TRIBUNAL DE CONTAS EUROPEU

Decisão nº 041-2021 do Tribunal de Contas sobre as regras de segurança aplicáveis à proteção das informações classificadas da UE (ICUE)

O TRIBUNAL DE CONTAS EUROPEU

TENDO EM CONTA o artigo 13º do Tratado da União Europeia,

TENDO EM CONTA o artigo 287º do Tratado sobre o Funcionamento da União Europeia,

TENDO EM CONTA o artigo 257º do Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho, de 18 de julho de 2018, relativo às disposições financeiras aplicáveis ao orçamento geral da União,

TENDO EM CONTA o artigo 1º, nº 6, das normas de execução do Regulamento Interno do Tribunal de Contas (Decisão nº 21-2021 do Tribunal de Contas),

TENDO EM CONTA as regras de segurança aplicáveis à proteção das informações classificadas da UE provenientes de outras instituições e organismos da União,

TENDO EM CONTA a política de segurança das informações do Tribunal de Contas (Decisão nº 127/15 final) e a política de classificação de informações (Comunicação ao Pessoal nº 123/2020),

CONSIDERANDO que, nos termos to artigo 287º, nº 3, do TFUE, o Tribunal de Contas tem o direito de aceder a todos os documentos e informações pertinentes que considere necessários para desempenhar o seu mandato, incluindo a informações classificadas da UE (ICUE), devendo tal acesso fazer-se no pleno respeito do princípio da cooperação leal entre as instituições e do princípio da atribuição. Este direito de acesso a ICUE, salvaguardado pelo TFUE, não pode ser questionado pela entidade de origem das ICUE, embora possa ser solicitado ao Tribunal de Contas que implemente e respeite determinadas medidas de segurança, conforme explicado em maior detalhe na presente decisão;

CONSIDERANDO que os Membros do Tribunal de Contas, bem como os seus funcionários e demais pessoal, estão vinculados, mesmo após cessarem funções, a uma obrigação de confidencialidade nos termos do artigo 339º do TFUE, do artigo 17º do Estatuto dos Funcionários e dos atos adotados para lhes dar cumprimento;

CONSIDERANDO que, atendendo à sua natureza sensível, o manuseamento de ICUE exige que se assegure o cumprimento da obrigação de confidencialidade através de medidas de segurança adequadas, passíveis de garantir um elevado nível de proteção destas informações e que sejam equivalentes às medidas implementadas pelas regras de proteção de ICUE adotadas pelas demais instituições e organismos da UE, sendo assente que, caso o Tribunal de Contas

considere que tais medidas de segurança não se justificam à luz da natureza e do tipo de ICUE, se reserva o direito de formular as observações que considere adequadas, respeitando embora o nível de classificação das ICUE;

CONSIDERANDO que as medidas de segurança destinadas a proteger a confidencialidade, integridade e disponibilidade das informações comunicadas ao Tribunal de Contas devem ser adequadas à natureza e ao tipo de informações em questão;

CONSIDERANDO que o acesso a informações classificadas deve ser concedido ao Tribunal de Contas em conformidade com o princípio da necessidade de tomar conhecimento, com vista ao desempenho das tarefas que lhe são atribuídas pelos Tratados e por atos jurídicos adotados com base nos mesmos;

CONSIDERANDO que, em virtude da natureza e do teor sensível de determinadas informações, é adequado criar um procedimento específico para efeitos de manuseamento, pelo Tribunal de Contas, de documentos que contenham ICUE;

CONSIDERANDO que a instituição tem de garantir a aplicação da presente decisão em conformidade com todas as regras aplicáveis, e em especial com as disposições relativas à proteção de dados pessoais, à segurança física das pessoas, edifícios e ativos informáticos e ao acesso público a documentos;

DECIDE:

Artigo 1º **Objeto e âmbito de aplicação**

1) A presente decisão estabelece os princípios básicos e as normas de segurança mínimas para a proteção das informações classificadas manuseadas pelo Tribunal de Contas no cumprimento do seu mandato.

2) Para efeitos da presente decisão, entende-se por "informações classificadas" um ou todos os seguintes tipos de informações:

   a) "informações classificadas da UE" (ICUE), conforme definidas nas regras de segurança de outras instituições, órgãos ou organismos da UE, e que ostentem uma das seguintes marcas de classificação de segurança:

      - TRÈS SECRET UE/EU TOP SECRET: informações e material cuja divulgação não autorizada possa causar danos excecionalmente graves para os interesses essenciais da União Europeia ou de um ou mais Estados-Membros;
      - SECRET UE/EU SECRET: informações e material cuja divulgação não autorizada possa prejudicar seriamente os interesses essenciais da União Europeia ou de um ou mais Estados-Membros;
      - CONFIDENTIEL UE/EU CONFIDENTIAL: informações e material cuja divulgação não autorizada possa prejudicar os interesses essenciais da União Europeia ou de um ou mais Estados-Membros;
      - RESTREINT UE/EU RESTRICTED: informações e material cuja divulgação não autorizada possa ser desfavorável aos interesses da União Europeia ou de um ou mais Estados-Membros.

b) as informações classificadas fornecidas pelos Estados-Membros e que ostentem uma marca de classificação nacional equivalente a uma das marcas de classificação de segurança das ICUE[1] indicadas na alínea a);

c) as informações classificadas fornecidas ao Tribunal de Contas Europeu por Estados terceiros ou organizações internacionais que ostentem uma marca de classificação de segurança equivalente a uma das marcas de classificação de segurança das ICUE indicadas na alínea a), de acordo com o previsto nos acordos relativos à segurança das informações ou nas disposições administrativas pertinentes.

