

CONSELHO SUPERIOR DOS TRIBUNAIS ADMINISTRATIVOS E FISCAIS

Despacho (extrato) n.º 13595/2025

Sumário: Cria o NAIRC – Núcleo de Auditoria Interna, Risco e Cibersegurança, em aditamento ao Regulamento Interno do Conselho Superior dos Tribunais Administrativos e Fiscais.

Por despacho da Juíza-Secretária do Conselho Superior dos Tribunais Administrativos e Fiscais de 10 de novembro de 2025, tendo em conta o disposto no artigo 136.º, n.ºs 1 e 2, do CPA e artigo 11.º, n.º 4, do Decreto-Lei n.º 31/2023, de 5 de maio, foi criado o NAIRC – Núcleo de Auditoria Interna, Risco e Cibersegurança, concebido como unidade técnica de suporte estratégico à governação, transparência e resiliência digital dos tribunais, em aditamento ao Regulamento Interno do Conselho Superior dos Tribunais Administrativos e Fiscais CSTAF, com a seguinte redação:

Regulamento Interno do Conselho Superior dos Tribunais Administrativos e Fiscais

CAPÍTULO I

Disposições gerais

[...]

Artigo 3.º

Secção de expediente, arquivo, gestão informática e comunicação (SEAIC)

[...]

7) O serviço de gestão informática depende funcionalmente do Juiz-Secretário do Conselho Superior dos Tribunais Administrativos e Fiscais;

8) A dependência funcional direta do Juiz-Secretário do Conselho Superior dos Tribunais Administrativos e Fiscais impõe, todavia, ainda, o dever de reporte e a superintendência do Presidente do Conselho Superior dos Tribunais Administrativos e Fiscais.

Artigo 3.º-A

Núcleo de Auditoria Interna, Risco e Cibersegurança

1) É criado o Núcleo de Auditoria Interna, Risco e Cibersegurança (NAIRC) que é uma unidade técnica especializada integrada na Secretaria do CSTAF, mas funcionando sob dependência funcional do Gabinete de Apoio ao Presidente e ao Juiz-Secretário.

2) O NAIRC atua em articulação estruturada com o Gabinete Técnico-Jurídico (GTJ), o Encarregado de Proteção de Dados (EPD), o Núcleo de Acompanhamento da Gestão dos Tribunais do CSTAF e os Serviços de Informática, inseridos na Secção de expediente, arquivo, gestão informática e comunicação (SEAIC) da Secretaria do CSTAF.

3) O NAIRC assegura a dimensão tecnológica, digital, documental e procedural, de risco e de segurança transversal às áreas de auditoria interna, constituindo o núcleo especializado responsável pela auditoria digital e de conformidade eletrónica dos processos internos do CSTAF.

Artigo 3.º-B

Missão

A missão do NAIRC consiste em:

a) Garantir a segurança, integridade e conformidade dos sistemas procedimentais administrativos e fluxos digitais do CSTAF;

- b) Avaliar, prevenir e mitigar riscos operacionais, tecnológicos, financeiros, de gestão de recursos humanos, de gestão de contratos públicos, digitais e de compliance;
- c) Realizar auditorias especializadas em ambiente digital, documental, financeiro e de gestão de recursos humanos;
- d) Proteger os dados e assegurar a cibersegurança da infraestrutura digital do CSTAF;
- e) Verificar a rastreabilidade e integridade dos atos administrativos praticados em ambiente eletrónico;
- f) Apoiar a decisão dos órgãos do CSTAF mediante relatórios técnicos, avaliações de risco e pareceres especializados;
- g) Garantir o cumprimento do RGPD, do AI ACT, das normas ISO relevantes, das orientações do Tribunal de Contas e das melhores práticas de controlo interno geral.

