PROTEÇÃO DE DADOS

CSM
Conselho Superior da Magistratura

NEWSLETTER
JANEIRO 2026

4

Nesta edição

Editorial

O destaque da 4.ª edição desta newsletter vai para o Dia da Proteção de Dados, que se celebra anualmente por todo o mundo, no dia 28 de janeiro, e é uma ocasião especial para festejar o passado, pensar o presente e preparar o futuro. É notável o progresso das matérias de proteção de dados e da privacidade no século XXI, com a adoção de legislação nos cinco continentes e a criação de um número crescente de autoridades de controlo independentes. A generalização da utilização da Internet e a evolução galopante das tecnologias de informação e comunicação e dos sistemas de inteligência artificial trouxeram novos desafios e geraram novos riscos, que é preciso analisar, discutir e enfrentar sempre na perspetiva da defesa dos direitos fundamentais.

Por isso, também estão presentes nesta edição as iniciativas políticas mais recentes, a nível nacional e europeu, no domínio da inteligência artificial.

Também se faz um ponto da situação da publicação das decisões judiciais dos tribunais da primeira instância, no âmbito da base de dados de jurisprudência do CSM.

No que toca à jurisprudência do Tribunal de Justiça, analisa-se um acórdão muito recente de interpretação do artigo 13.º e do artigo 14.º do RGPD, a propósito de um caso sueco de prestação de informação aos passageiros que eram filmados por *bodycams* num transporte público.

Esta edição dá continuidade às duas novas rubricas estreadas no número anterior. 'Feito por Humanos' aborda as transferências internacionais de dados e o conceito de pseudonimização. No campo da cibersegurança, apresentam-se mais duas dicas muito úteis para apoiar os utilizadores a protegerem melhor os seus dados pessoais e a sua privacidade. E pode ficar a saber o que é uma 'botnet'.

Boa leitura!
Clara Guerra

CSM
Conselho Superior da Magistratura

Dia da Proteção de Dados 2026

Celebra-se no dia 28 de janeiro o Dia da Proteção de Dados. Instituído pelo Conselho da Europa, este dia foi comemorado pela primeira vez em 2007 pelos seus Estados-Membros, no continente europeu. No entanto, em poucos anos, tornou-se uma data celebrada em todo o mundo para assinalar a importância da defesa dos direitos à proteção de dados e à privacidade.

E em 2026, o Dia da Proteção de Dados festeja o seu 20.º aniversário!

O Serviço da Proteção de Dados do CSM associa-se naturalmente a esta celebração, ciente da necessidade e da relevância em contribuir, na sua atividade diária, para a garantia destes direitos fundamentais. A constante evolução tecnológica a que assistimos, tendo por base o tratamento de dados pessoais, agora especialmente no âmbito do desenvolvimento de sistemas de inteligência artificial, tem consequências diretas nos nossos direitos, individualmente enquanto cidadãos, mas também coletivamente enquanto sociedade.

O dia 28 de janeiro marca a data da assinatura do primeiro instrumento jurídico internacional sobre proteção de dados pessoais – a Convenção 108, do Conselho da Europa. Esta Convenção desempenhou um importante papel como propulsora da adoção de legislação nacional em matéria de proteção de dados em países fora do espaço europeu, por estar aberta à assinatura de Estados não-membros do Conselho da Europa, alargando as fronteiras do direito à proteção de dados. E teve a adesão de oito Estados dos continentes africano e americano.

Atualmente, quando passam 45 anos sobre a assinatura da Convenção 108, e a convenção já tem um texto modernizado em 2018, há legislação e autoridades de proteção de dados nos cinco continentes. Daí a partilha em todo o mundo do dia 28 de janeiro como o Dia da Proteção de Dados.

As celebrações são momentos únicos para lembrar o muito que se percorreu no passado e as conquistas alcançadas, e para refletir sobre os objetivos futuros e o caminho que se quer fazer para os atingir. Aproveite e reserve um tempo para isso. Bom Dia da Proteção de Dados 2026! ■

Saber+
Dia da Proteção de Dados (Conselho da Europa)

Convenção 108+ (modernizada)

CSM
Conselho Superior da Magistratura

Base de dados de jurisprudência do CSM

Decisões da 1.ª Instância já começaram a ser publicadas

Os tribunais de 1.ª instância começaram a publicar as suas decisões na base de dados de jurisprudência do CSM, que já disponibiliza ao público cerca de 700 decisões dos tribunais de comarca.

