c) Em todos os atos praticados ao abrigo desta delegação de competências deve ser feita menção expressa ao Chefe do Serviço de Finanças, através da expressão "Por delegação do Chefe do Serviço de Finanças", com indicação da data em que foi publicada a presente delegação no *Diário da República* e respetiva série.

V — Produção de efeitos — o presente despacho produz efeitos a partir de 1 de dezembro de 2012, inclusive, quanto ao Adjunto Eurico Bento Bernardino, ficando assim ratificados todos os atos e despachos entretanto proferidos sobre as matérias ora objeto de delegação.

7 de março de 2013. — O Chefe do Serviço de Finanças das Caldas da Rainha, *Rui José da Costa*.

207324152

Direção-Geral da Administração e do Emprego Público

Declaração de retificação n.º 1136/2013

Por ter sido publicado com inexatidão o despacho n.º 13035/2013, inserto no *Diário da República,* 2.ª série, n.º 198, de 14 de outubro de 2013, retifica-se que onde se lê «2- A presente designação produz efeitos a 1 de outubro de 2012» deve ler-se «2 — A presente designação produz efeitos a 1 de outubro de 2013».

14 de outubro de 2013. — A Diretora-Geral, *Maria Joana de Andrade Ramos*.

207322598

MINISTÉRIOS DAS FINANÇAS E DA DEFESA NACIONAL

Gabinetes da Ministra de Estado e das Finanças e do Ministro da Defesa Nacional

Despacho n.º 13687/2013

Considerando que

Em 20 de janeiro de 2009, foi celebrado nos termos do número quatro do artigo 6.º da Lei Orgânica n.º 3/2008, de 8 de setembro, Lei de Programação das Infraestruturas Militares (LPIM), um Protocolo entre o Ministério das Finanças e da Administração Pública e o Ministério da Defesa Nacional, tendo por objeto a definição das linhas estratégicas de colaboração entre estes dois ministérios, com vista à valorização do parque imobiliário afeto ao Ministério da Defesa Nacional (MDN);

Nos termos do número três da Cláusula Oitava do referido Protocolo, foi prevista a criação, por despacho conjunto dos Ministros das Finanças e da Defesa Nacional, de uma Comissão Paritária para coordenação da execução das operações resultantes do Protocolo;

Através do Despacho n.º 10543/2009, do Ministro de Estado e das Finanças e do Ministro da Defesa Nacional, publicado no DR 2.ª série, n.º 79, de 23 de abril de 2009, foi criada a Comissão Paritária de Coordenação da Execução das Operações relativas à Rentabilização dos Imóveis abrangidos pela LPIM, e designados os respetivos membros;

Atendendo à atual situação conjuntural do mercado imobiliário, consubstanciada no acentuado decréscimo de transações imobiliárias enquadradas no âmbito da LPIM, e tendo presente critérios de racionalidade económico-financeira, não se justifica a manutenção de uma Comissão Paritária cujo objetivo é precisamente a rentabilização dos imóveis abrangidos pela LPIM;

As atividades desenvolvidas por esta Comissão poderão facilmente ser assumidas pelos serviços competentes dos dois ministérios na área da gestão imobiliária, sendo competências já existentes e delegadas na Direção-Geral de Armamento e Infraestruturas da Defesa, e na Direção-Geral do Tesouro e Finanças;

Assim, atento o supra exposto, determina-se o seguinte:

1 - É extinta a Comissão Paritária de Coordenação da Execução das Operações relativas à Rentabilização dos Imóveis abrangidos pela Lei Orgânica n.º 3/2008, de 8 de setembro (LPIM).

2 - É revogado o Protocolo de 20 de janeiro de 2009, celebrado entre o Ministério das Finanças e da Administração Pública e o Ministério da Defesa Nacional.

3 - O disposto nos números anteriores produz efeitos a partir da data da publicação do presente Despacho.