Artigo 3.º-C

Auditoria Interna Digital, Financeira e de Recursos Humanos

- 1) Compete ao NAIRC:
 - a) Elaborar o Plano Anual de Auditorias,
 - b) Auditar os sistemas, fluxos administrativos e digitais associados aos procedimentos de gestão de recursos humanos, em especial:
 - i) Recrutamento, constituição de vínculos e mobilidade,
 - ii) Assiduidade, férias, faltas e licenças;
 - iii) Registos e processamentos remuneratórios, suplementos, trabalho suplementar e outros;
 - iv) Formação contínua,
 - v) Avaliação de desempenho e
 - vi) Acumulação de funções;
 - c) Auditar os sistemas administrativos e eletrónicos de gestão financeira e execução orçamental, incluindo:
 - i) Ciclo da despesa (cabimentação, compromisso, liquidação, pagamento);
 - ii) Registo de receita;
 - iii) Tesouraria;
 - iv) SNC-AP;
 - v) Execução orçamental;
 - vi) Prevenção de fraude financeira;
 - vii) Contratação pública digital;
 - d) Verificar a conformidade legal, digital e documental dos procedimentos internos do CSTAF, assegurando a legalidade procedural, a legalidade da despesa, a legalidade orçamental e financeira e a legalidade dos procedimentos administrativos de recursos humanos;
- 2) Compete ainda à auditoria à gestão de expediente e controlo documental do NAIRC, em especial:
 - a) Auditar os procedimentos de receção, registo, classificação, distribuição e arquivo de expediente em ambiente físico e digital;

- b) Verificar a integridade dos sistemas de arquivo digital e físico e dos mecanismos de controlo de acessos;
 - c) Avaliar a conformidade com CPA, LADA, RGPD, regulamentos internos e demais regulamentos europeus diretamente aplicáveis;
 - d) Auditar a tabela de temporalidade documental e critérios de conservação e eliminação;
 - e) Garantir a segurança geral e digital da documentação e a rastreabilidade dos atos administrativos;
- 3) Em matéria de acesso aos processos individuais dos magistrados judiciais de primeira instância, a sua inclusão num plano de auditoria trienal de auditoria interna, acompanhada de parecer do Encarregado de proteção de Dados, devidamente autorizada pelo Conselho Superior dos Tribunais Administrativos e Fiscais, é bastante;
- 4) Em matéria de acesso aos processos individuais dos magistrados judiciais dos tribunais superiores, apenas mediante uma autorização especial do Conselho Superior dos Tribunais Administrativos e Fiscais, devidamente fundamentada pelo Encarregado de proteção de dados, é possível ser autorizado o seu acesso para efeitos de uma auditoria interna;
- 5) Em matéria de Gestão Integrada do Risco Institucional, compete ao NAIRC:
- a) Elaborar e atualizar o Mapa de Riscos Institucional;
 - b) Identificar riscos operacionais, tecnológicos, financeiros, documentais e reputacionais;
 - c) Manter o registo de riscos de compliance;
 - d) Monitorizar o cumprimento das normas de controlo de risco (RGPD, ética, conflitos de interesse, prevenção da corrupção);
 - e) Emitir parecer prévio sobre alterações organizacionais ou tecnológicas com impacto no risco.

Artigo 3.º-D

Cibersegurança e Segurança da Informação

Compete ainda ao NAIRC:

- a) Monitorizar vulnerabilidades nos sistemas informáticos e plataformas digitais;
 - b) Realizar testes de intrusão, auditorias de segurança e análises de vulnerabilidade;
 - c) Avaliar perfis de acesso, permissões, logs e rastreabilidade dos utilizadores;
 - d) Elaborar planos de resposta a incidentes e assegurar a sua ativação em caso de necessidade;
 - e) Formar magistrados e trabalhadores em boas práticas de cibersegurança;
- f) No âmbito das Resposta a Incidentes e Recuperação, definir e ativar planos de resposta a incidentes de cibersegurança, com fluxos internos claros de reporte e atuação; colaborar com as autoridades competentes em caso de ataque ou violação (em especial com a Polícia Judiciária ou unidades de cibercriminais) – e assegurar a existência e a execução de procedimentos de backup, recuperação de sistemas e continuidade de operações em caso de falha ou ataque.
- g) Ao nível da Gestão de Risco Tecnológico e Documental, elaborar mapa de risco tecnológico, digital e documental, identificando vulnerabilidades, grau de impacto, probabilidade e definindo planos de mitigação, verificar a integridade documental em ambiente digital: acesso, controlo de versões, conservação, rastreabilidade e monitorizar e gerir contornos de risco ao archive digital e à gestão de dados pessoais sensíveis ou confidenciais.
- h) Elaborar relatórios trimestrais de auditoria digital, risco e cibersegurança;
- i) Emitir pareceres técnicos sempre que solicitado;

- j) Reportar imediatamente qualquer incidente grave ao Presidente e ao Juiz-Secretário;
- k) Assegurar um sistema de fiscalização do uso da IA pelos magistrados judiciais, garantindo que está em conformidade com as diretrizes europeias e constitucionais de:
 - i) Transparência e Explicabilidade: as operações do sistema de IA devem ser transparentes e inteligíveis, permitindo aos cidadãos compreenderem e contestarem os resultados.
 - ii) Não Discriminação e Equidade: devem ser prevenidas e ativamente combatidas práticas que promovam enviesamentos ou preconceitos algorítmicos, garantindo a utilização equitativa dos sistemas.
 - iii) Qualidade e Segurança: devem ser utilizados dados intangíveis e fontes certificadas, garantindo a integridade e robustez do sistema.
 - iv) Controlo Humano: a intervenção humana deve ser garantida e o sistema não pode restringir a autonomia do utilizador, permitindo aos profissionais rever as suas escolhas.