Após a atualização dos critérios de seleção das decisões judiciais a publicar online pelos tribunais de primeira instância e do refinamento dos critérios e das técnicas de pseudonimização a aplicar a toda a jurisprudência nacional, aprovados em junho de 2025 pelo Plenário do CSM, iniciou-se uma fase piloto da publicação das decisões selecionadas dos tribunais de comarca.

Por seu lado, a base de dados de jurisprudência do CSM, que é o coordenador nacional do identificador europeu de jurisprudência (ECLI), tem estado a ser reformulada e estima-se que a nova versão esteja em produção brevemente, com conteúdo alargado, novo visual e novas funcionalidades, constituindo-se a sua consulta como uma mais-valia indispensável para magistrados, advogados, académicos e juristas em geral.

As decisões judiciais de 1ª instância, provenientes de um universo de 27 tribunais, ocuparão a médio prazo uma parte relevante da jurisprudência disponível ao público na Internet.

Todas as decisões judiciais publicadas nesta base de dados são pseudonimizadas, de modo a tentar conciliar a necessidade da sua publicitação e inteligibilidade com os direitos fundamentais das pessoas cujos dados pessoais constam das decisões e que requerem a adoção de garantias e salvaguardas que o regime de proteção de dados lhes confere.

O Serviço de Proteção de Dados assegura apoio aos tribunais sobre a aplicação prática dos critérios de pseudonimização, bem como na utilização da ferramenta designada por "anonimizador", a qual já incorpora os critérios de pseudonimização aprovados, sem prejuízo do necessário e constante aperfeiçoamento e da inevitável avaliação casuística em relação à probabilidade de reidentificação dos titulares dos dados. ■

Saber+
Base de dados de jurisprudência

Critérios de seleção e publicação de decisões judiciais (2025)

CSM
Conselho Superior da Magistratura

Feito por humanos

O número
15

Total de países terceiros que gozam de uma decisão de adequação quanto ao seu nível de proteção de dados, não havendo obstáculos à transferência internacional de dados para esses destinos, pelo simples facto de estarem fora do Espaço Económico Europeu. As decisões de adequação são aprovadas pela Comissão Europeia, e podem abranger a totalidade do país terceiro, um território ou setores específicos de um país terceiro.
Atualmente, são considerados destinos adequados para a transferência internacional de dados pessoais: Andorra, Argentina, Canadá, EUA, Guernsey, Ilhas Faroé, Ilha de Man, Israel, Japão, Jersey, Nova Zelândia, Reino Unido, República da Coreia, Suíça, Uruguai.

A palavra
Pseudonimização

O tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.
[Artigo 4.º, ponto 5), do Regulamento Geral sobre a Proteção de Dados – RGPD]