7 de outubro de 2013. — A Ministra de Estado e das Finanças, *Maria Luís Casanova Morgado Dias de Albuquerque.* — O Ministro da Defesa Nacional, *José Pedro Correia de Aguiar-Branco.*

207326542

MINISTÉRIO DOS NEGÓCIOS ESTRANGEIROS

Secretaria-Geral

Despacho (extrato) n.º 13688/2013

Nos termos do disposto na alínea *b*) do n.º 1 e no n.º 2 do artigo 37.º da Lei n.º 12-A/2008, de 27 de fevereiro, conjugado com o n.º 3 do artigo 17.º da Lei n.º 59/2008, de 11 de setembro, torna-se público que, na sequência de despacho de 28 de maio de 2013, de S. Ex.ª a Secretária Geral do Ministério dos Negócios Estrangeiros, que autorizou a consolidação definitiva da mobilidade interna, na carreira e categoria de assistente técnico, foi celebrado um contrato de trabalho em funções públicas por tempo indeterminado, com Armanda Beatriz Lopes dos Santos, com efeitos a 16 de agosto de 2013, mantendo-se posicionada na 11.ª posição remuneratória da carreira de assistente técnico e nível remuneratório 16, da tabela remuneratória única aprovada pela Portaria n.º 1553-C/2008, de 27 de fevereiro.

10 de outubro de 2013. — A Diretora Adjunta do Departamento Geral de Administração, *Paula Crispim*.

207327774

Camões — Instituto da Cooperação e da Língua, I. P.

Despacho n.º 13689/2013

Para efeitos do disposto no n.º 6 do artigo 12.º da Lei n.º 12-A/2008, de 27 de fevereiro, por força do disposto no artigo 73.º do Regime do Contrato de Trabalho em Funções Públicas, aprovado pela Lei n.º 59/2008, de 11 de setembro, e após a minha homologação da avaliação final e demais deliberações do júri constituído para o efeito, torna-se público que foi concluído, com sucesso, o período experimental da técnica superior Maria de Fátima Pires Mendes, com a classificação final de 19,15 valores.

O tempo de serviço decorrido no período experimental será contado, para todos os efeitos legais, na carreira e categoria da trabalhadora.

16 de setembro de 2013. — A Presidente do Conselho Diretivo, *Prof.ª Doutora Ana Paula Laborinho*.

207323561

Despacho n.º 13690/2013

Nos termos e ao abrigo do disposto nas alíneas n.os 3 e 4 do artigo 24.º da Lei n.º 2/2004, de 15 de janeiro, alterada e republicada pela Lei n.º 64/2011, de 22 de dezembro, foi autorizada a cessação de funções como Chefe de Divisão de Apoio Jurídico e Contencioso, em regime de substituição, da licenciada Tânia José Lemos Marques Ramos.

O presente despacho produz efeitos a partir de 15 de outubro de 2013.

2 de outubro de 2013. — A Presidente do Conselho Diretivo, *Prof.ª Doutora Ana Paula Laborinho.*

207322995

MINISTÉRIO DA DEFESA NACIONAL

Gabinete do Ministro

Despacho n.º 13691/2013

Atento o exposto na informação 797, de 1 de outubro de 2013, da Direção-geral de Armamento e Infraestruturas de Defesa, nos termos das disposições do artigo 9.º da Lei n.º 2/2004, de 15 de janeiro, alterada pela Lei n.º 64/2011, de 22 de dezembro e artigos 35.º a 40.º do Código do Procedimento Administrativo, delego no Diretor-Geral de Armamento e Infraestruturas de Defesa, Major-General Manuel de Matos Gravilha Chambel, a condução de todos os trâmites procedimentais com vista à aquisição dos serviços de arbitragem - peritagem.

9 de outubro de 2013. — O Ministro da Defesa Nacional, *José Pedro Correia de Aguiar-Branco.*

207326567

Despacho n.º 13692/2013

Considerando que o atual Conceito Estratégico de Defesa Nacional, aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 21 de março, antecipa como grande tendência no ambiente de segurança global, o potencial devastador dos ataques cibernéticos, identificando o ciberterrorismo e a cibercriminalidade como ameaças e riscos prioritários;

Considerando que essas ações têm como alvo redes indispensáveis ao funcionamento da economia e da sociedade da informação globalizada, constituindo por isso, riscos e ameaças prioritários que se replicam e multiplicam diretamente no plano interno;

Reconhecendo que essas ações representam uma ameaça crescente sobre infraestruturas críticas, cujos efeitos e impactos podem provocar o colapso da estrutura tecnológica da organização social e económica do País;

Tendo presente que o atual Conceito Estratégico de Defesa Nacional, reconhecendo esses desafios de segurança do ciberespaço, preconiza a edificação ao nível das Forças Armadas de uma capacidade de Ciberdefesa;

