igualmente, notificar a outra Parte da conclusão deste procedimento e indicar-lhe o número de registo atribuído.

Feito em seis páginas, aos 4 dias do mês de julho de 2012, em dois exemplares originais na língua portuguesa, fazendo ambos os textos igualmente fé.

Pela República Portuguesa:

Dr. João Pedro Aguiar-Branco, Ministro da Defesa Nacional.

Pela República de Moçambique:

Eng.º Filipe Jacinto Nyusi, Ministro da Defesa.

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Resolução do Conselho de Ministros n.º 36/2015

A sociedade, a economia e o Estado são dependentes das tecnologias de informação e de comunicação (TIC).

Temos assistido a um desenvolvimento acelerado da sociedade da informação e a uma crescente dependência das TIC em funções vitais do funcionamento do País.

A definição de uma agenda digital permite disponibilizar benefícios económicos e sociais, estimular a criação de emprego, a sustentabilidade e a inclusão social, extrair o máximo benefício das novas tecnologias e melhorar a estrutura de enquadramento nacional.

Estas tecnologias são, no entanto, vulneráveis, criando riscos sociais e materiais. Se, por um lado, trazem claros benefícios à sociedade, por outro lado, vêm aumentar, de forma significativa, os riscos decorrentes da sua dependência e da quantidade de informação armazenada e em circulação, expondo o Estado, as empresas e os cidadãos.

O ciberespaço transpõe a vida real para um mundo virtual, com características únicas que impõem novas formas de interação e de relacionamento.

No plano dos bens jurídicos de natureza pessoal têm vindo a revelar um aumento exponencial os crimes sexuais contra menores praticados através da Internet, assumindo amiúde este fenómeno criminoso dimensão transacional e acentuada sofisticação de meios, o que reclama uma intervenção firme, determinada e eficaz.

Este «mundo em rede» desenvolve novos modos de atuação com características únicas, de onde se destacam o cibercrime e, em particular, o cibercrime organizado, associado à fraude bancária e à usurpação de identidade com este mesmo propósito, o *hacktivismo* político nas suas várias expressões, como são o desvio e a revelação de informação sensível ou classificada e a sabotagem informática, ou ainda a crescente espionagem de Estado e industrial.

Tanto a nível interno como internacional, são evidentes as capacidades de ativismos políticos e religiosos, criminosos ou terroristas para conduzir ações com impacto na segurança de infraestruturas vitais de informação, criando sérias ameaças à sobrevivência do Estado de Direito democrático e ao espaço de liberdade, segurança e justiça.

A necessidade de proteger as áreas que materializam a soberania nacional, assegurando a autonomia política e estratégica do País, bem como o crescente número de incidentes e ataques maliciosos, impõe que a segurança do ciberespaço seja considerada como uma prioridade nacional.

Por isso, é fundamental que o País disponha de uma Estratégia Nacional de Segurança do Ciberespaço, que estabeleça objetivos e linhas de ação com vista a uma eficaz gestão de crises, a uma coordenação da resposta operacional a ciberataques, a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio.

O esforço destinado a reduzir debilidades ao nível da segurança das redes e da informação, aumentando a resiliência das suas infraestruturas críticas, apresenta-se também como fundamental, quer no quadro da União Europeia, ao nível da Estratégia da União Europeia para a Cibersegurança, quer das políticas de Ciberdefesa da Organização do Tratado do Atlântico Norte (OTAN). O reforço da cooperação traduz-se num exponencial ganho de eficácia da proteção destes bens, impondo-se o seu aprofundamento.

Neste contexto, importa definir uma visão e um enquadramento estratégico, lógico e coerente.

Assim:

Nos termos das alíneas *d*), *f)* e *g*) do artigo 199.º e da alínea *a*) do n.º 1 do artigo 200.º da Constituição, o Conselho de Ministros resolve:

1 — Aprovar a Estratégia Nacional de Segurança do Ciberespaço, que consta do anexo à presente resolução e que dela faz parte integrante.