Novidades da IA no plano político

A Comissão Europeia apresentou, em novembro último, uma Proposta de Regulamento para alterar o Regulamento da Inteligência Artificial (RIA), visando simplificar a concretização de normas harmonizadas sobre IA (Omnibus digital sobre IA).
Esta iniciativa legislativa pretende superar os atrasos verificados na aplicação do regulamento, quer na designação de autoridades nacionais competentes, quer na falta de *standards* harmonizados relativos aos requisitos, orientações e ferramentas de conformidade para os sistemas e IA de risco elevado.
No seguimento de várias consultas promovidas a nível europeu entre diferentes setores da sociedade, a Comissão considerou que há «desafios de execução» que podem prejudicar a entrada em aplicação de disposições-chave do RIA, pelo que propôs medidas de simplificação específicas, designadamente, estender a simplificação regulatória das PMEs às pequenas empresas de média capitalização; envolver a Comissão e os Estados-Membros na promoção da literacia sobre IA; reduzir as obrigações de registo.
Há outras alterações importantes, que não têm eventualmente um propósito tão simplificador, mas que se encontram agora em cima da mesa, como o reforço de poderes de supervisão da Comissão, quer diretamente, quer através do Serviço de IA (AI Office).
Pela sua relevância do ponto de vista do regime de proteção de dados, destaca-se a possibilidade, agora aberta, de tratar categorias especiais de dados para efeitos de detetar e corrigir enviesamentos em relação a todos os sistemas de IA e não apenas ao universo dos sistemas de risco elevado, como está atualmente previsto no RIA. Acresce que essa possibilidade, até aqui adstrita aos 'prestadores', é estendida também aos 'responsáveis pela implantação' dos sistemas, o que alarga substancialmente o universo de tratamentos de dados pessoais sensíveis no contexto da IA.
Outra das alterações mais relevantes prende-se com as modificações ao calendário de aplicação de certas disposições do RIA, relativas às obrigações no contexto dos sistemas de IA de elevado risco, que é objeto de adiamento e passa a ficar alinhado com a adoção de uma Decisão pela Comissão que confirme que as medidas de apoio à conformidade do Capítulo III do regulamento estão disponíveis. No caso de sistemas de risco elevado, previstos no Anexo III do RIA, como os da Justiça, os artigos 6.º a 27.º só passarão a ser aplicados seis meses após a adoção dessa Decisão ou, na sua ausência, a partir de 2 de dezembro de 2027.
Novidade mais recente da IA, foi a publicação este mês da Resolução de Conselho de Ministros n.º 2/2026, que aprova a Agenda Nacional da Inteligência Artificial e o seu Plano de Ação para o quinquénio 2026-2030. Nesse plano, a Iniciativa IV contém ações no âmbito do regime regulatório, em especial sobre a implementação do RIA (nomeadamente, definição das autoridades competentes, do modelo de coordenação e do quadro sancionatório) e a criação de um guia prático para apoiar as entidades no cumprimento do RIA.
As alterações propostas pela Comissão, a serem aprovadas, terão algum impacto no desenrolar das ações previstas no Plano de Ação da Agenda de IA. ■

Saber+
Omnibus Digital sobre IA

RCM n.º 2/2026, de 8 de janeiro

CSM
Conselho Superior da Magistratura

Glossário de A a Z

Bluetooth

é uma tecnologia sem fios que permite aos dispositivos comunicar e trocar dados a curtas distâncias sem necessidade de cabos ou fios. Encontra-se em vários dispositivos, como smartphones, tablets, computadores portáteis, auscultadores, altifalantes, smartwatches, rastreadores de fitness e em certos eletrodomésticos, como frigoríficos. Permite, suportando encriptação, transferir ficheiros entre dispositivos equipados com Bluetooth, como fotografias, vídeos ou outros documentos e ficheiros, embora a velocidade seja mais lenta em comparação com outros métodos como o WIFI. O alcance do Bluetooth mais comum é de cerca de 10 metros, mas pode atingir os 240m.
Quando não está a emparelhar dispositivos, deve manter desativada a função de Bluetooth do seu telemóvel; caso contrário, a emissão de sinais dos dispositivos, captada por 'beacons' Bluetooth instalados, por exemplo, em centros comerciais, permite estimar com grande rigor a sua localização e posicionamento, designadamente numa área específica do espaço interior, podendo assim ser inferidos os seus interesses ou preferências, associados aos identificadores do seu telemóvel, o que permite a individualização e facilita a identificabilidade.

