a. . .
. . m. área metropolitana
. l. . de lisboa

Conselho Metropolitano de Lisboa
Mandato 2017-2021

EDITAL

N.º 04/CML/2019

(Protocolo de Cooperação entre o Gabinete Nacional de Segurança/ Centro Nacional de Cibersegurança e a Área Metropolitana de Lisboa)

FERNANDO MEDINA, Presidente do Conselho Metropolitano de Lisboa, no exercício das competências previstas no art.º 72º do Anexo I aprovado pela Lei n.º 75/2013, de 12 de setembro, e nos termos do n.º 1 do art.º 56º aplicável às áreas metropolitanas por força do disposto no artigo 104ºdo mesmo diploma, torna público que o Conselho Metropolitano de Lisboa, reunido ordinariamente em 22 de janeiro de 2019, apreciou a proposta de iniciativa da Comissão Executiva e aprovou por unanimidade, com 14 voto(s) a favor, do(s) município(s) de Alcochete, Almada, Amadora, Barreiro, Cascais, Lisboa, Mafra, Montijo, Odivelas, Palmela, Seixal, Sesimbra, Setúbal e Vila Franca de Xira, representando 1.728.077 eleitores (71,59%), a Proposta n.º 192/CEML/2018 - Aprovação da submissão ao Conselho Metropolitano de Lisboa de Protocolo de Cooperação entre o Gabinete Nacional de Segurança/ Centro Nacional de Cibersegurança e a Área Metropolitana de Lisboa, em anexo.

Para constar e produzir os efeitos legais se publica o presente edital, que vai ser afixado nos locais do costume.

Lisboa, 22 de janeiro de 2019

O Presidente do Conselho Metropolitano de Lisboa

Fernando Medina

Rua Cruz de Santa Apolónia, 23, 25, 25A.
1100-187 Lisboa
Tel: (+351) 218 428 570
Fax: (+351) 218 428 577
amlcorreio@aml.pt
www.aml.pt

a. . .
. . m. área metropolitana
. l. . de lisboa

Aprovado por unanimidade.

Lisboa, 29 de novembro de 2018

PROPOSTA N.º 192/CEML/2018

[Aprovação da submissão ao Conselho Metropolitano de Lisboa de Protocolo de Cooperação entre o Gabinete Nacional de Segurança/ Centro Nacional de Cibersegurança e a Área Metropolitana de Lisboa]

A. Considerando que nos termos da alínea e) do nº 1 do artigo 67.º do anexo I da Lei nº 75/2013, de 12 de setembro constitui atribuição da Área Metropolitana de Lisboa participar, nos termos da lei, na definição de redes de serviços e equipamentos de âmbito metropolitano;

B. Considerando que o GNS/CNCS pretende obter a participação da AML numa estratégia em rede de cibersegurança;

C. Considerando que a celebração do presente Protocolo, atenta as suas características a natureza e funções do GNS/CNCS, está excluída da Parte II do CCP, por força da disciplina prevista no nº 1 e na alínea a) do nº 4, ambos do artigo 5º do CCP;

D. Considerando que a alínea dd) do nº 1 do artigo 71.º do anexo I da Lei nº 75/2013, de 12 de setembro comete ao Conselho Metropolitano a competência para deliberar sobre todos os assuntos que visem a prossecução das atribuições da área metropolitana;

Neste sentido, tenho a honra de propor que a Comissão Executiva submeta ao Conselho Metropolitano para deliberar, nos termos da al. dd) do n.º 1 do artigo 71.º do Anexo I da Lei 75/2013, de 12 de setembro:

1. Aprovar a minuta do Protocolo de Cooperação entre o Gabinete Nacional de Segurança/ Centro Nacional de Cibersegurança e a Área Metropolitana de Lisboa, conforme anexo.

Lisboa, 22 de novembro de 2018
O Primeiro Secretário Metropolitano

Carlos Humberto de Carvalho

PROTOCOLO DE COOPERAÇÃO ENTRE O
GABINETE NACIONAL DE SEGURANÇA / CENTRO NACIONAL DE CIBERSEGURANÇA
E A ÁREA METROPOLITANA DE LISBOA

Considerando que, nos termos do n.º 2 do artigo 2.º do Decreto-Lei n.º 3/2012, de 16 de janeiro, alterado pelos Decretos-Leis n.ºs 162/2013, de 4 de dezembro, 69/2014, de 9 de maio, maio e 136/2017, de 6 de novembro, no âmbito do Gabinete Nacional de Segurança (GNS) funciona o Centro Nacional de Cibersegurança (CNCS).