3) O Tribunal de Contas manuseará, nas suas instalações, informações de nível RESTREINT UE/EU RESTRICTED, e tomará todas as medidas de proteção necessárias para o efeito. Devem ser adotadas disposições que assegurem que o pessoal do Tribunal de Contas que necessite de aceder a níveis mais elevados de ICUE o possa fazer em instalações adequadas de outras instituições ou organismos da UE.

4) A presente decisão é aplicável a todos os serviços e instalações do Tribunal de Contas.

5) Excetuando os casos em que uma disposição diga respeito a grupos de pessoal específicos, a presente decisão é aplicável aos Membros do Tribunal de Contas, ao pessoal do Tribunal de Contas abrangido pelo âmbito de aplicação do Estatuto dos Funcionários da União Europeia e pelo Regime Aplicável aos Outros Agentes da União Europeia[2], aos peritos nacionais destacados (PND) no Tribunal de Contas, aos prestadores de serviços e seu pessoal, aos estagiários e a qualquer pessoa com acesso aos edifícios ou outros bens do Tribunal de Contas ou a informações tratadas pelo Tribunal de Contas.

6) Salvo indicação em contrário, as disposições relativas a ICUE aplicam-se de forma idêntica às informações classificadas a que se refere o nº 2, alíneas b) e c), do presente artigo.

Artigo 2º **Definições**

Para efeitos da presente decisão, entende-se por:

a) "autorização de acesso a ICUE": uma decisão tomada pelo Diretor dos Recursos Humanos, Finanças e Serviços Gerais do Tribunal de Contas, com base na garantia dada por uma autoridade competente de um Estado-Membro de que pode ser facultado acesso a ICUE a um funcionário ou outro membro do pessoal do Tribunal de Contas, ou a um PND, até determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), e até determinada data, depois de estabelecida a necessidade de essa pessoa tomar conhecimento de tais informações e tendo a mesma sido adequadamente informada das responsabilidades que lhe incumbem; diz-se da pessoa em questão que "possui autorização de segurança".

b) "classificação": a atribuição de um nível de classificação a informações, com base no grau de prejuízo suscetível de ser causado pela sua divulgação não autorizada;

---

[1] Ver o Acordo entre os Estados-Membros da União Europeia, reunidos no Conselho, sobre a proteção das informações classificadas trocadas no interesse da União Europeia, de 4 de maio de 2011, bem como o respetivo anexo (JO 2011/C 202/13).

[2] Regulamento nº 31 (CEE) que fixa o Estatuto dos Funcionários e o Regime aplicável aos outros agentes da Comunidade Económica Europeia e da Comunidade Europeia da Energia Atómica, alterado, JO 01962R0031-1.1.2020-019.003-1 (https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:01962R0031-20140501&from=EN).

c) "material criptográfico": algoritmos criptográficos, módulos criptográficos de hardware e software, e produtos que incluam regras de aplicação e documentação conexa, bem como material de cifragem;

d) "desclassificação": a eliminação de qualquer classificação de segurança;

e) "documento": qualquer informação registada, independentemente da sua forma ou das suas características físicas;

f) "desgraduação": uma redução do nível de classificação de segurança;

g) "Credenciação de Segurança da Empresa" (CSE): uma decisão administrativa, emitida por uma autoridade de segurança competente, de que, do ponto de vista da segurança, determinada entidade está apta a garantir um nível adequado de proteção das ICUE a um nível de classificação de segurança específico.

h) "manuseamento": todas as ações a que as ICUE possam ser sujeitas ao longo do seu ciclo de vida: produção, registo, tratamento, transporte, desgraduação, desclassificação e destruição. Em relação aos sistemas de comunicação e informação (SCI), compreende igualmente a sua recolha, visualização, transmissão e armazenamento;

i) "detentor": uma pessoa devidamente autorizada com necessidade comprovada de tomar conhecimento, que está na posse de informações classificadas e é consequentemente responsável pela sua proteção;

j) "autoridade para a segurança das informações": o Responsável pela Segurança das Informações do Tribunal de Contas, que pode delegar total ou parcialmente as atribuições previstas na presente decisão;

k) "informações": qualquer informação escrita ou oral, independentemente do suporte ou do autor;

l) "material": qualquer meio, suporte de dados ou peça de maquinaria ou equipamento;

m) "entidade de origem": uma instituição, órgão ou agência da UE, um Estado-Membro, um Estado terceiro ou uma organização internacional sob cuja autoridade as informações tenham sido produzidas e/ou introduzidas nas estruturas da União;

n) "Credenciação de Segurança do Pessoal" (CSP): uma declaração de uma autoridade competente de um Estado-Membro, feita depois de concluída uma investigação de segurança conduzida pelas autoridades competentes de um Estado-Membro, pela qual se atesta que uma dada pessoa pode aceder a ICUE até determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), e até determinada data, depois de comprovada a necessidade de essa pessoa tomar conhecimento de tais informações e tendo a mesma sido devidamente informada das responsabilidades que lhe incumbem;

o) "Certificado de Credenciação de Segurança do Pessoal" (CCSP): um certificado emitido pelo Diretor dos Recursos Humanos, Finanças e Serviços Gerais do Tribunal de Contas pelo qual se atesta que uma dada pessoa possui uma credenciação de segurança válida ou uma autorização de segurança e que indica o nível de ICUE a que a pessoa pode aceder (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), a data de validade da credenciação ou autorização de segurança pertinente e a data de caducidade do próprio certificado;

p) "autoridade de segurança física": o Responsável pela Segurança do Tribunal de Contas, a quem incumbirá adotar as medidas de segurança física e os procedimentos necessários para proteger as ICUE;

q) "Serviço de Registos": um serviço gerido pelo Secretariado do Tribunal, situado numa Zona Administrativa, e sob a alçada do Diretor dos Recursos Humanos, Finanças e Serviços Gerais do Tribunal de Contas. É responsável pela entrada e saída de informações RESTREINT UE/EU RESTRICTED, ou informações equivalentes, comunicadas pelo/ao Tribunal de Contas.