2 — Determinar que a presente resolução reporta os seus efeitos à data da sua aprovação.

Presidência do Conselho de Ministros, 28 de maio de 2015. — O Primeiro-Ministro, *Pedro Passos Coelho.*

ANEXO

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

1. A Estratégia Nacional de Segurança do Ciberespaço, doravante designada por Estratégia, funda-se 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.

2. A Estratégia assenta sobre os princípios gerais da soberania do Estado, das linhas gerais da Estratégia da União Europeia para a Cibersegurança e na estrita observância da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa, da Carta dos Direitos Fundamentais da União Europeia, da proteção dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade, e alicerça-se nos seguintes cinco pilares:

a) Subsidariedade:

A segurança do ciberespaço é parte integrante da segurança nacional e é essencial para o funcionamento do Estado, para o desenvolvimento económico e a inovação, bem como para a confiança dos cidadãos no mercado digital e no ciberespaço.

O Estado afirma o seu forte compromisso com a proteção do ciberespaço. No entanto, grande parte das infraestruturas tecnológicas que compõem o ciberespaço é detida

por operadores privados, a quem cabe a responsabilidade primária pela sua proteção. Esta responsabilidade inicia-se no próprio indivíduo, pela forma responsável como utiliza o ciberespaço, e termina no Estado, enquanto garante da soberania e dos princípios constitucionais.

b) Complementaridade:

A segurança do ciberespaço é uma responsabilidade partilhada entre os diferentes atores, sejam eles públicos ou privados, militares ou civis, coletivos ou individuais.

Uma abordagem alargada e integradora da segurança do ciberespaço reúne diferentes atores com diferentes responsabilidades e capacidades, para benefício de todos.

c) Cooperação:

Num mundo altamente interligado e interdependente, a segurança do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais e internacionais, alicerçada no desenvolvimento de confiança mútua.

d) Proporcionalidade:

Os riscos inerentes ao ciberespaço devem ser avaliados e geridos de forma adequada, assegurando-se a proporcionalidade dos meios e medidas para o seu exercício.

e) Sensibilização:

A garantia da segurança das infraestruturas tecnológicas, das redes e dos sistemas de informação depende da capacidade de os utilizadores finais saberem tomar medidas que previnam os riscos a que se encontram expostos. A sensibilização constitui um eixo essencial à preservação da segurança no ciberespaço.

3. A Estratégia desenvolve-se nos seguintes objetivos estratégicos:

a) Promover uma utilização consciente, livre, segura e eficiente do ciberespaço;
b) Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;
c) Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais;
d) Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.

4. As implicações e necessidades associadas a cada um dos objetivos estratégicos permite definir uma orientação geral e específica, traduzida em seis eixos de intervenção, enformados em medidas concretas e respetivas linhas de ação, destinadas a reforçar o potencial estratégico nacional no ciberespaço, a saber:

Eixo 1 — Estrutura de segurança do ciberespaço;
Eixo 2 — Combate ao cibercrime;
Eixo 3 — Proteção do ciberespaço e das infraestruturas;
Eixo 4 — Educação, sensibilização e prevenção;
Eixo 5 — Investigação e desenvolvimento;
Eixo 6 — Cooperação.

Eixo 1 — Estrutura de segurança do ciberespaço:

A complexidade e a abrangência dos desafios da segurança do ciberespaço requerem uma liderança e governação forte e transversal, uma coordenação operacional ágil, célere e eficaz, uma capacidade de resposta e salvaguarda dos interesses nacionais e, acima de tudo, uma envolvência de recursos, conhecimentos e competências. Assim, devem ser adotadas as seguintes medidas:

1) Estabelecer a coordenação político-estratégica para a segurança e defesa do ciberespaço:

A responsabilidade pela segurança do ciberespaço nacional encontra-se distribuída por diferentes atores com missões e objetivos diversos, não existindo um fio condutor nem a coerência necessária nas políticas e iniciativas desenvolvidas por cada um deles.