Tendo presente as orientações específicas da Reforma "Defesa 2020", decorrentes da Resolução do Conselho de Ministros n.º 26/2013, de 19 de abril, que preveem o levantamento da capacidade de Ciberdefesa nacional, e preconizam em concreto a criação de um Centro de Ciberdefesa, no âmbito do Estado-Maior-General das Forças Armadas, em simultâneo com a criação de um único serviço que coordene as comunicações e os sistemas de informação, em articulação com os Ramos, procurando-se, numa lógica de centralização e especialização dos recursos existentes, num único polo e a implementação de uma plataforma transversal de apoio à decisão, designadamente no que diz respeito às funções de comando, controlo e direção;

Considerando em especial o meu Despacho n.º 7527-A/2013, de 11 de junho, que publica a diretiva ministerial para a reforma estrutural na Defesa Nacional e nas Forças Armadas, Reforma "Defesa 2020", que, no âmbito da preparação inicial do projeto de revisão da Lei Orgânica de Bases de Organização das Forças Armadas (LOBOFA), estabelece como princípio orientador atribuir ao Chefe do Estado-Maior General das Forças Armadas, em articulação com os órgãos e serviço centrais do Ministério da Defesa Nacional, a tutela de um Serviço de Comunicações e Sistemas de Informação e do Centro de Ciberdefesa;

Considerando as atribuições da Secretaria-geral para a área dos sistemas de informação e tecnologias de informação e comunicação no universo da Defesa Nacional;

Tendo presente as iniciativas conducentes à definição e implementação da Estratégia Nacional de Segurança da Informação que compreende, designadamente, a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança, e que, nesse âmbito, através do meu Despacho n.º 5590/2012, de 11 de abril de 2012, nomeei um representante na Comissão Instaladora deste centro;

Considerando, ainda, a Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões [JOIN (2013) 1 final], apresentada pela Comissão Europeia e pela Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, relativa à Estratégia da União Europeia para a Cibersegurança, de 7 fevereiro de 2013, e que estabelece como prioridade estratégica desenvolver a política e as capacidades no domínio da Ciberdefesa no quadro da Política Comum de Segurança e Defesa;

Reconhecendo a conveniência e oportunidade em formular orientações específicas sobre esta matéria e a necessidade de garantir o alinhamento deste processo com o ciclo de reforma em curso;

Determino a publicação da diretiva iniciadora com a Orientação Política para a Ciberdefesa, anexa ao presente despacho e que dele faz parte integrante.

11 de outubro de 2013. — O Ministro da Defesa Nacional, *José Pedro Correia de Aguiar-Branco.*

ANEXO

ORIENTAÇÃO POLÍTICA PARA A CIBERDEFESA

I. INTRODUÇÃO

1. ENQUADRAMENTO

O ciberespaço é por natureza um espaço aberto desprovido de fronteiras tangíveis, onde tanto o setor público como o privado, civis e militares, atores nacionais e internacionais interagem em simultâneo e de forma interdependente e interligada. Por essas razões, não é um espaço seguro e protegido, sendo vulnerável a ataques cibernéticos, que podem ter como consequência perdas relevantes no plano económico e social ou constituir uma ameaça séria à Defesa Nacional, quer no plano da degradação ou destruição de infraestruturas críticas quer no plano da neutralização ou negação ao acesso a recursos informacionais.

Compreende-se assim, que o ciberespaço constitua um novo domínio operacional, onde podem vir a ser conduzidas operações militares e onde o levantamento de mecanismos de proteção e defesa obedece à mesma lógica e fundamentos que caracterizam a Segurança e a Defesa do Estado. Com efeito, as missões das Forças Armadas dependem, cada vez mais, da livre utilização do ambiente de informação e do próprio ciberespaço para a condução de todo o espectro de operações.

Por conseguinte, a dependência crescente em relação aos sistemas de informação que garantem o exercício do comando e controlo na prossecução das missões das Forças Armadas, em particular, e em relação às tecnologias de informação e comunicação, em geral, colocam importantes desafios à organização e funcionamento da Defesa Nacional. Estas dependências, conjugadas com o crescente poder disruptivo e destrutivo dos ataques lançados através da internet e das redes com esta interligadas, exige o levantamento de estruturas especializadas no âmbito da ciberdefesa e obriga a Defesa Nacional a adotar respostas concertadas e articuladas, tanto no plano nacional como internacional.