r) "Registo das ICUE": uma área criada dentro de uma Zona de Segurança. Este Registo será gerido pelo Responsável do Controlo do Registo – autorizado e com credenciação de segurança – do Tribunal de Contas, sendo responsável pela entrada e saída de informações CONFIDENTIEL UE/EU CONFIDENTIAL, ou informações equivalentes, comunicadas pelo/ao Tribunal de Contas.

s) "Autoridade de Acreditação de Segurança (AAS)": o Diretor dos Recursos Humanos, Finanças e Serviços Gerais do Tribunal de Contas.

Artigo 3º **Medidas para proteger ICUE**

1) O Tribunal de Contas deve assegurar que todas as informações classificadas por si recebidas são protegidas de forma proporcional ao nível de classificação determinado pela entidade de origem e em conformidade com a presente decisão.

2) Para tal, o Tribunal de Contas deve sujeitar o manuseamento de ICUE a medidas de segurança físicas e, se for caso disso, a medidas de segurança adequadas relativas ao pessoal, incluindo autorizações de acesso para as pessoas identificadas e medidas para a proteção de sistemas de comunicação e informação. Tais medidas são descritas nos artigos 4º a 6º e devem aplicar-se ao longo do ciclo de vida das ICUE. Devem ser proporcionais, em particular, à classificação de segurança das ICUE, à forma e ao volume das informações ou do material, à localização e construção dos estabelecimentos nos quais as ICUE são armazenadas e à avaliação local da ameaça de atos mal-intencionados e/ou atividades criminosas, nomeadamente de espionagem, sabotagem e terrorismo.

3) As ICUE devem ser protegidas através de medidas de segurança física, e as informações classificadas como CONFIDENTIEL UE/EU CONFIDENTIAL devem, para além disso, ser protegidas por medidas de segurança relativas ao pessoal.

4) As ICUE apenas podem ser fornecidas a pessoas da instituição que necessitem de tomar conhecimento das mesmas. O detentor de qualquer elemento de ICUE deve protegê-lo conforme exigido pela presente decisão.

5) As ICUE não devem ser divulgadas oralmente ou por escrito. As observações preliminares, relatórios, pareceres, comunicados de imprensa e outros produtos do Tribunal de Contas, bem como o seu sítio Web e intranet, intervenções orais, respostas a pedidos de acesso a documentos[3] e gravações de voz ou de vídeo não devem conter nem fazer referência a ICUE ou a excertos das mesmas. No entanto, caso a entidade de origem tenha publicado documentos ou informações que incluam uma referência a ICUE, essa referência pode ser mencionada.

6) Não obstante o disposto no nº 5, o Tribunal de Contas e a entidade de origem poderão concordar que, no caso de uma auditoria específica, o Tribunal pode reproduzir ou utilizar elementos de ICUE num documento. Se tal acontecer, o documento do Tribunal de Contas deve ser primeiro enviado à entidade de origem das ICUE em questão antes ou durante o processo contraditório. Nesta situação, o Tribunal de Contas e a entidade de origem devem chegar a acordo quanto à necessidade de classificar o documento emitido pelo Tribunal. Caso um Membro do Tribunal de Contas, atuando como relator, considere necessário comunicar um relatório de auditoria total ou parcialmente classificado no que se refere a determinados destinatários do Parlamento Europeu ou do Conselho – tendo em conta todas as medidas de segurança associadas à presente decisão –, tal comunicação exigirá o consentimento da

[3] Nos termos da Decisão nº 12-2005 do Tribunal de Contas relativa ao acesso do público aos documentos do Tribunal de Contas, alterada pela Decisão nº 14-2009 (JO 2009/C 67/1).

entidade de origem das informações classificadas. O quadro jurídico e o procedimento aplicáveis à transmissão desses documentos são descritos no artigo 7º.

7) Sempre que o exercício do seu mandato exija uma partilha mais ampla de determinados elementos de informações ou documentos classificados, o Tribunal de Contas deve, tendo em devida conta a marca de classificação de segurança, consultar a entidade de origem antes de decidir utilizar tais elementos ou informações, caso considere que essa utilização tem por base um interesse público prevalecente. As informações apenas serão utilizadas no relatório de uma forma que não lese os interesses da entidade de origem. O que precede pode ser devidamente acautelado solicitando à entidade de origem que forneça comentários para se chegar a acordo quanto à forma de anonimizar, condensar ou generalizar as informações, etc., e, ao mesmo tempo, respeitar os interesses dos principais visados pelas informações publicadas.

8) O Tribunal de Contas não fornece ICUE a outras instituições, órgãos ou organismos da UE, nem a qualquer Estado-Membro, Estado terceiro ou organização internacional, sem primeiro consultar a entidade de origem e obter o seu consentimento expresso por escrito.