[fonte: www.lenovo.com **e** www.cnpd.pt**]**

Jurisprudência

Noção de recolha direta de dados

O Tribunal de Justiça da União Europeia (TJUE) analisou num acórdão recente, de 18 de dezembro de 2025, um caso envolvendo a captação e gravação de imagem e som através de uma câmara corporal (bodycam) e concluiu que tal constitui uma recolha de dados junto do titular e, por conseguinte, é aplicável o artigo 13.º do RGPD, ou seja, a informação a prestar ao titular dos dados tem de ser fornecida aquando da recolha de dados e não posteriormente.
A questão foi suscitada, a título prejudicial, por um tribunal sueco, na sequência de um recurso da autoridade de proteção de dados que tinha aplicado uma coima a uma empresa de transporte público por incumprimento do dever de prestar informação aos passageiros que eram filmados pelos revisores dos bilhetes.
A empresa de transporte equipou os seus revisores com câmaras corporais, que filmavam e gravavam em contínuo os passageiros, sendo as imagens apagadas automaticamente ao fim de dois minutos (período reduzido para 1minuto, após intervenção da autoridade de proteção de dados), a menos que o revisor interrompesse a eliminação automática das imagens, bastando para o efeito carregar num botão. Isto aconteceria se um passageiro não possuísse bilhete válido sendo-lhe aplicada uma coima. Neste caso, a câmara conserva o minuto de imagem com som que antecede a suspensão do seu apagamento e as imagens que são captadas a seguir.
A utilização das câmaras tem como objetivo prevenir e documentar as ameaças e a violência exercida contra os revisores e verificar a identidade dos passageiros sujeitos a coima.
O tribunal de reenvio pretendia saber se, quando os dados pessoais são recolhidos através de uma câmara corporal, o dever de prestar informação aos titulares dos dados se realiza ao abrigo do artigo 13.º ou do artigo 14.º do RGPD. Por outras palavras, a questão prejudicial incidia sobre se a captação de imagem por uma câmara corporal se considerava uma recolha de dados junto do titular (artigo 13.º) ou se os dados não eram recolhidos junto do titular (artigo 14.º).
É a primeira vez que o TJUE se pronuncia sobre o âmbito de aplicação do artigo 13.º e do artigo 14.º do RGPD.
O TJUE, interpretando o conceito de "recolhidos junto do titular", constante da epígrafe do artigo 13.º do RGPD, entende que se aplica à recolha de dados através da câmara corporal, pois há um contacto direto com o titular, apesar de este não dar os seus dados pessoais de forma proativa, (como ocorreria se preenchesse um formulário). O Tribunal considerou que era irrelevante o grau de atividade do titular para delimitar o âmbito de aplicação do artigo 13.º em relação ao artigo 14.º, que se aplica apenas quando os dados não são recolhidos junto do titular, isto é, quando são recolhidos de outra fonte. Essa é a razão pela qual a obrigação de informar pode ser diferida para momento posterior e é necessário prestar informação ao titular sobre a «origem dos dados». ■

Saber+
Acórdão de 18 de dezembro de 2025
Caso SL, C-422/24, ECLI:EU:C:2025:980

CSM
Conselho Superior da Magistratura

Botnet

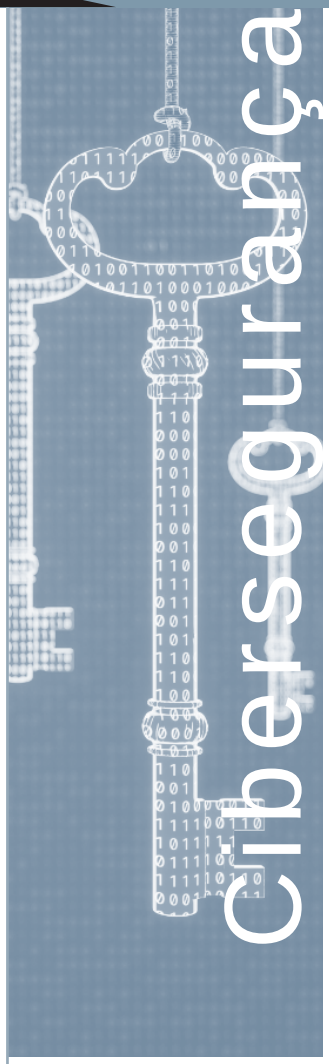
é um termo que se refere a um conjunto de computadores ligados entre si para realizar uma tarefa específica. Embora as botnets tenham sido criadas há umas décadas com o objetivo de executar tarefas úteis, como gerir salas de conversação na Internet ou contabilizar a pontuação durante um jogo online, a sua capacidade de executarem código dentro de outro computador tornou-as num instrumento poderoso para fins ilícitos. Atualmente uma botnet é muito perigosa e uma ameaça real, porque transformada numa rede de computadores infetados por software malicioso e controlados à distância por um único ciberatacante, sem o conhecimento dos utilizadores. Após ter o controlo de cada máquina individual (bot), o ciberatacante usa essa rede de computadores para vários fins ilícitos, tais como, enviar mensagens eletrónicas não solicitadas (spam), roubar informações pessoais, obter ganhos financeiros ou lançar ciberataques coordenados.