Considerando que o CNCS tem por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

Considerando que, nos termos das alíneas a) a d) do n.º 1 do artigo 2.º-A do aludido Decreto-Lei, compete ao CNCS desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção, destinadas a fazer face a incidentes de cibersegurança e ciberataques; promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança; exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais e contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais.

Considerando que a Estratégia Nacional de Segurança do Ciberespaço, aprovada em anexo à Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, se funda no compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas.

Considerando a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, que tem como objetivo aumentar as capacidades em cibersegurança, a cooperação entre os Estados membros, a aplicação de medidas de segurança e a notificação de incidentes por parte dos operadores de serviços essenciais e dos prestadores de serviços digitais.

Considerando que o CERT.PT é o serviço de coordenação nacional de resposta a incidentes, que opera no GNS/CNCS e participa como membro na Rede Nacional de CSIRT (rede de equipas de reação a incidentes de cibersegurança), com a missão de estabelecer laços de confiança entre elementos responsáveis pela segurança informática, de criar indicadores e informação estatística nacional sobre incidentes de segurança, de criar instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão e de promover uma cultura de segurança em Portugal.

Considerando o disposto na Lei da Proteção de Dados Pessoais, aprovada pela Lei n.º 67/98, de 26 de outubro e alterada pela Lei n.º 103/2015, de 24 de agosto que transpõe para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

Considerando a participação internacional do GNS / CNCS na Agência Europeia para a Segurança das Redes e da Informação (ENISA), na *Task Force* de CSIRT Europeia (TF-CSIRT europeia), no *Forum of Incident Response and Security Teams (*FIRST*)* e na Organização para a Segurança e Cooperação na Europa (OSCE).

Considerando que, nos termos da alínea e) do nº 1 do artigo 67º do Anexo I da Lei nº 75/2013, de 12 de setembro constitui atribuição da Área Metropolitana de Lisboa participar, nos termos da lei, na definição de redes de serviços e equipamentos de âmbito metropolitano;

Considerando a necessidade de implementar melhores práticas de promoção da segurança e privacidade no uso dos sistemas e das tecnologias de informação e comunicação no âmbito da atuação dos Municípios integrantes da Área Metropolitana de Lisboa;

Considerando que, nos termos do n.º 2 do artigo 9.º do Decreto-lei n.º 3/2012, de 16 de janeiro, alterado pelos Decretos-Leis n.ºs 162/2013, de 4 de dezembro, 69/2014, de 9 de maio, e 136/2017, de 6 de novembro, para assegurar o exercício das suas atribuições, pode o GNS estabelecer parcerias, protocolos e outras formas de cooperação com quaisquer entidades, nacionais ou estrangeiras.

Entre

O Gabinete Nacional de Segurança / Centro Nacional de Cibersegurança, doravante designado GNS/CNCS, com sede na Rua da Junqueira, n.º 69, em Lisboa, representado neste ato pelo subdiretor-geral do GNS responsável pela coordenação do CNCS, _____ ao abrigo do n.º __ do Despacho n.º ____/201_, de __ de _____, do diretor-geral do GNS, Contra-Almirante António Gameiro Marques, publicado no Diário da República, 2.ª série, n.º __, de __ de _____;

E a Área Metropolitana de Lisboa, doravante designada AML, com sede na Rua Cruz de Santa Apolónia 23, 25 e 25A, em Lisboa, representada neste ato pelo Primeiro-Secretário Metropolitano, Carlos Humberto Palácios Pinheiro de Carvalho, ao abrigo do n.º 3 do artigo 76.º do Anexo I da Lei 75/2013, de 12 de setembro;

Celebram o presente Protocolo que se rege pelo disposto nas cláusulas seguintes:

Cláusula Primeira

Objeto

O presente Protocolo tem por objeto estabelecer as formas de cooperação entre o GNS/CNCS e a AML, doravante referidos como Partes, no desenvolvimento das capacidades nacionais de cibersegurança, troca de conhecimento e no aprofundamento mútuo das capacidades de cibersegurança.