9) A menos que a entidade de origem de um documento classificado como SECRET UE/EU SECRET ou de nível inferior tenha aplicado restrições à sua replicação ou tradução, tais documentos podem ser replicados ou traduzidos a pedido do detentor e em conformidade com as instruções de trabalho práticas da autoridade para a segurança das informações do Tribunal de Contas. As medidas de segurança aplicáveis ao documento original são igualmente aplicáveis às respetivas cópias e traduções.

10) Caso o Tribunal de Contas precise que um documento classificado por si recebido, ou ao qual tenha direito de acesso, seja desgraduado ou desclassificado, deverá consultar a entidade de origem, solicitando-lhe se pode fornecer uma versão desgraduada ou desclassificada do documento.

Artigo 4º Requisitos de segurança do pessoal

1) Por força das funções que desempenham, os Membros do Tribunal de Contas devem ser autorizados a aceder a todas as ICUE, bem como a participar em reuniões nas quais sejam manuseadas ICUE. O Membros devem ser informados das suas obrigações de segurança em matéria de proteção de ICUE, devendo reconhecer, por escrito, que são responsáveis por proteger tais informações.

2) Um membro do pessoal do Tribunal de contas, seja ele um funcionário, um membro do pessoal sujeito ao Estatuto dos Funcionários ou um PND, apenas deverá ter o direito de aceder a ICUE após:

   i. ter ficado estabelecida a sua necessidade de tomar conhecimento de tais informações;

   ii. ter sido informado das regras de segurança aplicáveis à proteção das ICUE e das normas e orientações de segurança pertinentes e ter reconhecido, por escrito, as suas responsabilidades no que respeita à proteção dessas informações;

   iii. no caso das informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, após lhe terem sido concedidas credenciação de segurança e autorização de acesso.

3) O procedimento para determinar se um funcionário ou outro membro do pessoal do Tribunal de Contas pode ser autorizado a aceder a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, tendo em conta a lealdade, integridade e fiabilidade da pessoa, e

após a obtenção de garantias das autoridades competentes de um Estado-Membro, conforme referido no artigo 2º, alínea n), deve ser estabelecido numa decisão delegada adotada em conformidade com o artigo 10º, nº 10. As decisões de concessão de autorização de acesso devem ser tomadas pelo Diretor dos Recursos Humanos, Finanças e Serviços Gerais do Tribunal de Contas.

4) O Diretor dos Recursos Humanos, Finanças e Serviços Gerais do Tribunal de Contas pode emitir CCSP que especifiquem o nível de classificação das ICUE a que a pessoa pode aceder (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), a data de validade da respetiva autorização de acesso e a data de caducidade do CCSP.

5) Apenas as pessoas que possuam a autorização a que se refere a alínea iii) do nº 2 acima, bem como os Membros do Tribunal de Contas, nos termos do nº 1, podem participar em reuniões nas quais sejam manuseadas informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior. O Tribunal de Contas e a entidade de origem devem estipular, caso a caso, as modalidades práticas aplicáveis a tais reuniões.

6) Os serviços do Tribunal de Contas responsáveis por organizarem reuniões nas quais serão manuseadas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior devem informar atempadamente a autoridade para a segurança das informações acerca das datas, horas e locais dessas reuniões, fornecendo também as listas de participantes.

7) Qualquer pessoa que se encontre na posse de ICUE sem a devida autorização e/ou sem ter necessidade de tomar conhecimento dessas informações é obrigada a comunicar o mais depressa possível a situação à autoridade para a segurança das informações, bem como a certificar-se de que as ICUE são protegidas conforme exigido pela presente decisão.

Artigo 5º Medidas de segurança física destinadas a proteger informações classificadas

1) Por "segurança física" entende-se a utilização de medidas de proteção física e técnica para impedir o acesso não autorizado a informações classificadas da UE.

2) Devem ser concebidas medidas de segurança física que permitam impedir a entrada sub-reptícia ou forçada de intrusos, dissuadir, impedir e detetar ações não autorizadas e permitir uma diferenciação do pessoal no que se refere ao acesso a ICUE, segundo o princípio da necessidade de tomar conhecimento de tais informações. Essas medidas devem ser determinadas com base num procedimento de gestão do risco, implementado em conformidade com a presente decisão.

3) As zonas onde se proceda ao manuseamento ou armazenamento de ICUE são periodicamente inspecionadas pela autoridade de segurança competente do Tribunal de Contas.

4) Para efeitos de manuseamento e armazenamento das ICUE apenas devem ser utilizados os equipamentos e os dispositivos que cumpram as regras de proteção de ICUE aplicáveis no seio das instituições ou organismos da UE.

5) O pessoal do Tribunal de Contas pode aceder a ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, ou a informações equivalentes, nas Zonas de Segurança situadas fora das instalações do Tribunal de Contas.

6) O Tribunal de Contas pode celebrar um contrato de nível de serviço com outra instituição da UE situada no Luxemburgo com vista a poder manusear e armazenar informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior numa Zona de Segurança dessa instituição. Salvo nos casos em que a entidade de origem o tenha consentido especificamente,

as ICUE não devem ser manuseadas ou armazenadas nas instalações do Tribunal de Contas, que tampouco as deve replicar ou traduzir.

7) As informações com classificação RESTREINT UE/EU RESTRICTED devem ser registadas pelo Tribunal de Contas. Por motivos de segurança, deve proceder-se ao registo das consultas de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, ou informações equivalentes, realizadas fora das instalações do Tribunal de Contas.