Artigo 3.º-E

Articulação com outros serviços

- 1) Compete ao NAIRC, no desempenho das suas funções, particularmente:
 - a) Executar auditorias conjuntas quando o objeto envolva, conjuntamente, sistemas digitais, financeiros, RH ou/e de contratação pública;
 - b) Realizar ações de seguimento conjuntas (follow-up) de recomendações cuja execução dependa de sistemas tecnológicos, em conjugação com as áreas da gestão de recursos humanos, gestão financeira e orçamental e da contratação pública.
- 2) Os auditores do NAIRC podem aceder a toda a informação julgada necessária ao desempenho pleno das suas competências e missão, sem prejuízo das limitações constantes no artigo 3.º C, n.ºs 3 e 4 do presente Regulamento interno.

Artigo 3.º-F

Plano Anual de Auditoria

- 1) O NAIRC elabora o Plano Anual de Auditorias, baseado nas avaliações de risco potencial, em cada área – gestão de recursos humanos, gestão financeira e orçamental, contratação pública e cibersegurança –, submetendo-o a parecer do Juiz-Secretário que os sujeita a aprovação do Presidente do Conselho Superior dos Tribunais Administrativos e Fiscais, até 30 de novembro do ano anterior à execução do plano.
- 2) O Plano Anual de Auditorias deverá conter o cronograma das ações e prazos de apresentação dos respetivos relatórios finais.
- 3) Até 31 de janeiro de cada ano será feito um Relatório Anual-Síntese de auditorias do ano anterior, subscrito por toda a equipa do NAIRC, sujeitando-o a parecer do Juiz-Secretário para posterior aprovação do Conselho Superior dos Tribunais Administrativos e Fiscais.
- 4) O Conselho Superior dos Tribunais Administrativos e Fiscais aprovará o Relatório-Síntese das auditorias do ano anterior até 31 de março.
- 5) Os relatórios de auditoria de dada ação devem incluir recomendações, depois de cumprido o direito de audiência prévia do serviço visado.
- 6) No ano seguinte à realização das auditorias, devem ser efetuadas ações de seguimento, para confirmar o grau de cumprimento das recomendações aprovadas pelo Presidente do Conselho Superior dos Tribunais Administrativos e Fiscais, devendo ser produzido Relatório-Síntese de Seguimento, a apresentar ao Conselho Superior dos Tribunais Administrativos e Fiscais até 15 de dezembro de cada ano.

7) O Conselho Superior dos Tribunais Administrativos e Fiscais apreciará Relatório-Síntese de Seguimento até 31 de março do ano seguinte.

8) As ações de auditoria devem desenvolver-se com o menor impacto funcional possível no serviço auditado.

Artigo 3.^º-G

Execução do Plano Anual

1) A execução do Plano Anual de Auditorias inicia-se com a comunicação ao serviço/secção/unidade objeto da ação do respetivo objeto e prazo de execução;

2) A ação de auditoria fica circunscrita ao seu objeto, desenvolvendo-se nos termos do procedimento administrativo;

3) O projeto de relatório deve ser notificado ao serviço visado para exercer o direito de audiência prévia, pelo prazo de 30 dias;

4) Após o exercício do direito de audiência prévia, é elaborado Relatório Final da ação;

5) Os Relatórios Finais de auditoria interna incluem avaliação de riscos, recomendações e prazos de implementação;

6) O Juiz-Secretário emitirá parecer submetendo o Relatório Final a aprovação do Conselho Superior dos Tribunais Administrativos e Fiscais.

7) Os relatórios de seguimento devem identificar a percentagem de cumprimento quanto às medidas implementadas, referindo expressamente as situações em que o seu cumprimento depende de terceiros.

8) Os relatórios de seguimento são sujeitos a parecer do Juiz-Secretário que os submeterá a aprovação do Conselho Superior dos Tribunais Administrativos e Fiscais.

10 de novembro de 2025. — A Juíza-Secretária do Conselho Superior dos Tribunais Administrativos e Fiscais, Eliana Cristina de Almeida Pinto.

319761606