Quarta-feira, 10 de Dezembro de 2025 I Série – N.º 232

DIÁRIO DA REPÚBLICA

ÓRGÃO OFICIAL DA REPÚBLICA DE ANGOLA

Preço deste número - Kz: 1.190,00

SUMÁRIO

Presidente da República

Decreto Presidencial n.º 263/25 22523
Cria o Centro Nacional de Cibersegurança e aprova o respectivo Estatuto Orgânico.

Conselho Superior da Magistratura do Ministério Público

Resolução n.º 22/25 22540
Cessa as funções de Luís de Assunção Pedro da Mota Liz, Procurador-Geral Adjunto da República, no Órgão do Ministério Público junto da Câmara Criminal do Tribunal Supremo, João Simão Chapópia Leonardo, Procurador-Geral Adjunto da República, no Órgão do Ministério Público junto do Tribunal Constitucional, Neto Joaquim Neto, Procurador-Geral Adjunto da República, do cargo de Coordenador da Região Judiciária Norte, Astrigildo João Pedro Culolo, Procurador-Geral Adjunto da República, do cargo de Coordenador da Região Judiciária Leste, Betsabé Luísa de Jorge Jamba Nunes, Subprocuradora-Geral da República, do cargo de Coadjutora da Região Judiciária Noroeste da Procuradoria-Geral da República, Cláudia de Jesus Santos da Piedade, Subprocuradora-Geral da República, do cargo de Titular da Província do Icolo e Bengo, Deodato José Paim Santos Inácio, Subprocurador-Geral da República, do cargo de Titular da Província do Huambo, Mário Lombundo, Subprocurador-Geral da República, do cargo de Titular Interino da Província de Cabinda, Elias Chingueta, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Cuando, Pedro Raimundo Serra, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Cubango, Rosário Mateus João Baptista, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Cuanza Norte, Carlos André Vungula, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Cunene, Rui João da Luz, Subprocurador-Geral da República, do cargo de Titular Interino da Província da Lunda Norte, Rui José André, Subprocurador-Geral da República, do cargo de Titular Interino da Província da Lunda Sul, Olívia Patrícia Baptista Pedro António, Subprocuradora-Geral da República, do cargo de Titular Interina da Província de Malanje, José Brás leze Macosso, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Moxico, Eder Joaquim José, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Moxico Leste, Beatriz Sita Bento dos Santos, Subprocuradora-Geral da República, do cargo de Titular Interina da Província do Namibe, Isaac Nguendangongo Salvador Eduardo, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Uíge, Ricardo Jorge de Almeida Fernandes, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Zaire, Iracema Natacha Soares de Andrade, Subprocuradora-Geral da República, do cargo de Titular do Órgão do Ministério Público junto da Comarca de Belas, Elizabeth Irene Figueiredo, Subprocuradora-Geral da República, do cargo de Titular do Órgão do Ministério Público junto da 3.ª Secção da Sala Criminal, letras D e F do Tribunal da Comarca de Belas e Neusa Patrícia Dias Domingos Fonseca, Subprocuradora-Geral da República, colocada no Órgão do Ministério Público junto da 3.ª Secção da Sala do Trabalho do Tribunal da Comarca de Belas.

PRESIDENTE DA REPÚBLICA

Decreto Presidencial n.º 263/25

de 10 de Dezembro

Considerando que, no actual contexto de digitalização, a vida quotidiana dos cidadãos e o funcionamento da economia dependem, cada vez mais, das tecnologias digitais, expondo, apesar dos avanços, organizações e nações a novas e complexas ameaças cibernéticas;

Tendo em conta que a cibersegurança se tornou uma prioridade essencial para governos, empresas e utilizadores da Internet, configurando-se como um pilar fundamental para o progresso seguro e sustentável das sociedades modernas;

Atendendo que os conflitos no ciberespaço representam uma grave ameaça à soberania dos estados, dado o potencial de exploração do ciberespaço para ultrapassar fronteiras, causar prejuízos significativos e, inclusive, paralisar infra-estruturas críticas e serviços essenciais;

Havendo a necessidade de se reforçar a soberania digital, mediante a implementação de políticas e estratégias eficazes para mitigar as ameaças cibernéticas e proteger o ciberespaço nacional;

Atendendo ao disposto no artigo 18.º do Decreto Legislativo Presidencial n.º 2/20, de 19 de Fevereiro, que estabelece as Regras de Criação, Organização, Funcionamento, Avaliação e Extinção de Institutos Públicos;

O Presidente da República decreta, nos termos da alínea d) do artigo 120.º e do n.º 1 do artigo 125.º, ambos da Constituição da República de Angola, o seguinte:

ARTIGO 1.º

(Criação e aprovação)

É criado o Centro Nacional de Cibersegurança e aprovado o respectivo Estatuto Orgânico, anexo ao presente Diploma, de que é parte integrante.

ARTIGO 2.º

(Dúvidas e omissões)

As dúvidas e omissões suscitadas pela interpretação e aplicação do presente Decreto Presidencial são resolvidas pelo Presidente da República.

ARTIGO 3.º

(Entrada em vigor)

O presente Decreto Presidencial entra em vigor a partir da data da sua publicação.

Apreciado em Conselho de Ministros, em Luanda, aos 27 de Outubro de 2025.

Publique-se.

Luanda, aos 2 de Dezembro de 2025.

O Presidente da República, JOÃO MANUEL GONÇALVES LOURENÇO.