8) As ICUE classificadas como RESTREINT UE/EU RESTRICTED podem ser armazenadas em mobiliário de escritório apropriado e fechado à chave, numa Zona Administrativa ou numa Zona de Segurança. As ICUE classificadas como CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET devem ser armazenadas, nos termos de um acordo de nível de serviço, num recipiente de segurança mantido numa Zona de Segurança de outra instituição da UE situada no Luxemburgo.

9) Sempre que se encontrem fora do registo, as ICUE devem ser transferidas entre serviços e instalações da seguinte forma:

   a) as ICUE são, regra geral, transmitidas por meios eletrónicos protegidos por produtos criptográficos aprovados nos termos do artigo 6º, nº 8;

   b) se não foram transmitidas conforme descrito na alínea a), as ICUE devem ser transferidas com recurso a um suporte de dados (por exemplo, um dispositivo de armazenamento USB, um CD ou um disco rígido) protegido por produtos criptográficos aprovados nos termos do artigo 6º, nº 8, ou sob a forma de uma cópia em formato de papel, armazenada num envelope opaco selado.

10) As informações com classificação RESTREINT UE/EU RESTRICTED podem ser destruídas pelo detentor, sob reserva das regras de arquivamento aplicáveis no Tribunal de Contas. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior apenas devem ser destruídas pelo Responsável do Controlo do Registo, após ter recebido instruções nesse sentido dadas pelo detentor ou por uma autoridade competente, em conformidade com as regras de arquivamento aplicáveis no Tribunal de Contas. Os documentos classificados como SECRET UE/EU SECRET devem ser destruídos na presença de uma testemunha que tenha credenciação de segurança correspondente, no mínimo, ao nível de classificação do documento a destruir. O Responsável do Controlo do Registo e, se for caso disso, a testemunha, devem assinar um registo da destruição, que deve ser arquivado no registo. O Responsável do Controlo do Registo mantém por um mínimo de cinco anos registos da destruição dos documentos classificados como CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET.

11) A autoridade de segurança física e a autoridade para a segurança das informações devem elaborar um plano conjunto, que tenha em conta as condições locais, destinado a salvaguardar as ICUE em momentos de crise, incluindo, se for esse o caso, planos para a destruição ou evacuação de tais informações em caso de emergência. Essas autoridades devem publicar as instruções que considerem adequadas para impedir que as ICUE possam chegar às mãos de pessoas não autorizadas.

12) Se for necessário transportar fisicamente ICUE, o Tribunal de Contas deve cumprir as medidas impostas pela entidade de origem com vista a proteger essas informações de divulgação não autorizada durante o transporte.

13) O anexo estabelece as medidas de segurança física aplicáveis nas Zonas Administrativas em que sejam manuseadas e armazenadas informações com a classificação RESTREINT UE/EU RESTRICTED.

<u>Artigo 6º</u> **Proteger ICUE no âmbito dos sistemas de comunicação e informação**

1) Para efeitos do presente artigo, por "sistema de comunicação e informação" entende-se qualquer sistema que possibilite o manuseamento de ICUE em formato eletrónico. Um sistema de comunicação e informação compreende todos os meios necessários ao seu funcionamento, designadamente a infraestrutura, a organização, o pessoal e os recursos em matéria de informação.

2) Por "utilizador legítimo" entende-se um Membro, funcionário ou outro membro do pessoal do Tribunal de Contas, ou ainda um PND, com uma necessidade estabelecida e reconhecida de acesso a um determinado sistema de informação.

3) O Tribunal de Contas deve dar garantias de que os seus sistemas protegerão a um nível adequado as informações por si manuseadas e funcionarão conforme necessário, nas alturas devidas e sob o controlo de utilizadores legítimos. Para tal, deve garantir níveis adequados de:

- autenticidade – a garantia de que a informação é genuína e provém de fonte fidedigna;
- disponibilidade – a propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada;
- confidencialidade – a propriedade de a informação não ser divulgada a pessoas ou entidades não autorizadas ou segundo processos não autorizados;
- integridade – a propriedade de salvaguardar o caráter exato e completo dos ativos e da informação;
- não rejeição – a capacidade de provar que um ato ou acontecimento teve lugar, de modo a que esse ato ou evento não possa ser subsequentemente negado.

Esta garantia baseia-se num processo de gestão do risco. Por "risco" entende-se a possibilidade de uma ameaça específica explorar as vulnerabilidades internas e externas de uma organização ou de um dos sistemas por ela utilizados, causando assim danos à organização e respetivos ativos corpóreos ou incorpóreos. Mede-se pela combinação da probabilidade de as ameaças ocorrerem e do respetivo impacto. O processo de gestão do risco consiste nas seguintes etapas: identificação das ameaças e vulnerabilidades, avaliação do risco, tratamento do risco, aceitação do risco e comunicação do risco.

- Por "avaliação do risco" entende-se a identificação das ameaças e vulnerabilidades e realização da análise de risco correspondente, ou seja, a avaliação da probabilidade e do impacto;
- Por "tratamento do risco" entende-se a atenuação, eliminação, redução (mediante uma combinação adequada de medidas técnicas, materiais, organizativas e processuais), transferência ou acompanhamento do risco;
- Por "aceitação do risco" entende-se a decisão de aceitar a persistência de um risco residual após o tratamento do risco;
- Por "risco residual" entende-se o risco que permanece após terem sido aplicadas medidas de segurança, dado que não é possível neutralizar todas as ameaças nem eliminar todas as vulnerabilidades;
- Por "comunicação do risco" entende-se a sensibilização, para os riscos, do grupo de utilizadores de um sistema de comunicação e informação, a informação das autoridades de aprovação quanto a esses riscos e a comunicação dos mesmos às autoridades operacionais.