2. FINALIDADE

A Orientação para a Política de Ciberdefesa tem por finalidade determinar os princípios essenciais, definir objetivos e estabelecer as correspondentes linhas orientadoras dos esforços a desenvolver, no âmbito da Defesa Nacional, visando, nomeadamente, o levantamento da capacidade nacional de Ciberdefesa.

3. PRESSUPOSTOS

A definição dos objetivos e a determinação das linhas de ação da Política de Ciberdefesa Nacional obedecem aos seguintes pressupostos:

a) O ciberespaço, pela sua importância para a afirmação da Soberania Nacional, constitui um espaço de defesa de valores e interesses, materializando uma área de responsabilidade coletiva.

b) O ambiente do moderno campo de batalha é cada vez mais descontínuo e multidimensional, constatando-se que as operações militares têm vindo progressivamente a incluir o desenvolvimento de operações em redes de computadores (defensivas, de exploração e ofensivas), juntando aos tradicionais espaços de atuação (terra, mar e ar) também o ciberespaço.

c) As Forças Armadas dependem, cada vez mais, da livre utilização do ambiente de informação e do próprio ciberespaço para conduzirem todo o espectro de operações.

d) As atividades de Ciberdefesa são orientadas para atender às necessidades da Defesa Nacional visando assegurar a utilização do espaço cibernético, impedindo ou dificultando o seu uso contra os interesses nacionais.

e) A segurança dos Sistemas de Informação e Comunicações (SIC) constitui a base para a defesa do ciberespaço, dependendo em grande medida do grau de sensibilização e consciencialização das organizações e das pessoas para o valor da informação que detêm ou processam. Não será possível assegurar a ciberdefesa sem garantir também a segurança da informação que circula nos SIC.

f) O desenvolvimento tecnológico associado ao levantamento da capacidade de ciberdefesa deve ser equacionado em harmonia com o Planeamento de Defesa Militar.

g) As iniciativas a desenvolver devem potenciar sinergias nacionais e atender aos esforços cooperativos em curso nas organizações internacionais de que Portugal faz parte integrante, nomeadamente, no âmbito da OTAN (*smart defence*) e da União Europeia (*pooling & sharing*).

h) A eficácia das ações de defesa do ciberespaço depende, fundamentalmente, da atuação sinérgica e colaborativa da sociedade portuguesa, envolvendo não apenas os órgãos do Ministério da Defesa Nacional (MDN), do Estado-Maior-General das Forças Armadas (EMGFA) e dos Ramos, mas também a comunidade académica, os setores público e privado e a base industrial de defesa.

II. PRINCÍPIOS DA CIBERDEFESA

O aumento exponencial do volume e sofisticação das atividades cibernéticas com fins maliciosos, bem como a velocidade com que os eventos decorrem no ciberespaço, reforçam a necessidade de atribuir especial prioridade à prevenção e contenção dos efeitos dos ataques. Nesse sentido, a capacidade de ciberdefesa deve ser estruturada e desenvolvida de forma a prevenir e retardar a rápida progressão dos ciberataques, garantindo a sua deteção antecipada, implementando ferramentas de vigilância e alerta avançado, procurando deste modo conter e limitar potenciais danos.

Os ataques cibernéticos podem ter como consequência perdas relevantes no plano económico, de vidas humanas ou constituir uma ameaça séria à Defesa Nacional. Neste contexto, através da avaliação das consequências da atividade cibernética hostil, deverá existir a flexibilidade operacional necessária para ajustar, de forma proporcional, a resposta a cada tipo de ataque e situação.

Para aumentar a capacidade de recuperação após um ataque cibernético, devem-se concentrar os esforços na segurança dos SIC considerados críticos, contemplando igualmente o apoio OTAN e da UE na defesa cooperativa destas infraestruturas.

As ações e operações militares conduzidas no âmbito da ciberdefesa são executadas no respeito do quadro legal em vigor, obedecendo à mesma lógica e fundamentos que caracterizam a Segurança e a Defesa Nacional.

Muitos dos serviços de ciberdefesa baseiam-se funcionalmente nas capacidades técnicas, tradicionalmente associadas à cibersegurança, que passam pela prevenção, deteção e recuperação dos SIC face à ocorrência de ataques cibernéticos.