[fonte: www.fortinet.com**]**

Cibersegurança

consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.

[fonte: Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho]



Boas & Práticas

A segurança dos dados pessoais é uma componente muito importante do regime jurídico de proteção de dados. Os titulares dos dados são os beneficiários diretos da existência de medidas de segurança adequadas nas organizações. Mas, enquanto utilizadores das aplicações, os titulares têm também um papel ativo na robustez geral dos sistemas de segurança. As suas ações podem ter repercussões positivas ou negativas, consoante seja maior ou menor o grau da sua consciencialização, do seu conhecimento e do seu empenho nessa matéria. Assim, deixamos aqui algumas dicas para usar no dia-a-dia quando se navega na Internet ou se passa informação de um lado para outro.

#1

À deriva? Não, obrigado.

Pode escolher as condições em que navega na Internet. Aproveite os bons ventos da privacidade e navegue com mais segurança, utilizando o modo de navegação privada. A navegação privada (também designada "modo incógnito") permite aceder à Internet sem guardar o histórico de páginas visitadas, palavras-passe ou cookies após o encerramento da sessão.

Esta funcionalidade é especialmente útil na redução do risco de exposição de dados quando se utilizam computadores partilhados, equipamentos pessoais em contexto profissional ou redes públicas.

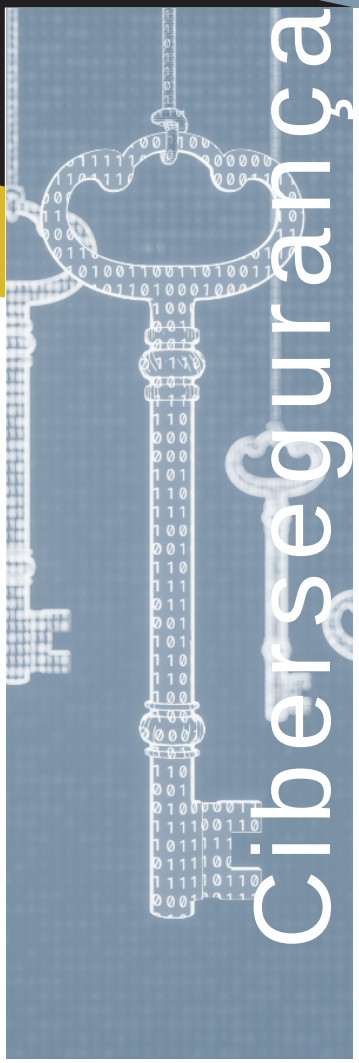
Sugestões:

- Utilize sempre o modo de navegação privada ao aceder ao e-mail institucional, plataformas judiciais ou áreas restritas quando está fora do posto de trabalho;
- Feche sempre todas as janelas do navegador para garantir que termina a sessão, pois só assim elimina o histórico dessa navegação. Não reutilize a mesma sessão privada.
- Mesmo em modo privado, esteja atento aos sítios visitados e evite iniciar sessão em plataformas inseguras (sem HTTPS).

Como ativar o modo de navegação privada:
Em Windows / macOS:

- **Google Chrome:** pressione Ctrl + Shift + N (Windows) ou ! ⌘ + Shift + N (Mac).
- **Microsoft Edge:** pressione Ctrl + Shift + N.
- **Mozilla Firefox:** pressione Ctrl + Shift + P (Windows) ou ⌘ + Shift + P (Mac).
- **Safari (Mac):** menu Ficheiro → Nova janela privada (⌘ + Shift + N).