4) Todos os dispositivos e equipamentos eletrónicos utilizados para manusear ICUE devem cumprir as regras aplicáveis em matéria de proteção de ICUE. Deve ser dada preferência a dispositivos e equipamentos eletrónicos já acreditados por outra instituição ou organismo da UE. Os dispositivos devem dar garantias de segurança ao longo de todo o seu ciclo de vida.

5) O sistema de comunicação e informação do Tribunal de Contas para efeitos de manuseamento de ICUE deve ser acreditado por uma autoridade pertinente. Para tal, o Tribunal de Contas deve celebrar um acordo de nível de serviço com uma autoridade de acreditação de segurança de uma instituição da UE que esteja em condições de acreditar um SCI no qual sejam manuseadas ICUE, com vista a obter uma declaração de acreditação para informações RESTREINT UE/EU RESTRICTED passíveis de serem manuseadas nesse SCI do Tribunal de Contas, bem como os correspondentes termos e condições de funcionamento. O acordo de nível de serviço também deve mencionar as normas a aplicar no processo de acreditação, devendo ser celebrado em conformidade com o procedimento previsto no artigo 10º, nº 3.

6) Caso o Tribunal de Contas necessite de definir um processo de acreditação próprio para o seu SCI, uma decisão delegada – nos termos do artigo 10º, nº 10, da presente decisão – deve definir o processo, em consonância com as normas relativas ao processo de acreditação para SCI que manuseiam ICUE no seio de outras instituições e organismos da UE.

7) A responsabilidade pela preparação dos processos e da documentação de acreditação, em conformidade com as normas aplicáveis, cabe inteiramente ao proprietário do SCI.

8) Caso as ICUE sejam protegidas por produtos criptográficos, o Tribunal de Contas deve dar preferência a produtos aprovados pelo Conselho ou pelo seu Secretário-Geral, na sua capacidade de autoridade de aprovação criptográfica, ou, alternativamente, a produtos aprovados por outras instituições e organismos da UE para efeitos de proteção de ICUE.

9) As informações classificadas como RESTREINT UE/EU RESTRICTED apenas devem ser manuseadas em dispositivos eletrónicos (tais como estações de trabalho, impressoras ou fotocopiadoras) situados numa Zona Administrativa ou numa Zona de Segurança. Os dispositivos eletrónicos nos quais se proceda ao manuseamento de informações classificadas como RESTREINT UE/EU RESTRICTED devem estar separados de outras redes informáticas e protegidos através de medidas físicas ou técnicas adequadas.

10) Todo o pessoal do Tribunal de Contas envolvido na conceção, desenvolvimento, ensaio, exploração, gestão ou utilização de SCI que manuseiem ICUE deve notificar o Responsável pela Segurança das Informações de todas as potenciais lacunas de segurança, incidentes, violações da segurança ou comprometimentos suscetíveis de ter impacto sobre a proteção do SCI e/ou das ICUE nele contidas.

<u>Artigo 7º</u> Procedimento aplicável ao intercâmbio de informações classificadas e à concessão de acesso às mesmas

1) Quando legalmente obrigadas a tal por força dos Tratados ou de atos jurídicos adotados com base nos Tratados, as instituições, órgãos e organismos da UE, bem como as autoridades nacionais, concedem ao Tribunal de Contas – por iniciativa própria ou na sequência de pedido por escrito do Presidente, de um ou mais Membros relatores ou do Secretário-Geral – acesso às ICUE de acordo com o procedimento a seguir descrito.

2) Os pedidos de acesso devem ser enviados às instituições em causa através do Serviço de Registos do Tribunal de Contas.

3) Se for caso disso, o Tribunal de Contas deve celebrar um acordo administrativo que abranja os aspetos práticos do intercâmbio de ICUE ou de informações equivalentes.

4) Para efeitos da celebração de tais acordos administrativos, o Tribunal de Contas deve fornecer à entidade de origem todas as informações necessárias acerca do seu sistema de segurança das informações. Se necessário, pode ser organizada uma visita de avaliação.

5) Esses acordos administrativos devem ser celebrados no pleno respeito dos princípios da atribuição de competências e da cooperação leal dispostos no artigo 13º do Tratado da União Europeia. Devem ser celebrados nos termos do artigo 10º, nº 4.

6) Caso não exista, em relação a uma instituição ou um organismo, um país terceiro ou uma organização internacional qualquer acordo administrativo relativo ao fornecimento de informações classificadas ao Tribunal de Contas, este assina uma declaração pela qual se compromete a proteger as informações classificadas por si recebidas.

Artigo 8º **Quebra de segurança, perda ou comprometimento de informações classificadas**

1) As quebras de segurança são atos ou omissões de uma pessoa que são contrários às regras de segurança estabelecidas na presente decisão e nas suas regras de execução.

2) O comprometimento ocorre quando, em consequência de uma quebra de segurança, são divulgadas, no todo ou em parte, ICUE a pessoas não autorizadas.

3) As quebras de segurança de que haja conhecimento ou suspeita devem ser imediatamente comunicadas à autoridade para a segurança das informações do Tribunal de Contas.