As atividades de ciberdefesa, constituindo uma área ligada às operações militares, devem por essa razão também complementar a implementação dos requisitos destinados a proteger a confidencialidade, integridade e disponibilidade dos SIC (criptografia, segurança da informação, segurança física e do pessoal), devendo para esse efeito manter-se permanentemente atualizadas e em conformidade com esses requisitos.

Uma capacidade operacional de ciberdefesa envolve o conhecimento e os recursos necessários para prever, influenciar ou bloquear as ações que potenciais adversários venham a desenvolver no ciberespaço, antes e durante as operações militares. Neste contexto, para avaliar o espectro da ameaça, identificar potenciais atacantes e as suas intenções, as Forças Armadas devem dispor de uma capacidade de recolha e análise de informações no ciberespaço, capaz de permitir, em tempo, uma resposta eficaz. Deverão ainda dispor de competências do foro jurídico, indispensáveis na condução de operações neste domínio.

A informação relativa à ciberdefesa, como sejam os detalhes relativos a ataques cibernéticos específicos, as avaliações de ameaças e vulnerabilidades, deverá ser classificada, manuseada e acedida conforme as determinações de segurança em vigor.

A dinâmica e complexidade do ciberespaço exigem uma adaptação contínua à envolvente operacional, colocando às Forças Armadas o desafio adicional de recrutar e reter o pessoal mais qualificado, capaz de integrar os requisitos inicialmente estabelecidos e, proativamente, promover a inovação e a evolução constante tanto do nível de conhecimento, competências e técnicas, como da própria doutrina de emprego operacional das capacidades.

As técnicas utilizadas pelos atores ou agentes perpetrantes são muitas vezes semelhantes e procuram explorar vulnerabilidades genéricas, comuns à maior parte das redes e sistemas. Só uma aproximação conjunta e cooperativa permitirá enfrentar as ameaças cibernéticas de forma a melhorar a cibersegurança e garantir a ciberdefesa de forma sustentável.

III. OBJETIVOS

São objetivos da Política de Ciberdefesa:

1) Garantir a proteção, a resiliência e a segurança das redes e dos SIC da Defesa Nacional contra ciberataques;

2) Assegurar 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;

3) Contribuir de forma cooperativa para a cibersegurança nacional.

IV. LINHAS ORIENTADORAS

ESTRUTURA DE CIBERDEFESA NACIONAL

Estabelecer uma estrutura de comando e controlo da ciberdefesa nacional, a incluir no processo de revisão da LOBOFA e da lei orgânica do EMGFA atualmente em curso, contemplando a existência de um órgão com caráter de orientação estratégica-militar das atividades de ciberdefesa e uma capacidade militar de resposta operacional a ciberataques e a incidentes informáticos.

As atribuições de orientação estratégica-militar da ciberdefesa deverão recair sobre o Conselho de Chefes de Estado-Maior. Para o efeito deverá o Conselho dispor de competência para deliberar sobre a doutrina conjunta de ciberdefesa, a submeter à confirmação do Ministro da Defesa Nacional. O Centro de Ciberdefesa, na dependência do CEMGFA, constitui o órgão responsável pela condução de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas.

PLANEAMENTO DE DEFESA MILITAR

Implementar a capacidade de ciberdefesa com vista a integrar as operações no ciberespaço no âmbito das capacidades militares. Para o efeito, incorporar no Processo de Planeamento de Defesa Militar, em conjugação com o NATO *Defence Planning Process* (NDPP) e com o *Capability Defence Plan* (CDP) da UE, o desenvolvimento da capacidade nacional de ciberdefesa. O levantamento desta capacidade deve ter por base o Conceito Estratégico de Defesa Nacional, o preconizado na diretiva "Defesa 2020", e todos os documentos relevantes para a mesma. De acordo com este enquadramento, identificar e hierarquizar através do Processo de Planeamento de Defesa os requisitos de ciberdefesa relevantes.

A defesa contra as ameaças cibernéticas deve incluir o reforço da proteção das redes, a monitorização e análise dos padrões de tráfego, a deteção precoce de ataques e a resposta aos mesmos, envolvendo para esse efeito, sempre que necessário, a condução de operações no ciberespaço.

CAPACIDADE PARA CONDUZIR OPERAÇÕES MILITARES EM REDES DE COMPUTADORES

Vários países estão em processo avançado de desenvolvimento ou possuem já hoje à sua disposição capacidades cibernéticas de natureza ofensiva para utilização militar. Atores não-Estado podem também constituir uma ameaça, nomeadamente, através da disrupção dos sistemas de Comando e Controlo (C2) das Forças Armadas e dos seus sistemas de gestão da informação.