ESTATUTO ORGÂNICO DO CENTRO NACIONAL DE CIBERSEGURANÇA

CAPÍTULO I
Disposições Gerais

ARTIGO 1.º
(Definição e missão)

1. O Centro Nacional de Cibersegurança é uma pessoa colectiva de direito público responsável pela supervisão dos mecanismos de cibersegurança e de resiliência do ciberespaço nacional, assegurando a prevenção, detecção, resposta e recuperação de incidentes cibernéticos.

2. O Centro Nacional de Cibersegurança tem como missão contribuir para a melhoria do sistema tecnológico, desenvolvendo acções que incluem a protecção de infra-estruturas e serviços críticos de informação, a promoção de uma cultura de segurança cibernética e a conformidade com as normas e boas práticas internacionais, devendo, para o efeito, formular ao Órgão de Superintendência as recomendações no domínio das políticas tecnológicas e de informação que se mostrem necessárias.

ARTIGO 2.º
(Natureza jurídica)

O Centro Nacional de Cibersegurança é um instituto público dotado de personalidade jurídica, autonomia administrativa, financeira e patrimonial.

ARTIGO 3.º
(Âmbito)

1. O Centro Nacional de Cibersegurança exerce a sua actividade em todo o território nacional.

2. O Centro Nacional de Cibersegurança tem a sua sede em Luanda, podendo ser criados, nos termos do presente Diploma, Serviços Locais, tendo como base critérios de natureza geográfica, económica e de cibersegurança.

ARTIGO 4.º
(Superintendência)

1. O Centro Nacional de Cibersegurança funciona sob a superintendência do Titular do Poder Executivo, exercida pelo Titular do Departamento Ministerial responsável pelo Sector das Telecomunicações e Tecnologias de Informação.

2. O exercício da superintendência prevista no número anterior inclui os seguintes poderes:

a) Aprovar os planos estratégicos e anuais;

b) Acompanhar e avaliar os resultados das actividades;

c) Nomear e exonerar o Director-Geral, Directores-Gerais Adjuntos e demais responsáveis do Centro;

d) Apreciar o orçamento e os relatórios de actividade;

e) Aprovar os relatórios de balanço e demonstração da origem e aplicação de fundos;

f) Assinar, em nome da Administração Directa, o contrato-programa a celebrar;

g) Autorizar a aquisição ou a alienação de bens imóveis e a realização de operações de crédito, nos termos da lei;

h) Exercer o poder disciplinar sobre o Director-Geral e os Directores-Gerais Adjuntos;

i) Ordenar inquéritos ou sindicâncias aos serviços;

j) Aprovar e fazer publicar os regulamentos internos;

k) Suspender e revogar os actos dos órgãos de gestão que violem a lei;

l) Exercer as demais competências estabelecidas por lei ou por orientação superior.

ARTIGO 5.º

(Legislação aplicável)

O Centro Nacional de Cibersegurança rege-se pelo presente Estatuto, pelos seus regulamentos internos, pelas Regras de Criação, Organização, Funcionamento, Avaliação e Extinção de Institutos Públicos e pela legislação sobre cibersegurança, bem como pelas demais legislações aplicáveis, com as devidas adaptações, em função da sua natureza e especificidade.

ARTIGO 6.º

(Atribuições)

O Centro Nacional de Cibersegurança tem as seguintes atribuições:

a) Exercer as funções de regulação, regulamentação, supervisão, fiscalização e sancionatórias em matéria de cibersegurança;

b) Emitir instruções de cibersegurança e definir o nível nacional de alerta de cibersegurança;

c) Actuar em articulação com a Agência Nacional de Protecção de Dados, quando estejam em causa incidentes que tenham dado origem à violação de dados pessoais;

d) Realizar inspecções e auditorias técnicas em matéria de cibersegurança às entidades e instituições públicas e privadas, por iniciativa própria ou mediante solicitação das autoridades judiciárias, quando entender necessário, nos termos da legislação aplicável;

e) Elaborar a Estratégia Nacional de Cibersegurança;

f) Supervisionar, fiscalizar e auditar os padrões técnicos de redes e sistemas informáticos;

g) Dar suporte técnico aos trabalhos do Conselho Nacional de Cibersegurança;

h) Operar o CERT.ao;

i) Monitorizar e responder a incidentes cibernéticos em tempo real;

j) Criar normas técnicas obrigatórias para a segurança digital de órgãos públicos e privados;

k) Acompanhar a evolução de boas práticas técnicas e tendências específicas para cibersegurança e sua aplicabilidade e divulgação;

l) Promover a capacitação técnica no domínio da cibersegurança;

m) Exercer outras atribuições previstas na legislação aplicável.

ARTIGO 7.º

(Instrumentos vinculativos)

1. No exercício das suas atribuições, o Centro Nacional de Cibersegurança emite, com força de interpretação normativa, de assuntos correntes ou de instrução vinculativa, de cumprimento obrigatório pelas entidades supervisionadas, os seguintes instrumentos:

a) Circulares, de natureza regulamentar, sobre normas e regras técnicas, no âmbito das matérias que estejam especialmente atribuídas à sua competência pela legislação aplicável;

b) Deliberações tomadas no âmbito das matérias referentes a autorizações e aprovações, no exercício de atribuições que lhe sejam expressamente atribuídas pela legislação aplicável;

c) Instrutivos sobre as medidas resultantes da sua intervenção e fiscalização do mercado, para a regularização, pelas entidades supervisionadas, das situações detectadas.

2. Os instrumentos referidos no número anterior devem indicar as normas legais que habilitam a sua emissão pelo Centro Nacional de Cibersegurança e devem ser obrigatoriamente publicitados, através do *Diário da República* e de um jornal de circulação nacional.

ARTIGO 8.º

(Relações de cooperação com outros organismos)

1. O Centro Nacional de Cibersegurança deve manter relações com organizações internacionais de cibersegurança, bem como participar e representar o País em organizações e eventos internacionais no âmbito das suas atribuições.