4) Nos casos em que se saiba, ou em que existam motivos razoáveis para pressupor, que foram comprometidas ou perdidas ICUE, a autoridade para a segurança das informações deve informar o Diretor dos Recursos Humanos, Finanças e Serviços Gerais, bem como o Secretário-Geral do Tribunal de Contas. O Diretor dos Recursos Humanos, Finanças e Serviços Gerais deve informar imediatamente a autoridade para a segurança da entidade de origem. O referido diretor do Tribunal de Contas deve levar a cabo um inquérito, informando o Secretário-Geral do Tribunal e a autoridade para a segurança da entidade de origem dos resultados do mesmo e das medidas empreendidas para evitar que a situação se repita. Caso a situação envolva um Membro do Tribunal de Contas, a tomada de medidas cabe ao Presidente do Tribunal de Contas, em colaboração com o Secretário-Geral.

5) Qualquer funcionário ou outro membro do pessoal do Tribunal de Contas que seja responsável por uma violação das regras de segurança estabelecidas na presente decisão e nas respetivas regras de execução fica sujeito às sanções constantes do Estatuto dos Funcionários da União Europeia e do Regime Aplicável aos Outros Agentes da União.

6) Qualquer membro do Tribunal de Contas que não cumpra os termos da presente decisão fica sujeito às medidas e sanções previstas no artigo 286º, nº 6, do TFUE.

7) O responsável pela perda ou pelo comprometimento de ICUE pode ser alvo de ação disciplinar e/ou judicial, em conformidade com as disposições legislativas e regulamentares aplicáveis.

Artigo 9º **Segurança em caso de intervenção externa**

1) O Tribunal de Contas pode confiar a contratantes registados num Estado-Membro o desempenho de tarefas que, por força do contrato celebrado com os mesmos, envolvam ou exijam acesso a ICUE. Esta situação pode suceder, em especial, no âmbito da manutenção dos sistemas de comunicação e informação e da rede informática.

2) Em caso de intervenção externa, o Tribunal de Contas deve adotar todas as medidas de segurança necessárias a que se refere o nº 3 do presente artigo, que incluem solicitar uma credenciação de segurança da empresa para garantir que as ICUE são protegidas pelos candidatos e proponentes ao longo do processo de concurso e de contratação, bem como pelos contratantes e subcontratantes durante a vigência do contrato. A autoridade

contratante garante que as normas mínimas de segurança previstas na presente decisão são mencionadas nos contratos, de modo a obrigar os contratantes a respeitá-las.

3) As regras de segurança, os procedimentos de contratação, os modelos para contratos e subcontratos que envolvam acesso a ICUE, os anúncios de contrato, as orientações sobre as circunstâncias que exigem credenciação de segurança da empresa, as instruções de segurança do programa ou projeto, as cláusulas adicionais de segurança, as visitas e a transmissão e transporte de ICUE ao abrigo desses contratos e subcontratos devem respeitar as regras e modelos estabelecidos pela Comissão Europeia para efeitos de contratos classificados na Decisão (UE, Euratom) 2015/444 da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE.

Artigo 10º **Aplicação da decisão e responsabilidades conexas**

1) Os serviços do Tribunal de Contas devem tomar, no âmbito da sua responsabilidade, todas as medidas necessárias para assegurar que, no manuseamento ou armazenamento de ICUE ou de quaisquer outras informações classificadas, aplicam a presente decisão e as regras de execução pertinentes.

2) O Secretário-Geral é a autoridade investida do poder de nomeação, bem como a autoridade habilitada a celebrar contratos de emprego no que se refere a todos os funcionários e demais membros do pessoal. O Secretário-Geral pode delegar no Diretor dos Recursos Humanos, Finanças e Serviços Gerais a responsabilidade de conceder aos funcionários e outros membros do pessoal a autorização de acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, de exercer a sua função de Autoridade de Acreditação de Segurança e de supervisionar o Secretariado do Tribunal no que se refere ao manuseamento de ICUE.

3) O Secretário-Geral deve estar habilitado a celebrar acordos de nível de serviço relacionados com a acreditação dos equipamentos e sistemas de comunicação e informação do Tribunal de Contas, com a utilização de uma Zona de Segurança de outra instituição da UE e com o procedimento de apresentação de pedidos de credenciação de segurança pessoal para efeitos de acesso a ICUE.

4) O Diretor dos Recursos Humanos, Finanças e Serviços Gerais terá competência para celebrar, com as instituições e organismos da UE, acordos administrativos relativos ao intercâmbio de ICUE de que o Tribunal de Contas necessite para cumprir o seu mandato. O Diretor também pode celebrar, com Estados terceiros ou organizações internacionais, acordos administrativos relativos à proteção das informações classificadas recebidas.

5) O Diretor dos Recursos Humanos, Finanças e Serviços Gerais terá competência para assinar quaisquer declarações de compromisso relativas à proteção de ICUE a fornecer no contexto de uma divulgação *ad hoc* excecional.

6) O Responsável pela Segurança das Informações do Tribunal de Contas atuará enquanto autoridade para a segurança das informações. O Responsável pela Segurança das Informações e as pessoas em quem delegue todas ou parte das suas tarefas devem possuir credenciação de segurança adequada. A autoridade para a segurança das informações deve assumir as suas responsabilidades em estreita cooperação com a Direção de Recursos Humanos, Finanças e Serviços Gerais, a Direção da Informação, Ambiente de Trabalho e Inovação e a Direção do Comité de Controlo da Qualidade da Auditoria (ver, em especial, os artigos 4º, 6º e 8º). A autoridade para a segurança das informações também é responsável pela formação e por reuniões de sensibilização para a segurança das informações, bem como por inspeções

periódicas para verificar a observância da presente decisão, incluindo em caso de intervenções externas, cabendo-lhe tomar medidas para assegurar tal observância.