Implementar a capacidade militar para conduzir todo o espetro de operações no ciberespaço (defensivas, de exploração e ofensivas), desenvolvendo e mantendo atualizada a doutrina de emprego das capacidades associadas à ciberdefesa, e definindo os princípios básicos que orientam a criação de legislação e normas específicas de apoio às atividades da Defesa Nacional no ciberespaço, constitui a única forma credível de promover uma ciberdefesa eficaz, capaz de constituir um fator de dissuasão a potenciais atacantes.

REFORÇO DA CAPACIDADE DE INFORMAÇÕES NO CIBERESPAÇO

A capacidade para avaliar a dinâmica das ameaças e perceber as possibilidades e intenções de potenciais atacantes constitui uma precondição para a proteção das infraestruturas de informação e para a condução de operações no ciberespaço. Um desafio complexo, que se coloca no contexto cibernético, é a atribuição da origem e a identificação dos atores responsáveis pelos ataques ou tentativas de ataque.

Os atores envolvidos na Defesa Nacional necessitam assim de reforçar a sua capacidade de recolha e análise de informações no ciberespaço e de integrar, em tempo oportuno, a informação obtida na condução das operações de ciberdefesa, devendo ainda ter a capacidade para bloquear e anular as atividades de informações conduzidas por terceiros.

Neste âmbito, devem ser capazes de avaliar a evolução das ameaças cibernéticas, através da realização periódica de avaliações de ameaças à ciberdefesa e de outros relatórios especializados.

Deste modo, devem os atores da Defesa Nacional contribuir para a produção de conhecimento situacional do ciberespaço e para a recolha de informações de interesse para a Defesa Nacional.

PARTILHA DA INFORMAÇÃO DE CIBERDEFESA

A prevenção e minimização dos efeitos causados por ataques cibernéticos resultam da partilha atempada de informação, da existência de um sistema de alerta imediato e da atualização permanente do panorama sobre as atividades maliciosas a decorrer no ciberespaço.

Constituindo a ciberdefesa uma área onde se torna necessário promover sinergias e potenciar o seu emprego dual (civil-militar), deverá desenvolver-se um sistema de partilha de informação aos vários níveis e patamares de decisão, procedimentos de alerta imediato em apoio aos objetivos definidos e de colaboração com a rede nacional de serviços de resposta a incidentes de segurança informática (CSIRT), instituições privadas, universidades e organizações internacionais como a OTAN e a UE.

De igual forma, deverá ser definida uma estratégia de ciência e tecnologia no domínio da ciberdefesa, sendo para esse efeito implementadas linhas de investigação, envolvendo estruturas de Investigação e Desenvolvimento (I&D) militares e civis, orientadas para o desenvolvimento de capacidades nesta área.

De modo a tornar toda esta estrutura mais robusta, deverão ser exploradas sinergias nacionais e a cooperação internacional de forma a melhorar a capacidade de Ciberdefesa do País.

SENSIBILIZAÇÃO, FORMAÇÃO E EXERCÍCIOS

Adequar a gestão dos recursos humanos de modo a garantir a sua permanência em atividades relacionadas com esta temática por períodos não inferiores a cinco anos.

Aumentar a sensibilização para as necessidades da ciberdefesa ao nível dos utilizadores dos SIC, desenvolver peritos em ameaças cibernéticas e na condução de operações em redes de computadores, treinar os procedimentos para operação em ambientes degradados pela realização de ataques cibernéticos, participar nos exercícios nacionais e internacionais de ciberdefesa, e manter atualizado o treino de ciberdefesa do pessoal.

Centralizar a formação e o treino em ciberdefesa e constituir um polo de excelência neste domínio, evitando duplicações e aproveitando as competências e os recursos já existentes nas Forças Armadas, tendo presente a ligação à Escola de Comunicações e Sistemas de Informação da OTAN, a implementar no nosso país, e a possibilidade de Portugal vir a liderar um projeto de "*smart defence*" no âmbito da "*education and training for cyberdefence*".

AQUISIÇÕES E CADEIA DE REABASTECIMENTO — GESTÃO DE RISCO

Promover uma cultura de gestão do risco através da incorporação de requisitos de gestão de risco nas aquisições a realizar e na cadeia

de abastecimento, com vista a mitigar os riscos de comprometimento do *software* ou do *hardware,* passíveis de adulterar intencionalmente o seu comportamento.