2. O Centro Nacional de Cibersegurança deve manter relações com autoridades de outros Estados que exerçam funções de supervisão e de regulação das actividades concernentes à cibersegurança.

3. O Centro Nacional de Cibersegurança deve promover as diligências adequadas junto dos serviços da Administração Directa e Indirecta do Estado para a correcta prossecução das suas atribuições.

4. No cumprimento das suas atribuições, deve também solicitar a quaisquer serviços e organismos a colaboração, as informações e os esclarecimentos necessários para salvaguarda do cumprimento da legislação em matéria de cibersegurança.

5. O Centro Nacional de Cibersegurança deve prestar a colaboração solicitada por outras entidades públicas e privadas, nacionais, regionais ou internacionais, em conformidade com a lei e com as boas práticas do Sector.

6. O Centro Nacional de Cibersegurança deve comunicar, para os devidos efeitos legais, às entidades competentes a violação do dever de cooperação e promover as providências necessárias para corrigir a situação.

CAPÍTULO II
Organização em Geral

ARTIGO 9.º
(Estrutura orgânica)

O Centro Nacional de Cibersegurança compreende os seguintes órgãos e serviços:

1. Órgãos de Gestão e Fiscalização:
   a) Conselho Directivo;
   b) Director-Geral;
   c) Conselho Fiscal.
2. Serviços Executivos:
   a) Departamento de Resposta a Emergências Informáticas (CERT.ao*);*
   b) Departamento de Protecção de Infra-Estruturas Críticas e Serviços Essenciais;
   c) Departamento de Operações de Cibersegurança.
3. Serviços de Apoio Agrupados:
   a) Departamento de Apoio ao Director-Geral;
   b) Departamento de Administração e Serviços Gerais;
   c) Departamento de Comunicação, Inovação Tecnológica e Modernização dos Serviços;
   d) Serviços Locais.

CAPÍTULO III
Organização em Especial

SECÇÃO I
Órgãos de Gestão

ARTIGO 10.º
(Conselho Directivo)

1. O Conselho Directivo é o órgão colegial que delibera sobre a gestão permanente do Centro Nacional de Cibersegurança.

2. O Conselho Directivo é presidido pelo Director-Geral e integra os Directores-Gerais Adjuntos.

3. Em função da matéria a apreciar, o Director-Geral pode convidar para participar na reunião do Conselho Directivo qualquer responsável dos Serviços Executivos, de Apoio Agrupado e Locais, bem como os Chefes de Secção e técnicos do Centro Nacional de Cibersegurança, ou qualquer personalidade cujo parecer seja considerado relevante.

ARTIGO 11.º
(Competências do Conselho Directivo)

O Conselho Directivo tem as seguintes atribuições:

a) Aprovar e garantir a execução dos planos de actividades do Centro Nacional de Cibersegurança;

b) Aprovar os avisos, circulares, deliberações e instrutivos emitidos no exercício das suas atribuições;

c) Assegurar a execução do orçamento anual aprovado;

d) Aprovar o relatório e contas anuais e os balancetes;

e) Aprovar regulamentos internos, nos termos da lei;

f) Aceitar heranças, legados testamentários ou doações;

g) Aprovar a proposta sobre a aquisição, arrendamento, alienação e oneração de imóveis;

h) Emitir pareceres sobre qualquer disposição legal de cibersegurança;

i) Propor a celebração e a revisão de acordos, protocolos ou contratos com entidades públicas ou privadas nacionais ou internacionais, incluindo as entidades congéneres do exterior, que se mostrem adequados à elevação dos padrões de cibersegurança do País;

j) Dirigir, executar e fazer cumprir todos os actos necessários à prossecução dos objectivos, funções e atribuições do Centro Nacional de Cibersegurança.

ARTIGO 12.º
(Funcionamento)

1. O Conselho Directivo reúne-se, ordinariamente, de 15 (quinze) em 15 (quinze) dias e, extraordinariamente, sempre que convocado pelo Director-Geral.

2. O Conselho Directivo delibera através do voto favorável da maioria simples dos seus membros.

3. As actas das reuniões são aprovadas e assinadas por todos os membros presentes na reunião.

4. O Conselho Directivo rege-se por regulamento próprio.

ARTIGO 13.º
(Director-Geral)

1. O Director-Geral é o órgão executivo singular de gestão permanente que assegura e coordena a realização das actividades do Centro Nacional de Cibersegurança.

2. O Director-Geral é nomeado pelo Órgão de Superintendência e tem as competências seguintes:

a) Dirigir e coordenar os serviços do Centro Nacional de Cibersegurança;

b) Propor a nomeação dos responsáveis do Centro Nacional de Cibersegurança;

c) Preparar os instrumentos de gestão previsional e os relatórios de actividades, e submeter à aprovação da superintendência após parecer do Órgão de Fiscalização;

d) Gerir o quadro do pessoal e exercer poder disciplinar sobre o pessoal;

e) Representar o Centro Nacional de Cibersegurança e constituir mandatário para o efeito;

f) Solicitar a quaisquer entidades públicas ou privadas toda a colaboração ou auxílio que julgue necessários para o exercício das suas atribuições;

g) Controlar e garantir o pagamento das prestações pecuniárias do sistema de protecção social;

h) Assegurar a gestão financeira e patrimonial;

i) Remeter à superintendência a proposta de criação, extinção, alteração de localização e instalações de novos serviços locais;

j) Promover a realização de auditorias internas e externas para a análise e emissão de parecer sobre demonstrativos económico-financeiros e contabilísticos e sobre processamento de benefícios;

k) Aprovar e fazer publicar os regulamentos e instrumentos necessários à boa execução das leis, que não sejam da competência de outra entidade;

l) Exercer as demais competências estabelecidas por lei ou determinadas superiormente.