7) O Responsável pela Segurança fica também encarregado das medidas de segurança física (em especial nos termos do artigo 5º).

8) Um Serviço de Registos estabelecido no seio do Secretariado do Tribunal agirá como ponto de entrada e saída de informações classificadas como RESTREINT UE/EU RESTRICTED passíveis de serem trocadas entre o Tribunal de Contas e outras instituições e organismos da UE, ou ainda com Estados-Membros. Servirá também de ponto de entrada e saída para informações equivalentes de Estados terceiros e organizações internacionais. O Serviço de Registos será estruturado conforme estabelecido numa decisão delegada. O Responsável pelo Serviço de Registos assume as seguintes responsabilidades principais:

   a) registo da entrada e saída de informações classificadas como RESTREINT UE/EU RESTRICTED;

   b) gestão de Zonas Administrativas específicas para o registo, manuseamento, armazenamento e consulta de ICUE com a classificação RESTREINT UE/EU RESTRICTED.

9) Deve ser criado um registo ao abrigo de um acordo de nível de serviço relativo à utilização da Zona de Segurança de outra instituição da UE. Este registo organizado pelo Secretariado do Tribunal, e da responsabilidade do Diretor de Recursos Humanos, Finanças e Serviços Gerais, servirá de ponto de entrada e saída para informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior passíveis de serem trocadas entre o Tribunal de Contas e outras instituições e organismos da UE, ou ainda com Estados-Membros. Servirá também de ponto de entrada e saída para informações equivalentes de Estados terceiros e organizações internacionais. Deve ser equipado com cofres adequados e outros equipamentos de segurança indicados para a proteção de informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior. O registo será estruturado conforme estabelecido numa decisão delegada. O Responsável do Controlo do Registo deve possuir credenciação de segurança adequada e assumir as seguintes responsabilidades principais:

   a) gestão das operações relativas ao registo, consulta, preservação, reprodução, tradução, transmissão, expedição e, se for caso disso, destruição de ICUE;

   b) quaisquer outras tarefas relacionadas com a proteção das ICUE definidas numa decisão delegada.

10) O Comité Administrativo deve adotar uma decisão delegada que estabeleça as regras de execução da presente decisão. O Responsável pela Segurança das Informações deve redigir orientações sobre a segurança das informações. O Comité de Controlo da Qualidade da Auditoria deve redigir orientações para auditorias.

<u>Artigo 11º</u> **Entrada em vigor**

A presente decisão entra em vigor no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito no Luxemburgo, em 3 de junho de 2021.

Pelo Tribunal de Contas

Klaus-Heiner Lehne
Presidente

Anexo: MEDIDAS DE SEGURANÇA FÍSICA RELACIONADAS COM ZONAS ADMINISTRATIVAS PARA ICUE

ANEXO

MEDIDAS DE SEGURANÇA FÍSICA RELACIONADAS COM ZONAS ADMINISTRATIVAS PARA ICUE

1) O presente anexo contém regras relativas à aplicação do artigo 5º da decisão. Tais regras representam as regras mínimas aplicáveis à proteção física de Zonas Administrativas situadas no Tribunal de Contas e dedicadas a informações classificadas como RESTREINT UE/EU RESTRICTED, ou seja, zonas designadas para o registo, armazenamento e consulta de informações com essa classificação.

2) As medidas de segurança física aplicadas nas Zonas Administrativas visam impedir o acesso não autorizado a tais zonas das seguintes formas:

   a) estabelecimento de um perímetro visivelmente definido que permita o controlo de pessoas;

   b) o acesso sem escolta só é concedido a pessoas devidamente autorizadas pela autoridade para a segurança das informações do Tribunal de Contas ou por outra autoridade competente;

   c) quaisquer outras pessoas devem ser permanentemente escoltadas ou sujeitas a controlos equivalentes.

3) A autoridade para a segurança das informações do Tribunal de Contas pode, a título excecional, conceder acesso a pessoas não autorizadas, incluindo para efeitos de trabalho numa Zona Administrativa, desde que este acesso não implique o acesso a ICUE, que devem permanecer trancadas. Tais pessoas apenas podem entrar na zona em questão se acompanhadas e vigiadas em permanência pela autoridade para a segurança das informações ou pelo Responsável do Controlo do Registo.

4) A autoridade para a segurança das informações deve estabelecer os procedimentos de gestão das chaves e/ou combinações de todas as Zonas Administrativas e mobiliário de segurança. Estes procedimentos visam evitar situações de acesso não autorizado.

5) As combinações devem ser memorizadas pelo menor número possível de pessoas que precisem de as conhecer. As combinações de mobiliário de segurança utilizado para armazenar informações classificadas como RESTREINT UE/EU RESTRICTED devem ser alteradas:

   - aquando da receção de um novo elemento de mobiliário de segurança;
   - sempre que mude o pessoal que conhece a combinação;
   - caso a combinação tenha ficado comprometida, ou se suspeite que possa ser este o caso;
   - caso uma fechadura tenha sido objeto de manutenção ou reparação;
   - pelo menos de 12 em 12 meses.

6) A autoridade para a segurança das informações e o Responsável pela Segurança ficam encarregados do cumprimento destas regras.