Neste contexto, entende-se como necessária e prioritária a existência de uma abordagem transversal e integradora das várias sensibilidades dos diversos setores da sociedade, nesta matéria.

Para este efeito, deve ser definida uma coordenação político-estratégica para a segurança do ciberespaço, na dependência direta do Primeiro-Ministro, com representantes de todas as partes interessadas.

Esta coordenação político-estratégica deve ser responsável pelo controlo e revisão da presente Estratégia e de cada uma das medidas que a compõe. A execução das medidas deve ser da responsabilidade de cada uma das partes, reportando periodicamente o seu estado de execução.

2) Consolidar o papel de coordenação operacional e de autoridade nacional em matéria de cibersegurança, relativamente às entidades públicas e às infraestruturas críticas, do Centro Nacional de Cibersegurança (CNCS):

a) Afirmar o exercício de poderes do CNCS, enquanto autoridade nacional competente em matéria de cibersegurança, relativamente às entidades públicas e às infraestruturas críticas nacionais;

b) A coordenação operacional é um fator essencial para o sucesso da execução das medidas previstas nesta estratégia. O CNCS assegura esta coordenação entre as várias partes responsáveis;

c) A segurança do ciberespaço pressupõe o conhecimento das ameaças e das vulnerabilidades existentes. Este conhecimento é essencial para a realização de análise de risco, com vista a uma melhor aplicação dos meios e recursos disponíveis para o tratamento dos riscos, bem como para a identificação das lacunas a colmatar;

d) O CNCS, enquanto coordenador operacional, deve desenvolver e aplicar medidas que visem a capacitação humana e tecnológica das infraestruturas públicas e das infraestruturas críticas, com vista à prevenção e à reação de e a incidentes de cibersegurança;

e) Com vista à eficácia operacional e a uma melhor avaliação situacional, devem ser criados mecanismos de reporte de incidentes de cibersegurança para entidades públicas e para os operadores de infraestruturas críticas. A desejada avaliação situacional resulta na criação de condições para a identificação de um nível de alerta nacional em matéria de segurança do ciberespaço, partilhado entre todas as entidades envolvidas;

f) Em articulação com as autoridades competentes e a comunidade nacional de segurança do ciberespaço, o CNCS deve criar uma base de conhecimento que reúna informação sobre ameaças e vulnerabilidades conhecidas, para servir as entidades públicas e os operadores de infraestruturas críticas;

g) O CNCS deve produzir e apresentar um quadro integral e atual dos incidentes, ameaças e vulnerabilidades que pendem sobre o ciberespaço nacional.

3) Desenvolver a capacidade de Ciberdefesa:

a) Concretizar a Orientação Política para a Ciberdefesa, aprovada pelo Despacho n.º 13692/2013, de 11 de outubro, publicado no Diário da República n.º 208, 2.ª série, de 28 de outubro, edificando a estrutura de ciberdefesa nacional;

b) Estabelecer e consolidar uma estrutura de comando e controlo da ciberdefesa nacional, recaindo as atribuições de orientação estratégica-militar da ciberdefesa sobre o Conselho de Chefes de Estado-Maior (CCEM) e o planeamento e resposta imediata e efetiva a uma crise no ciberespaço ao Centro de Ciberdefesa (CCD) e às capacidades dos ramos das Forças Armadas;

c) Implementar, 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;

d) Constituir a ciberdefesa uma área onde é necessário promover sinergias e potenciar o emprego dual das suas capacidades, no âmbito das operações militares e da cibersegurança nacional, desenvolvendo e consolidando um sistema de partilha de informação aos vários níveis e patamares de decisão.

4) Desenvolver a capacidade nacional de resposta a incidentes:

Num contexto de gestão distribuída como é o ciberespaço, a partilha de informação entre as partes interessadas é um fator crítico de sucesso para uma melhor deteção, prevenção e reação a falhas e interferências na segurança do ciberespaço.

a) O papel das comunidades de Computer Security Incident Response Team (CSIRT) deve ser reforçado como plataforma de excelência para a partilha de boas práticas e de informação relativa a ciberincidentes, para serviços operacionais de resposta a incidentes em Portugal e em território estrangeiro, neste caso, se constituir uma ameaça à soberania nacional.

b) Os diversos CSIRT devem usar uma taxonomia comum e mecanismos automáticos para partilha de informação operacional entre si e com as forças e serviços de segurança.