3. O Centro Nacional de Cibersegurança é representado, na prática de actos jurídicos, pelo Director-Geral, ou por mandatário especialmente designado, nos termos do presente Estatuto Orgânico.

4. Em situação de ausência ou impedimento, o Director-Geral é substituído pelo Director-Geral Adjunto por si designado.

ARTIGO 14.º
(Directores Gerais-Adjuntos)

1. Na prossecução das atribuições do Centro Nacional de Cibersegurança, o Director-Geral é coadjuvado pelos seguintes Directores-Gerais Adjuntos:

a) Director-Geral Adjunto para Área de Gestão Cibernética;

b) Director-Geral Adjunto para Área de Incidentes e Emergências.

2. Os Directores-Gerais Adjuntos são nomeados pelo Órgão de Superintendência, sob proposta do Director-Geral, e exercem as suas competências mediante delegação de poderes do Director-Geral.

SECÇÃO II
Órgão de Fiscalização

ARTIGO 15.º
(Conselho Fiscal)

1. O Conselho Fiscal é o órgão de controlo e fiscalização interna, ao qual cabe analisar e emitir pareceres de índole administrativa, financeira e patrimonial sobre a actividade do Centro Nacional de Cibersegurança.

2. O Conselho Fiscal é composto por três membros, sendo o Presidente indicado pelo Titular do Departamento Ministerial responsável pelo Sector das Finanças Públicas e dois Vogais indicados pelo Titular do Departamento Ministerial responsável pelo Sector de Telecomunicações, Tecnologias de Informação.

3. O Conselho Fiscal é nomeado por Despacho Conjunto dos Titulares dos Departamentos Ministeriais responsáveis pelo Sector das Finanças Públicas e de Telecomunicações, Tecnologias de Informação, para um mandato de três anos, renovável por igual período.

4. O Conselho Fiscal reúne-se ordinariamente uma vez por mês, e, extraordinariamente, sempre que convocado pelo seu Presidente ou por solicitação fundamentada de qualquer dos Vogais.

ARTIGO 16.º
(Competências)

O Conselho Fiscal tem as seguintes competências:

a) Apreciar e emitir, na data legalmente estabelecida, pareceres sobre as contas anuais, relatórios de actividades e sobre o orçamento do Centro Nacional de Cibersegurança;

b) Fiscalizar as finanças, a contabilidade e o património do Centro Nacional de Cibersegurança, nos termos da lei;

c) Proceder à verificação regular dos fundos existentes e fiscalizar a estruturação da contabilidade;

d) Remeter semestralmente aos Titulares do Departamento Ministerial responsável pelas Finanças Públicas e ao Órgão de Superintendência o relatório sobre a actividade de fiscalização e controlo desenvolvidos, bem como sobre o seu funcionamento;

e) Exercer as demais competências estabelecidas por lei ou determinadas superiormente.

SECÇÃO III
Serviços Executivos

ARTIGO 17.º
(Departamento de Resposta a Emergências Informáticas)

1. O Departamento de Resposta a Emergências Informáticas, doravante designado por CERT.ao, é a estrutura executiva central responsável pela coordenação e implementação das actividades operacionais de cibersegurança.

2. O Departamento de Resposta a Emergências Informáticas tem as seguintes competências:

a) Assegurar a prevenção, detecção, análise, resposta e mitigação de incidentes cibernéticos a nível nacional;

b) Assumir o papel de ponto focal para a articulação com a Rede de Equipas de Resposta a Incidentes de Segurança Informática (CSIRTs) sectoriais, institucionais e congéneres internacionais;

c) Exercer a coordenação operacional na resposta a incidentes, nomeadamente em articulação com as equipas de resposta a incidentes de segurança informática sectoriais existentes;

d) Monitorizar os incidentes com implicações a nível nacional;

e) Activar mecanismos de alerta rápido;

f) Intervir na reacção, análise e mitigação de incidentes;

g) Proceder à análise dinâmica dos riscos;

h) Coordenar a Rede de Equipas de Resposta a Incidentes de Segurança Informática (CSIRTs), assegurando a sua organização, funcionamento harmonizado, definição de protocolos operacionais comuns, bem como a promoção de sinergias entre os diversos CSIRTs sectoriais e institucionais, de forma a garantir uma resposta eficaz e articulada a incidentes de cibersegurança;

i) Assegurar mecanismos permanentes de cooperação, comunicação e troca de informações entre os CSIRTs sectoriais, institucionais e outras entidades relevantes, respeitando os princípios da confidencialidade, integridade e responsabilidade no tratamento da informação partilhada;

j) Assegurar a cooperação com entidades públicas e privadas;

k) Promover a adopção e a utilização de práticas comuns ou normalizadas;

l) Participar nos fóruns nacionais de cooperação de equipas de resposta a incidentes de segurança informática;

m) Assegurar a representação nacional nos fóruns internacionais de cooperação de equipas de resposta a incidentes de segurança informática;

n) Participar em eventos de treino nacionais e internacionais;

o) Exercer as demais competências estabelecidas por lei ou determinadas superiormente.

3. O Departamento de Resposta a Emergências Informáticas é dirigido por um Chefe de Departamento.

ARTIGO 18.º

(Departamento de Protecção de Infra-Estruturas Críticas e Serviços Essenciais)

1. O Departamento de Protecção de Infra-Estruturas Críticas e Serviços Essenciais é o serviço executivo responsável pela implementação de políticas, estratégias e medidas destinadas à protecção e resiliência das infra-estruturas críticas e serviços essenciais do País contra ameaças cibernéticas e outros riscos.