V. RESPONSABILIDADES E ATUALIZAÇÃO

O EMGFA, em coordenação com os órgãos e serviços centrais do MDN e com os Ramos, é responsável pelo levantamento da capacidade nacional de Ciberdefesa, visando garantir, no âmbito da Defesa Nacional, a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de segurança desejados.

Para esse efeito, deverão ser tidas em consideração as estruturas e recursos já existentes nas Forças Armadas, de forma a explorar sinergias, evitar duplicações e maximizar os recursos disponíveis.

Pretende-se que no final do ciclo de reforma da Defesa Nacional esteja edificada a capacidade de ciberdefesa e que as alterações da LOBOFA e da Lei Orgânica do EMGFA estejam em vigor.

Esta orientação política deve ser revista e atualizada periodicamente devendo a primeira revisão ocorrer após a implementação da "Defesa 2020".

207326583

MARINHA

Gabinete do Chefe do Estado-Maior da Armada

Portaria n.º 709/2013

Manda o Almirante Chefe do Estado-Maior da Armada, ao abrigo da alínea *c*) do n.º 1 do artigo 68.º do Estatuto dos Militares das Forças Armadas (EMFAR), após despacho conjunto n.º 7178/2013, de 24 de maio, do Ministro de Estado e das Finanças e do Ministro da Defesa Nacional, promover por diuturnidade ao posto de segundo-tenente, em conformidade com o previsto na alínea *e*) do artigo 216.º do mesmo estatuto, os *guardas-marinhas da classe de Médicos Navais*:

26805 Pedro Miguel da Costa Pecorelli Modas Daniel
26605 Nuno Miguel Mendão Rodrigues
26705 Paulo Jorge Lourenço Flores Figueira
26905 João Abranches de Soveral Figueiredo Pombeiro

(no quadro), que satisfazem as condições gerais e especiais de promoção fixadas, respetivamente nos artigos 56.º e 227.º do mencionado estatuto, a contar de 1 de outubro de 2012, data a partir da qual lhes conta a respetiva antiguidade, de acordo com a alínea *a*) do n.º 1 do artigo 175.º e para efeitos do n.º 2 do artigo 68.º, ambos daquele estatuto. As promoções produzem efeitos remuneratórios no dia seguinte ao da publicação da presente portaria, nos termos da alínea *a*) do n.º 7 do artigo 35.º da Lei n.º 66-B/2012, de 31 de dezembro, ficando colocados na 1.ª posição remuneratória do novo posto, conforme previsto no n.º 1 do artigo 8.º do Decreto-Lei n.º 296/2009, de 14 de outubro

Estes oficiais, uma vez promovidos e tal como vão ordenados, deverão ser colocados na lista de antiguidade do seu posto e classe à esquerda do *27904 segundo-tenente da classe de Médicos Navais Mário António Ferreira Canastro.*

11-10-2013. — O Almirante Chefe do Estado-Maior da Armada, *José Carlos Torrado Saldanha Lopes,* almirante.

207319658

Superintendência dos Serviços do Pessoal

Despacho n.º 13693/2013

Manda o Almirante Chefe do Estado-Maior da Armada, ao abrigo da alínea *d)* do número 1 do artigo 68.º do Estatuto dos Militares das Forças Armadas (EMFAR), após despacho conjunto n.º 7178/2013, de 24 de maio, do Ministro de Estado e das Finanças e do Ministro da Defesa Nacional, cessar a demora na promoção, de acordo com o previsto no número 3 do artigo 62.º e promover por diuturnidade ao posto de primeiro-marinheiro, o segundo-marinheiro da classe de taifa, subclasse despenseiro, em regime de Contrato:

9327506, Luís Miguel Barrocal que satisfaz as condições gerais e especiais de promoção fixadas, respetivamente, nos artigos 299.º e 305.º do mencionado estatuto, a contar de 2 de março de 2013, data a partir da qual lhe conta a respetiva antiguidade, de acordo com o número 2 do artigo 68.º, ambos daquele estatuto. A promoção produz efeitos remuneratórios no dia seguinte ao da publicação do presente despacho, nos termos da alínea *a)* do número 7 do artigo 35.º da Lei n.º 66-B/2012, de 31 de dezembro, ficando colocado na 1.ª posição remuneratória do novo posto, conforme previsto no número 1 do artigo 8.º do Decreto-Lei n.º 296/2009, de 14 de outubro.