5) Estabelecer um gabinete para gestão de crises no ciberespaço:

a) A resposta a ciberincidentes de grande impacto requer instrumentos específicos e especializados. É essencial operacionalizar um gabinete de gestão de crises no ciberespaço, que se insira numa abordagem integrada na resposta às ameaças e riscos num efetivo sistema nacional de gestão de crises e que integre atores relevantes neste domínio;

b) Devem ser organizados e realizados exercícios nacionais de gestão de crises no ciberespaço, que permitam avaliar o grau de preparação e a maturidade das diversas entidades para lidar com incidentes de grande dimensão, potenciando as sinergias decorrentes da integração, sempre que possível, com outros exercícios neste âmbito, organizados e conduzidos a nível nacional.

6) Definir e implementar processos de governação da segurança do ciberespaço:

Deve ser elaborada uma proposta, considerando os vários domínios de atuação, contendo alterações legislativas e regulamentares, bem como mecanismos de autorregulação e de governação para a segurança do ciberespaço nacional.

Eixo 2 — Combate ao Cibercrime:

O ciberespaço criou novos bens jurídicos que carecem de proteção, novos tipos de crimes e, ainda, novas formas de realizar crimes antigos.

Os desafios colocados pelo cibercrime implicam uma permanente atualização da legislação em ordem à sua máxima eficiência. Da mesma forma, as instituições vocacionadas para a investigação do cibercrime devem estar plenamente apetrechadas para realizar a sua missão, importando ainda que o sistema judicial, como um todo, esteja adaptado às novas tecnologias. Assim, devem ser adotadas as seguintes medidas:

1) Revisão e atualização da legislação:

As entidades competentes devem adotar as medidas necessárias para a elaboração e operacionalização de legislação com vista à criminalização dos novos tipos de delitos — contra ou tirando proveito do ciberespaço —, e intensificando a cooperação judicial nacional e internacional.

No mesmo sentido, a legislação de suporte à investigação criminal deve ser objeto de constante atualização, tendo em vista uma eficaz aplicação no ciberespaço.

2) Agilizar as capacidades da Polícia Judiciária:

A Polícia Judiciária deve robustecer as suas estruturas e as suas capacidades técnicas e humanas para o combate ao cibercrime, assim como devem ser reforçadas as competências técnicas e forenses para conduzir investigações no ciberespaço.

Eixo 3 — Proteção do ciberespaço e das infraestruturas:

As ameaças às infraestruturas e aos sistemas de informação são dirigidas simultaneamente às entidades públicas e privadas e aos cidadãos. Os serviços públicos servem de exemplo para a sociedade e devem ser capazes de melhorar a proteção dos sistemas de informação e da informação pelos quais são responsáveis.

No âmbito da proteção do ciberespaço e de infraestruturas devem ser adotadas as seguintes medidas:

1) Avaliar a maturidade e a capacidade das entidades públicas e privadas que administrem infraestruturas críticas ou serviços vitais de informação, no que respeita à segurança do ciberespaço;

2) Promover a adaptação e melhoria contínua da segurança dos sistemas de informação das entidades públicas, dos operadores das infraestruturas críticas e dos serviços vitais de informação, para assegurar uma maior resiliência (capacidade de sobrevivência) nacional, adaptando-os aos novos riscos e ameaças do ciberespaço;

3) Analisar o ambiente de informação, para tentar antecipar eventuais ataques e tomar as decisões apropriadas, acompanhando os últimos desenvolvimentos tecnológicos e analisando e antecipando ameaças;

4) Desenvolver a capacidade de deteção de ataques aos sistemas de informação, especialmente os das entida-

des públicas e as infraestruturas críticas nacionais, a qual deve permitir alertar as entidades competentes, ajudar a entender a natureza dos ataques e criar as necessárias contramedidas;