2. O Departamento de Protecção de Infra-Estruturas Críticas e Serviços Essenciais tem as seguintes competências:

a) Identificar e classificar as infra-estruturas críticas nacionais, de acordo com critérios técnicos e estratégicos;

b) Desenvolver e implementar planos nacionais de protecção para infra-estruturas críticas, em articulação com as entidades gestoras e operadores dessas infra-estruturas e serviços essenciais;

c) Monitorizar continuamente as condições de segurança das infra-estruturas críticas, identificando vulnerabilidades e propondo medidas correctivas;

d) Promover inspecções e auditorias técnicas regulares de segurança e resiliência em infra-estruturas críticas, emitindo relatórios e recomendações específicas;

e) Facilitar a troca de informações sobre ameaças e boas práticas entre os operadores de infra-estruturas críticas e as autoridades nacionais;

f) Implementar programas de formação e capacitação para profissionais responsáveis pela gestão de infra-estruturas críticas e serviços essenciais;

g) Conduzir simulações e exercícios de cenários de crise para testar a prontidão dos operadores e das entidades responsáveis;

h) Exercer as demais competências estabelecidas por lei ou determinadas superiormente.

3. O Departamento de Protecção de Infra-Estruturas Críticas e Serviços Essenciais é dirigido por um Chefe de Departamento.

ARTIGO 19.º
(Departamento de Operações de Cibersegurança)

1. O Departamento de Operações de Cibersegurança (DOC) é o serviço executivo, responsável pela monitorização, detecção, análise e resposta a incidentes de cibersegurança em tempo real.

2. O Departamento de Operações de Cibersegurança tem as competências:

a) Monitorizar continuamente as redes e sistemas informáticos para identificar e mitigar ameaças;

b) Detectar as actividades suspeitas e incidentes de segurança, com resposta imediata;

c) Analisar a correlação de eventos de segurança para identificar padrões e tendências;

d) Fornecer os relatórios e recomendações técnicas para fortalecer a postura de cibersegurança das organizações;

e) Dar apoio técnico e operacional a entidades públicas e privadas no tratamento de incidentes cibernéticos;

f) Exercer as demais competências estabelecidas por lei ou determinadas superiormente.

3. O Departamento de Operações de Cibersegurança é dirigido por um Chefe de Departamento.

4. O Departamento de Operações de Cibersegurança é integrado por técnicos especializados e operadores que funcionam em turnos rotativos de 24/24 horas por dia.

SECÇÃO IV
Serviços de Apoio Agrupados

ARTIGO 20.º
(Departamento de Apoio ao Director-Geral)

1. O Departamento de Apoio ao Director-Geral é o serviço ao qual incumbe realizar funções de secretariado, apoio técnico-jurídico, controlo interno, intercâmbio, protocolo e relações públicas.

2. O Departamento de Apoio ao Director-Geral tem as seguintes competências:

a) Controlar as actividades do Secretariado do Director-Geral;

b) Acompanhar a preparação e a organização das reuniões operativas;

c) Apoiar actividades protocolares;

d) Prestar apoio técnico-jurídico, intercâmbio e cooperação;

e) Cuidar dos aspectos logísticos e organizar toda a documentação referente a fóruns nacionais e internacionais e outros eventos relativos ao Centro Nacional de Cibersegurança, em que participe o Director-Geral e outros membros da Instituição;

f) Analisar os procedimentos de controlo interno do Centro Nacional de Cibersegurança e propor ao Director-Geral a adopção de medidas adequadas;

g) Proceder à aferição dos processos de trabalho da Instituição, exercendo acção fiscalizadora;

h) Verificar o cumprimento das disposições legais e propor a revisão ou substituição daquelas que se mostram inadequadas;

i) Emitir pareceres sobre os actos de fiscalização;

j) Realizar inquéritos, sindicâncias e inspecções quando determinado superiormente;

k) Realizar auditorias internas periódicas sobre todos os processos e elaborar o relatório final das auditorias internas;

l) Conduzir todo o processo de formação dos contratos públicos desencadeados pela Instituição nos termos da legislação em vigor;

m) Exercer as demais competências estabelecidas por lei ou determinadas superiormente.

3. O Departamento de Apoio ao Director-Geral é dirigido por um Chefe de Departamento.

ARTIGO 21.º

(Departamento de Administração e Serviços Gerais)

1. O Departamento de Administração e Serviços Gerais é o serviço de apoio técnico ao qual incumbe exercer as funções de planeamento, gestão orçamental, financeira e patrimonial, gestão de recursos humanos, manutenção de infra-estruturas e transportes.

2. O Departamento de Administração e Serviços Gerais tem as seguintes competências:

a) Gerir os serviços de natureza administrativa;

b) Velar pelo uso e conservação dos bens patrimoniais do Centro Nacional de Cibersegurança;

c) Recepcionar e expedir a correspondência da Instituição;

d) Garantir a higiene e limpeza da Instituição;

e) Manter o funcionamento em pleno dos equipamentos;

f) Zelar pelos serviços de transporte e alimentação do efectivo;

g) Organizar e manter o arquivo geral e garantir a reprodução de toda a documentação dos órgãos;

h) Propor e assegurar políticas de desenvolvimento dos recursos humanos;

i) Proceder à instauração de processos disciplinares;

j) Elaborar e gerir as políticas de gestão de recursos humanos;

k) Analisar o mercado de fornecedores de modo a encontrar soluções alternativas ou inovadoras;

l) Exercer as demais competências estabelecidas por lei ou determinadas superiormente.