Cláusula Segunda

Áreas de cooperação

1. No âmbito do presente Protocolo as áreas de cooperação entre as Partes são as seguintes:

- **a)** Desenvolvimento estratégico;
- **b)** Operações de cibersegurança;
- **c)** Formação e qualificação de recursos humanos;
- **d)** Sensibilização em matéria de cibersegurança;
- **e)** Políticas de cibersegurança;
- **f)** Exercícios de cibersegurança;
- **g)** Outras áreas da cibersegurança que sejam acordadas entre as Partes.

2. As iniciativas e projetos específicos constituem adendas próprias, que passam a fazer parte integrante do presente Protocolo, depois de aprovadas por escrito pelas Partes por quem, de acordo com os respetivos normativos internos em vigor, tenha competência para tal.

Cláusula Terceira

Partilha de informação de segurança

1. As partes comprometem-se a partilhar informação de segurança, cumprindo o princípio da necessidade de conhecer e o interesse setorial ou nacional da informação partilhada.

2. Os termos que regulam esta partilha de informação são definidos por iniciativa ou projeto, constando da respetiva adenda ao presente Protocolo.

Cláusula Quarta

Custos

Os custos decorrentes da execução do presente Protocolo são da exclusiva responsabilidade de cada uma das partes, salvo situações particulares que serão objeto de prévio acordo escrito e constarão como adendas ao presente Protocolo. A celebração do presente Protocolo não comporta custos diretos decorrentes de quotas anuais, participação em seminários, fóruns ou ações de formação obrigatórias.

Cláusula Quinta

Contatos de gestão e pontos de contato

1. Tendo em vista a gestão do presente Protocolo, são, desde já, definidos os seguintes contatos:

a) Pelo GNS/CNCS, o Coordenador do Departamento de Operações, com o endereço de correio eletrónico coordenador.operacoes@cncs.gov.pt e o telefone 910599492;

b) Pela AML

2. Tendo em vista a rápida e eficaz resolução de incidentes de segurança da informação, as Partes designam os seguintes elementos de coordenação operacional (ECO):

a) Pelo GNS/CNCS, CERT.PT, com o endereço de correio eletrónico cert@cert.pt e o telefone 210497399;

b) Pela AML

3. Qualquer alteração ao indicado nos números anteriores deverá ser comunicada de imediato e por escrito à outra Parte.

Cláusula Sexta

Reuniões de coordenação e relatório anual

1. Para efeitos da melhoria da execução do previsto no presente Protocolo e nas suas adendas, podem as Partes realizar reuniões de coordenação.
2. As reuniões de coordenação têm lugar, pelo menos, uma vez por ano e para as mesmas podem as Partes, por mútuo acordo, convidar outras entidades.
3. As Partes comprometem-se a elaborar um relatório anual que reflete os resultados da implementação do presente Protocolo e das suas adendas.

Cláusula Sétima

Revisão

1. O presente Protocolo pode ser revisto sempre que uma das partes o entenda conveniente, visando a introdução de adaptações consideradas necessárias, desde que obtido o consentimento da outra parte.
2. As alterações ao presente Protocolo revestirão sempre a forma escrita e poderão ser decididas em qualquer momento por comum acordo, assumindo a forma de substituição parcial ou integral ou de aditamento ao presente Protocolo, como adendas.

Cláusula Oitava

Vigência, denúncia e resolução

1. O presente Protocolo entra em vigor na data da sua assinatura, pelo período de um ano, sendo automaticamente renovado por iguais períodos.
2. Qualquer uma das Partes pode denunciar o presente Protocolo através de comunicação escrita, com uma antecedência mínima de 60 dias em relação à data do termo da vigência ou das suas renovações.
3. O presente Protocolo pode ser resolvido por qualquer das Partes, mediante comunicação à contraparte com efeitos imediatos, em caso de incumprimento pela outra parte de qualquer obrigação assumida nos termos do presente Protocolo.

Cláusula Nona

Casos Omissos

Os casos omissos no presente Protocolo e as eventuais dúvidas serão resolvidos ou esclarecidos por consenso entre as Partes.

O presente Protocolo é redigido em dois exemplares idênticos, o qual é assinado pelas Partes, ficando um exemplar na posse de cada uma das Partes.

Lisboa, aos ___ de _____ de 2018.

Pelo Gabinete Nacional de Segurança / Centro Nacional de Cibersegurança

_____

_____

(Função)

Pela Área Metropolitana de Lisboa

_____

Carlos Humberto Palácios Pinheiro de Carvalho
Primeiro-Secretário Metropolitano