5) Promover a aplicação, por parte das entidades públicas, das medidas necessárias à continuidade das operações, de modo a responder às principais crises que afetem ou ameacem a segurança dos sistemas de informação ou os operadores de infraestruturas críticas;

6) Incluir medidas de segurança do ciberespaço nos planos de proteção de infraestruturas críticas nacionais, seguindo uma abordagem baseada na gestão de risco;

7) Incluir medidas para fazer face a ameaças no ciberespaço nos planos de segurança dos operadores de infraestruturas críticas nacionais e europeias;

8) Promover a utilização de normas de segurança da informação nas infraestruturas e sistemas de informação e de comunicação das entidades públicas. A adoção de normas e boas práticas de segurança do ciberespaço funcionam, simultaneamente, como mecanismo de harmonização e de interoperabilidade e como instrumento de medida por referência;

9) Promover uma política de segurança da informação para as entidades públicas e criar instâncias que garantam a segurança da informação em todas essas entidades que acedam a informação sensível, a dados pessoais ou prestem serviços em linha considerados críticos, devendo a identificação das medidas de aplicação da política de segurança seguir uma abordagem de gestão de risco, de acordo com as melhores práticas internacionais;

10) Reforçar as capacidades de prevenção, deteção e reação a incidentes de segurança do ciberespaço. Os operadores de infraestruturas críticas têm o dever de reportar falhas e interferências de segurança do ciberespaço nos seus sistemas. Por outro lado, deve ser estabelecido, em cada um destes operadores, um conjunto de meios técnicos e humanos mínimos dedicados à função de segurança do ciberespaço. Estes meios devem funcionar em rede dentro e fora do setor de atividade;

11) Avaliar e desenvolver os quadros regulamentares setoriais;

12) Adaptar a legislação nacional, de forma a incorporar a evolução tecnológica e as novas práticas;

13) Garantir a proteção das infraestruturas de informação críticas, através de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN).

Eixo 4 — Educação, sensibilização e prevenção:

O sucesso da segurança do ciberespaço passa pela promoção de uma cultura de segurança que proporcione a todos o conhecimento, a consciência e a confiança necessários para a utilização dos sistemas de informação, reduzindo a exposição aos riscos do ciberespaço. É fundamental informar, sensibilizar e consciencializar não só as entidades públicas e as infraestruturas críticas, mas também as empresas e a sociedade civil. Por outro lado, é fundamental que o país se dote de recursos humanos qualificados para lidar com os complexos desafios da segurança do ciberespaço. No âmbito da educação, sensibilização e capacitação devem ser adotadas as seguintes medidas:

1) Promover campanhas de informação e alerta, tendo como alvos principais os cidadãos e as empresas;

2) Sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática;

3) Promover uma cultura de segurança do ciberespaço, através da promoção de campanhas e iniciativas de sensibilização para a segurança do ciberespaço coordenadas e desenvolvidas dentro de uma abordagem comum e positiva, que chame a atenção para os perigos e as ameaças da Internet e, em simultâneo, aponte soluções e medidas para os mitigar. Neste contexto, devem ser criados instrumentos e reforçadas as medidas de sensibilização da sociedade civil para a temática do uso seguro e responsável das TIC;

4) Reforçar a oferta de formação em segurança do ciberespaço. Reforçar a educação e formação de forma ampla e alargada, com o objetivo de, na estrutura curricular do ensino básico, secundário e superior, se criarem competências e conhecimentos para uma utilização segura das TIC;

5) Promover a utilização segura das TIC e do ciberespaço, dando particular importância à capacitação e conhecimento obtidos por adolescentes e pessoas idosas e outros grupos de risco;

6) Promover a formação especializada em matéria de segurança do ciberespaço, criando ou reforçando a oferta de cursos multidisciplinares, e adaptar as respetivas estruturas curriculares;

7) Promover formação especializada junto dos decisores e gestores públicos e de infraestruturas críticas, numa ótica de consciencialização e prevenção para a necessidade de salvaguardar os interesses e informação crítica nacional;

8) Estabelecer programas específicos para as Pequenas e Médias Empresas (PME), para as associações socioprofissionais e, em particular, para os profissionais liberais.