3. O Departamento de Administração e Serviços Gerais é dirigido por um Chefe de Departamento.

ARTIGO 22.º

(Departamento de Comunicação, Inovação Tecnológica e Modernização dos Serviços)

1. O Departamento de Comunicação, Inovação Tecnológica e Modernização dos Serviços é o serviço de apoio técnico ao qual incumbe as funções no domínio da informática, modernização e inovação tecnológica, documentação, arquivo e informação.

2. O Departamento de Comunicação, Inovação Tecnológica e Modernização dos Serviços tem as seguintes competências:

a) Elaborar o plano estratégico e Director;

b) Elaborar o regulamento sobre o uso e conservação dos recursos tecnológicos em harmonização com o Órgão de Fiscalização da Instituição;

c) Apoiar tecnicamente a elaboração de cadernos de encargo, selecção, contratação, aquisição e instalação dos equipamentos de comunicação, informática, aplicações e serviços;

d) Avaliar, conceber e implementar o Plano de Infra-Estruturas de Telecomunicações e Tecnologias da Informação;

e) Desenvolver e dar suporte técnico às plataformas *Web* e redes sociais da Instituição;

f) Proceder à validação da documentação técnica, dos projectos tecnológicos;

g) Proceder ao levantamento e controlo periódico dos meios técnicos e elaborar os planos de inovação para a renovação dos recursos técnicos e tecnológicos;

h) Assessorar aos utilizadores na utilização dos recursos tecnológicos;

i) Definir e garantir a operacionalidade do fluxo de conteúdos, nomeadamente a forma de circulação da informação entre os distintos níveis;

j) Criar políticas de segurança, nomeadamente a confidencialidade, integridade e disponibilidade da informação, e mitigar ataques internos e externos;

k) Inserir as fichas e gerir o arquivo documental electrónico;

l) Exercer as demais competências estabelecidas por lei ou determinadas superiormente.

3. O Departamento de Comunicação, Inovação Tecnológica e Modernização dos Serviços é dirigido por um Chefe de Departamento.

CAPÍTULO IV

Serviços Locais

ARTIGO 23.º
(Serviços Locais)

1. Os Serviços Locais são unidades administrativas desconcentradas do Centro Nacional de Cibersegurança.

2. Sempre que se justifique, podem ser criados Serviços Locais do Centro Nacional de Cibersegurança.

CAPÍTULO V

Gestão Financeira e Patrimonial

ARTIGO 24.º
(Regime financeiro e instrumentos de gestão)

A gestão financeira do Centro Nacional de Cibersegurança é exercida de acordo com as normas vigentes no País e orientada na base dos seguintes instrumentos:

a) Plano de actividades anual e plurianual;

b) Orçamento próprio anual;

c) Relatórios de actividades;

d) Balanço e demonstração da origem e aplicação dos fundos.

ARTIGO 25.º

(Receitas)

1. Constituem receitas do Centro Nacional de Cibersegurança:

a) As dotações que lhe são atribuídas pelo Orçamento Geral do Estado;

b) Os subsídios e comparticipação atribuídos por quaisquer entidades públicas ou privadas, nacionais ou estrangeiras;

c) Produto das coimas decorrentes das contra-ordenações;

d) Outras receitas provenientes da sua actividade que por lei, contrato ou outro título lhe sejam atribuídos.

2. A receita arrecadada dá entrada na Conta Única do Tesouro (CUT) mediante a utilização da Referência Única de Pagamento ao Estado (RUPE).

3. O valor da receita arrecadada é revertido da seguinte forma:

a) 40% a favor do Tesouro Nacional;

b) 30% a favor do Centro Nacional de Cibersegurança;

c) 30% a favor do Fundo de Cibersegurança.

ARTIGO 26.º

(Despesas)

Constituem encargos do Centro Nacional de Cibersegurança os seguintes:

a) Todas aquelas que se destinam à aquisição de material cibernético ou para qualquer actividade relativa ao exercício das suas atribuições;

b) Aquisição de equipamentos;

c) Despesas com bens e serviços;

d) Despesas de carácter administrativo como salários, abonos, ajudas de custo, subsídios e outros encargos com o pessoal.

ARTIGO 27.º

(Património)

Constitui património do Centro Nacional de Cibersegurança o direito e obrigações, os bens imóveis e móveis recebidos ou adquiridos no âmbito das suas atribuições e actividades.

CAPÍTULO VI

Gestão de Pessoal

ARTIGO 28.º

(Quadro de pessoal)

1. O quadro de pessoal do Centro Nacional de Cibersegurança integra funcionários públicos e trabalhadores recrutados por contrato de trabalho.

2. O orçamento anual deve prever os recursos necessários para a promoção dos trabalhadores necessários, de acordo com planeamento anual de efectivo.

3. O quadro de pessoal dos Serviços Centrais e dos Locais constam dos Anexos I e II do presente Diploma que dele é parte integrante.

ARTIGO 29.º
(Organigrama)

O organigrama consta do Anexo III do presente Diploma, de é parte integrante.

ARTIGO 30.º
(Segredo profissional)

1. Os funcionários e trabalhadores do Centro Nacional de Cibersegurança, bem como as entidades que lhe prestem serviços por qualquer tipo de contrato devem guardar sigilo profissional dos factos ligados aos exercícios das suas funções ou que por causa delas tenham conhecimento.

2. O dever do sigilo profissional mantém-se ainda que as pessoas ou entidades a eles sujeitas, nos termos do número anterior, deixem de estar ao serviço.

