da ENISA	01/01/2019	31/12/2023	PCM/CNCS	Representa/não Representa	Representa	Representa	Representa	Executada	
		E6LA4AD4	C - CI	OE1	Representar Portugal na National Liasion Officers Network da ENISA	01/01/2019	31/12/2023	PCM/CNCS	Representa/não Representa	Representa	Representa	Representa	Executada	
E6LA5	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;	E6LA5AD2	COT - EOC	OE3	Participar ativamente na Rede Nacional CSIRT	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Participa/não Participa	Participa	Participa	Participa	Executada	- Garantida presença nas reuniões da rede
		E6LA5AD3	C - CN	OE1	Estabelecer protocolos de cooperação com atores relevantes para a segurança do ciberespaço	01/01/2019	31/12/2023	MDN/EMGFA/CCD	Nº de protocolos	2	2	2	Executada	- USEUCOM - CISCO
		E6LA5AD4	COT - EOC	OE3	Participar ativamente na Rede Nacional CSIRT	01/01/2019	31/12/2020	MCTES/FCT	Participa/não Participa	Participa	Participa	Participa	Executada	
		E6LA5AD6	C - CN	OE3	Participar consórcio público-privado Centro Internet Segura	01/01/2019	31/12/2023	ME/DGE	Participa/não Participa	Participa	Participa	Participa	Executada	Participação nas diversas reuniões do Consórcio Internet Segura. Dinamização conjunta por todos os membros do Consórcio do Seminário Dia da Internet Mais Segura 2019 que contou com cerca de 300 participntes entre alunos, professores, outos agentes educativos e partes interessadas.
		E6LA5AD7	C - CN	OE1	Participar no Grupo Informal de sobre Literacia para os Media (GILM)	01/01/2019	31/12/2023	ME/DGE	Participa/não Participa	Participa	Participa	Participa	Executada	Participação nas diversas reuniões do GILM tendo sido dinamizado em conjunto a Conferência Literacia Media e Cidadania envolvendo cerca de 150 participantes.
E6LA6	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;	E6LA6AD1	C - CN	OE1	Estabelecer Protocolos de Serviços com entidades para fornecimento de serviços de confiança da Entidade Certificadora Comum do Estado.	01/01/2019	31/12/2019	PCM/CEGER	Nº total de entidades	100	200	132	Com Desvio	A ECCE possui 132 Protocolos ativos, sendo que todos serão revistos em 2020, por força da entrada em vigor do Despacho 7338/2019, de 20 de agosto, e pela entrada em produção do Portal de Serviços da ECCE.