Eixo 5 — Investigação e desenvolvimento:

Tendo em conta a importância estratégica da segurança no ciberespaço, é fundamental apoiar, fomentar e potenciar as capacidades tecnológicas, para que sejam desenvolvidas soluções nacionais, seguras e confiáveis, que possam ser certificadas, permitindo assim potenciar a proteção dos sistemas perante as diversidades das ameaças. É crucial fomentar e apoiar todas as atividades e iniciativas de investigação e desenvolvimento, envolvendo empresas e indústria, entidades de investigação e academia. Assim, devem ser adotadas as seguintes medidas:

1) Promover a investigação científica e o desenvolvimento nos vários domínios da segurança do ciberespaço. A investigação científica e aplicada, bem como o desenvolvimento de soluções inovadoras são um importante fator para a segurança do ciberespaço. Deve ser promovida e incentivada a produção científica nas várias áreas do saber e no desenvolvimento de soluções aplicadas aos vários domínios de atuação;

2) Estimular e potenciar as capacidades científicas, técnicas, industriais e humanas do país, de forma a manter e afirmar a independência nacional neste domínio;

3) Apoiar a participação nacional em projetos internacionais;

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

5) Explorar a experiência recolhida pela participação das Forças Armadas em missões no exterior neste domínio, para, em colaboração com as universidades, centros de investigação e a indústria, desenvolver soluções tecnológicas com interesse para duplo uso civil militar;

6) Apoiar a participação da academia e das empresas nacionais em projetos de investigação e desenvolvimento internacionais.

Eixo 6 — Cooperação:

A segurança e defesa do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais ou internacionais. Responder aos desafios da segurança e defesa do ciberespaço requer uma abordagem em rede, pelo que a cooperação nacional e internacional nos diversos domínios de atuação é da maior importância. Para este eixo, devem ser adotadas as seguintes medidas:

1) Desenvolver iniciativas de cooperação. Desenvolver iniciativas de cooperação em áreas ligadas à segurança dos sistemas de informação, cibercrime, ciberdefesa e ciberterrorismo, ciberespionagem, ciberdiplomacia, de forma a potenciar o conhecimento necessário à proteção dos sistemas de informação nacionais;

2) Cooperar e colaborar multilateralmente. Neste contexto, devem ser reforçados os atuais mecanismos de cooperação multilateral, no âmbito nacional e internacional, designadamente, da União Europeia, no quadro da Estratégia europeia para a segurança do ciberespaço, e da Organização do Tratado do Atlântico Norte (OTAN), no âmbito da cibersegurança e ciberdefesa com os parceiros;

3) Participar e cooperar nos diversos fora de CSIRT. Os fora de CSIRT são instrumentos de partilha de informação e de geração da confiança necessária para a atividade de resposta a incidentes no ciberespaço. Deve ser promovida a participação nos principais fora de CSIRT;

4) Participação em exercícios. Os exercícios de segurança do ciberespaço permitem a avaliação e o desenvolvimento de capacidades doutrinárias e operacionais neste domínio. Deve ser fomentada a participação dos diversos atores nos principais exercícios de segurança e defesa do ciberespaço, nacionais e internacionais, designadamente no contexto da União Europeia e da OTAN.

Revisão da Estratégia:

A rápida evolução intrínseca ao ciberespaço e, consequentemente, a crescente evolução das ameaças, das vulnerabilidades, dos processos e das infraestruturas, bem como dos modelos económicos, sociais e culturais que assentam na sua utilização, exigem que a presente Estratégia seja objeto de revisão regular e periódica, considerando-se que, sem prejuízo de processos de revisão extraordinários, sempre que as circunstâncias o exijam, aquela deve ocorrer com a seguinte periodicidade:

a) Revisão num prazo máximo de três anos;

b) Verificação anual dos objetivos estratégicos e das linhas de ação e adequação dos mesmos à evolução das circunstâncias.