3. Sem prejuízo da responsabilidade civil e criminal que dela resulte, a violação do dever de sigilo estabelecida no presente artigo, quando cometida por um membro dos órgãos e serviços ou pelo seu pessoal, implica para o infractor as sanções disciplinares correspondentes à sua gravidade que podem ir até à demissão e quando praticada por pessoa ou entidade vinculada ao Instituto por um contrato de prestação e serviços ou de outra natureza ao Instituto o direito de resolução imediata do contrato.

CAPÍTULO VII
Disposições Finais

ARTIGO 31.º
(Regulamento interno)

O Centro Nacional de Cibersegurança deve elaborar regulamentos internos para o correcto funcionamento dos seus órgãos e serviços, a ser aprovado por Decreto Executivo do Departamento Ministerial responsável pela Política de Tecnologias de Informação e Comunicações.

ANEXO I

Quadro de Pessoal dos Serviços Centrais do Centro Nacional de Cibersegurança, a que se refere o artigo 28.º do presente Diploma

Grupo	Categoria/cargo	Especialidade	N.º de lugares
Direcção e Chefia	Director Geral	Economia, Direito, Administração e Finanças, Estatística, Contabilidade, Recursos Humanos, Relações Internacional, Engenharia, Informática, Ciências da Computação.	1
	Directores Gerais-Adjuntos		2
	Chefes de Departamento		6
	Chefes de Secção		
Técnico Superior	Assessor principal	Economia, Direito, Administração e Finanças, Estatística, Contabilidade, Recursos Humanos, Relações Internacional, Engenharia, Informática e Ciências da Computação.	64
	1º Assessor		
	Assessor		
	Técnico Superior Principal		
	Técnico Superior de 1.ª Classe		
	Técnico Superior de 2.ª Classe		
Técnico	Técnico Especialista Principal	Economia, Direito, Administração e Finanças, Estatística, Recursos Humanos, Engenharia, Informática e Ciências da Computação.	40
	Técnico Especialista de 1.ª Classe		
	Técnico Especialista de 2.ª Classe		
	Técnico de 1.ª Classe		
	Técnico de 2.ª Classe		
	Técnico de 3.ª Classe		
Técnico Médio	Técnico Médio Principal de 1.ª Classe	Economia, Direito, Administração e Finanças, Estatística, Recursos Humanos, Contabilidade, Engenharia, Informática e Ciências da Computação, Secretariado, Relações Públicas e Arquivo	31
	Técnico Médio Principal de 2.ª Classe		
	Técnico Médio Principal de 3.ª Classe		
	Técnico Médio de 1.ª Classe		
	Técnico Médio de 2.ª Classe		
	Técnico Médio de 3.ª Classe		
Auxiliar	Motorista Principal	Motorista Profissional, Higiene e Segurança.	6
	Motorista de 1ª Classe		
	Motorista de 2.ª Classe		
	Auxiliar de Limpeza Principal		
	Auxiliar de Limpeza 1ª Classe		
	Auxiliar de Limpeza 2ª Classe		
TOTAL			**169**