Este militar, uma vez promovido, deverá ser colocado na lista de antiguidade do seu posto e classe à esquerda do 9309007 primeiro-marinheiro TFD RC Fábio Rudolfo Serra Fonseca e à direita do 9317107 primeiro-marinheiro TFD RC Ricardo Alexandre dos Santos Barbosa.

15 de outubro de 2013. — Por subdelegação do Diretor do Serviço de Pessoal, o Chefe da Repartição de Efetivos e Registos, *Miguel Nuno Pereira de Matos Machado da Silva,* capitão-de-mar-e-guerra.

207327458

EXÉRCITO

Comando do Pessoal

Direção de Administração de Recursos Humanos

Repartição de Pessoal Militar

Portaria n.º 710/2013

Manda o General Chefe do Estado-Maior do Exército, por portaria de 18 de outubro de 2013, promover ao posto de tenente, nos termos do n.º 1 do artigo 183.º e da alínea *e*) do artigo 216.º do EMFAR, por satisfazerem as condições gerais e especiais de promoção estabelecidas nos artigos 56.º e 238.º do referido Estatuto, os seguintes militares:

Infantaria

Alferes 09635205, Francisco Miguel Sousa da Silva
Alferes 09845209, Luís Carlos Martins da Silva
Alferes 08138803, Pedro Gonçalo Esteves Simões
Alferes 19829803, Sérgio Aurélio Cerqueira da Encarnação
Alferes 13094306, Pedro Miguel Pires da Silva
Alferes 19252906, Nuno Filipe Gonçalves Carvalho
Alferes 03881803, Rodrigo José de Oliveira Ferreira
Alferes 11122506, João Francisco Godinho Baptista
Alferes 13937505, Luís Carlos Orvalho Conde da Luz
Alferes 03623906, Filipe Coutinho Valente Simão Freire
Alferes 17944706, Rui Jorge Portela dos Anjos
Alferes 14572103, Hugo Miguel de Almeida Pereira
Alferes 13909306, Bruno Ricardo Pereira Reis
Alferes 05666309, Miguel Cândido Pereira e. Domingos de Almeida
Alferes 16168009, João Pedro Silva Sousa
Alferes 16283806, Carlos Manuel Ramos da Silva Rainho
Alferes 09761509, Rui Emanuel Martins Pina
Alferes 03599004, João Miguel Teixeira Magalhães
Alferes 10724504, Gonçalo Luís Pita de Carvalho
Alferes 05411204, André Filipe Pinto da Fonseca
Alferes 16719403, Bruno Miguel dos Santos Folhas
Alferes 01416906, Paulo Henrique Moniz Franco de Torres Soares

Artilharia

Tenente GRAD 02627899, Cristóvão José Teixeira Fernandes
Alferes 18165805, Daniela Braga Salvador Pestana Santos
Alferes 02614006, João António Soares Saraiva
Alferes 05779102, Ricardo Jorge Lourenço Pinto Loureiro
Alferes 06224409, Marisa Figueiredo Cardoso
Alferes 11012705, João Paulo Martins Silva
Alferes 11094105, João Manuel Marques Arnaut
Alferes 00905009, Pedro Herculano Gonçalves de Sousa
Alferes 04062306, João Pedro Martins Pereira
Alferes 03020909, Afonso Manuel da Silva Peralta
Alferes 04588305, Bruno Filipe Porto Preto

Cavalaria

Alferes 03866809, Mauro Daniel Pires Covas
Alferes 11791604, Frederico Ferreira Santos
Alferes 14336306, Pedro Miguel da Costa Júlio
Alferes 08155301, Daniel José Oliveira Fernandes
Alferes 11998305, Cristina Isabel Abelho Borralho
Alferes 05282406, João Miguel Martins Ferreira dos Santos
Alferes 16685106, Sandra Sofia Nunes Amaro
Alferes 05616905, Vasco Rafael Caridade Monteiro
Alferes 17464904, Bruno Manuel Sousa Ferreira
Alferes 13663305, Diogo José Silva Carrilho

Administração militar

Alferes 06258106, Vasco Lobato de Faria Rijo
Alferes 15301109, Jorge Nuno Pessoa Silva