Resolução do Conselho de Ministros n.º 37/2015

Considerando que nos termos da Resolução do Conselho de Ministros n.º 127/2006, de 9 de outubro, foi autorizada a permuta do imóvel do Estado Português designado por «Jardim da Parada» por imóveis propriedade do Município de Cascais;

Considerando que a referida permuta não foi formalizada, na medida em que, por deliberação da Assembleia Municipal de Cascais, de 24 de setembro de 2012, que aprovou a proposta n.º 1444/2012, da reunião da respetiva Câmara Municipal, foi revogada a deliberação camarária de 26 de abril de 2006 que aprovou a permuta de imóveis com o Estado Português;

Considerando que, por deliberação da Assembleia Municipal de Cascais, de 27 de abril de 2015, foi aprovado um acordo quadro para a cooperação e a delegação de competências do Estado no Município de Cascais, cooperação no domínio do património — Ministério da Administração Interna, reiterando a intenção de prosseguir com a permuta do imóvel do Estado com alguns dos imóveis propriedade do Município, constantes da referida Resolução do Conselho de Ministros n.º 127/2006, de 9 de outubro;

Considerando que no imóvel designado por «Jardim da Parada», sito em Cascais, propriedade do Estado Português, o Município de Cascais construiu o «Museu do Mar» e a «Casa das Histórias»;

Considerando que, tendo em vista a construção de importantes infraestruturas coletivas, o Município de Cascais cedeu gratuitamente ao Estado Português, em regime de direito de superfície, um conjunto de imóveis no concelho de Cascais, destinados à construção de instalações para os serviços e forças de segurança pública, do Hospital de Cascais, e do Palácio da Justiça de Cascais;

Considerando que urge regularizar a situação jurídica do imóvel designado por «Jardim da Parada», tendo presente as construções promovidas pelo Município de Cascais, bem como consolidar na sua esfera jurídica o direito de propriedade plena sobre os imóveis nos quais se encontram instalados diversos serviços públicos;

Considerando que o Estado Português e o Município de Cascais mantêm a intenção alcançar este objetivo por meio de uma permuta;

Considerando que os imóveis a permutar foram objeto da competente avaliação, que os imóveis a adquirir se revestem de especial interesse para o Estado Português, e que o valor de avaliação dos imóveis a adquirir é inferior ao valor do imóvel dado em permuta, estando pela sua atual utilização por serviços públicos já previamente determinados, dando-se assim cumprimento ao disposto no artigo 107.º do Decreto-Lei n.º 280/2007, de 7 de agosto;

Considerando ainda que a competência para autorizar a permuta dos imóveis em apreço recai no Primeiro-Ministro, de acordo com as disposições conjugadas do n.º 3 do artigo 107.º e do n.º 3 do artigo 32.º do Decreto-Lei n.º 280/2007, de 7 de agosto, importa proceder à revogação da Resolução do Conselho de Ministros n.º 127/2006, de 9 de outubro;

Assim:

Nos termos do n.º 3 do artigo 32.º, do artigo 36.º e do artigo 107.º do Decreto-Lei n.º 280/2007, de 7 de agosto, e da alínea *g*) do artigo 199,º da Constituição, o Conselho de Ministros resolve:

1 — Autorizar a permuta, com dispensa de consulta ao mercado, do prédio urbano, propriedade do Estado Português, designado por «Jardim da Parada», sito em Cascais, inscrito na matriz predial urbana sob o artigo 15118, da União das Freguesias de Cascais e Estoril, descrito na 1.ª Conservatória do Registo Predial de Cascais sob o n.º 9571, da freguesia de Cascais, com o valor de € 4 050 000,00, pelos seguintes imóveis, propriedade do Município de Cascais, com o valor global de € 3 909 870,00:

a) Prédio urbano, sito na Avenida de Portugal, na Amoreira, Estoril, inscrito na matriz predial urbana da União