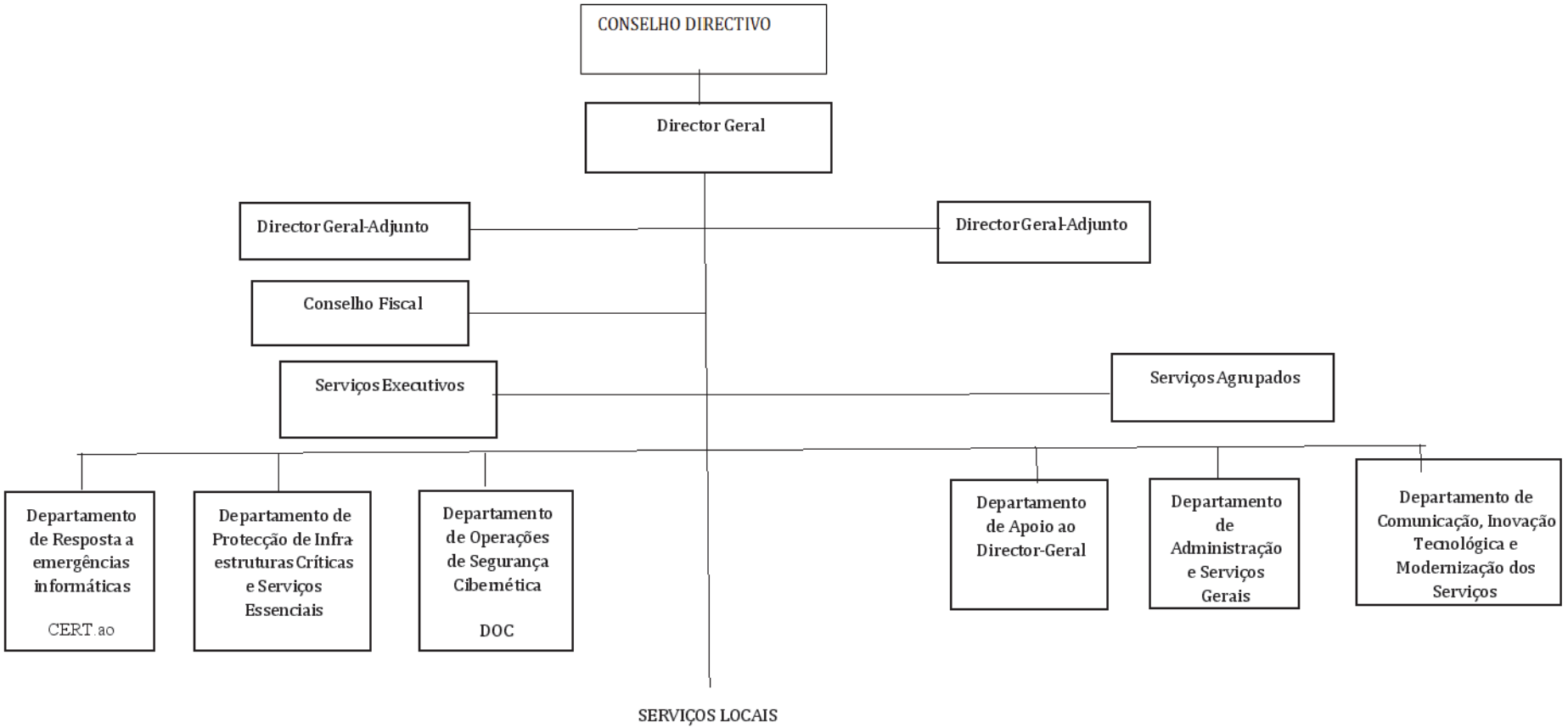
ANEXO II

Quadro de Pessoal dos Serviços Locais do Centro Nacional de Cibersegurança, a que se refere o artigo 28.º do presente Diploma

Grupo	Categoria/cargo	Especialidade	Número de lugares
Chefia	Chefe de Departamento	Economia, Direito, Administração e Finanças, Estatística, Contabilidade, Recursos Humanos, Relações Internacional, Engenharia e Informática	1
	Chefe de Secção		2
Técnico Superior	Assessor principal		
	1º Assessor	Economia, Direito, Administração e Finanças, Estatística, Contabilidade, Recursos Humanos, Relações Internacional, Engenharia e Informática	
	Assessor		10
	Técnico Superior Principal		
	Técnico Superior de 1.ª Classe		
	Técnico Superior de 2.ª Classe		
Técnico	Técnico de 1.ª Classe	Economia, Direito, Administração e Finanças, Estatística, Recursos Humanos, Engenharia e Informática	2
	Técnico de 2.ª Classe		
	Técnico de 3.ª Classe		
Técnico Médio	Técnico Médio Principal de 1.ª Classe	Economia, Direito, Administração e Finanças, Estatística, Recursos Humanos, Contabilidade, Engenharia, Informática e Logística, Transportes, Secretariado, Relações Pública e Arquivo	2
	Técnico Médio Principal de 2.ª Classe		
	Técnico Médio Principal de 3.ª Classe		
	Técnico Médio de 1.ª Classe		
	Técnico Médio de 2.ª Classe		
	Técnico Médio de 3.ª Classe		
Auxiliar	Motorista Principal	Motorista Profissional, Higiene e Segurança.	3
	Motorista de 1ª Classe		
	Motorista de 2.ª Classe		
	Auxiliar de Limpeza Principal		
	Auxiliar de Limpeza 1ª Classe		
	Auxiliar de Limpeza 2ª Classe		
TOTAL			**20**

ANEXO III

Organigrama do Centro Nacional de Cibersegurança, a que se refere o artigo 29.º do presente Diploma



O Presidente da República, JOÃO MANUEL GONÇALVES LOURENÇO.

(25-0522-C-PR)

CONSELHO SUPERIOR DA MAGISTRATURA DO MINISTÉRIO PÚBLICO

Resolução n.º 22/25

de 10 de Dezembro

O Conselho Superior da Magistratura do Ministério Público, reunido no dia 1 de Agosto de 2025, deliberou sobre a matéria de cessação da comissão de serviço de Magistrados do Ministério Público o seguinte:

1. Cessar, por conveniência de serviço, as funções de Luís de Assunção Pedro da Mota Liz, Procurador-Geral Adjunto da República, no Órgão do Ministério Público junto da Câmara Criminal do Tribunal Supremo, com efeitos imediatos;
2. Cessar, por conveniência de serviço, as funções de João Simão Chapópia Leonardo, Procurador-Geral Adjunto da República, no Órgão do Ministério Público junto do Tribunal Constitucional, com efeitos imediatos;
3. Cessar, por conveniência de serviço, as funções de Neto Joaquim Neto, Procurador-Geral Adjunto da República, do cargo de Coordenador da Região Judiciária Norte, com efeitos a partir do dia 1 de Setembro de 2025;
4. Cessar, por conveniência de serviço, as funções de Astrigildo João Pedro Culolo, Procurador-Geral Adjunto da República, do cargo de Coordenador da Região Judiciária Leste, com efeitos a partir do dia 1 de Setembro de 2025;
5. Cessar, por conveniência de serviço, as funções de Betsabé Luísa de Jorge Jamba Nunes, Subprocuradora-Geral da República, do cargo de Coadjutora da Região Judiciária Noroeste da Procuradoria-Geral da República, com efeitos imediatos;
6. Cessar, por conveniência de serviço, as funções de Cláudia de Jesus Santos da Piedade, Subprocuradora-Geral da República, do cargo de Titular da Província do Icolo e Bengo, com efeitos imediatos;
7. Cessar, por conveniência de serviço, as funções de Deodato José Paim Santos Inácio, Subprocurador-Geral da República, do cargo de Titular da Província do Huambo, com efeitos a partir do dia 1 de Setembro de 2025;
8. Cessar, por conveniência de serviço, as funções de Mário Lombundo, Subprocurador-Geral da República, do cargo de Titular Interino da Província de Cabinda;
9. Cessar, por conveniência de serviço, as funções de Elias Chingueta, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Cuando;
10. Cessar, por conveniência de serviço, as funções de Pedro Raimundo Serra, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Cubango;
11. Cessar, por conveniência de serviço, as funções de Rosário Mateus João Baptista, Subprocurador-Geral da República, do cargo de Titular Interino da Província do Cuanza-Norte;