CSM
Conselho Superior da Magistratura



Em Android / iPhone:

- **Google Chrome:** toque nos três pontos → Novo separador anónimo.
- **Mozilla Firefox:** toque no ícone que mostra as abas abertas (geralmente junto à barra de endereço), na visão de abas, toque no ícone de máscara para mudar para o modo de abas privadas, depois toque em "+ Privado" ou "+" para abrir uma nova aba privada.
- **Microsoft Edge:** toque nas três riscas → Novo separador InPrivate.

Ao encerrar todas as janelas privadas, o navegador elimina automaticamente o histórico e os cookies dessa sessão, mantendo a sua navegação mais privada e segura.

#2

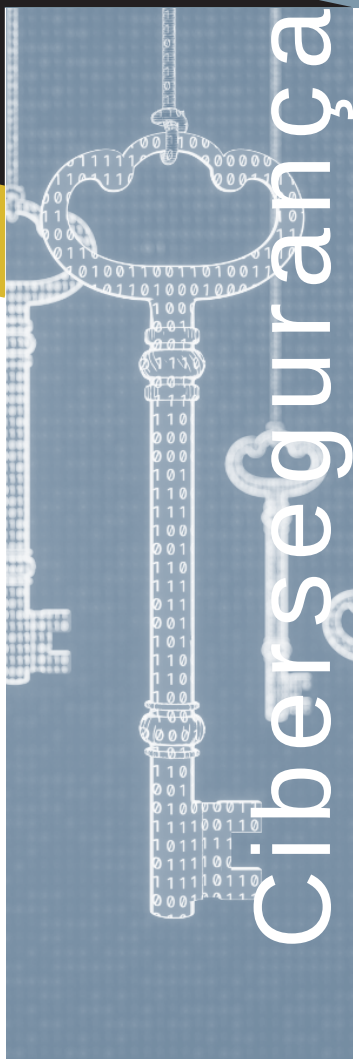
Perdidos e Achados (por outros)

Já todos perdemos uma 'pen' pelo menos uma vez na vida. Ou então nunca a conseguimos voltar a encontrar. Seja como for, os dispositivos amovíveis de armazenamento são auxiliares preciosos, na vida profissional ou na vida pessoal, para transportar ficheiros, passar informação de um lado para outro, guardar cópias de segurança de documentos, armazenar dados em grandes quantidades.
Estes dispositivos, sejam *pen drives,* discos externos ou outros, porque se deslocam connosco, correm o risco de se perderem, extraviarem ou serem furtados. Além do grande incómodo que tal pode acarretar se não tivermos a informação duplicada, a gravidade da situação reside na potencial exposição de dados, sensíveis, nossos ou de outras pessoas, a terceiros não autorizados.
A encriptação destes dispositivos garante, na maioria das vezes, que, em caso de perda ou furto, os dados pessoais permanecem inacessíveis sem a respetiva chave ou palavra-passe. É uma solução fácil de executar e extremamente útil para quem lida com informação sigilosa.

Sugestões:

- Utilize sempre encriptação em dispositivos que contenham dados pessoais;
- Evite armazenar informação sensível em suportes não cifrados, mesmo que temporariamente;
- Guarde cópias de segurança dos dados antes de iniciar a encriptação e, após confirmar o acesso ao volume cifrado, elimine as cópias não encriptadas;
- Use palavras-passe longas, únicas e complexas (ver dica na Newsletter #3);
- Sempre que possível, utilize o 'smart card' profissional* para desbloquear unidades cifradas, oferece maior segurança e dispensa a gestão de palavras-passe.
- Não partilhe a chave de recuperação em canais inseguros (ex.: e-mail);
- Armazene a chave de recuperação num local seguro e separado do dispositivo cifrado (ex.: cofre de senhas).

CSM
Conselho Superior da Magistratura



O que pode fazer:

- Utilize a ferramenta BitLocker To Go, integrada no Windows, para cifrar discos amovíveis (USB, HDD externos, cartões SD, etc.);
- O BitLocker utiliza algoritmos de encriptação robustos, que garantem a proteção total do conteúdo.

Como fazer:

- Ligue o dispositivo amovível ao computador;
- No Explorador de Ficheiros em Este PC, clique com o botão direito do rato sobre a unidade (amovível) e selecione "Ativar BitLocker";
- Escolha o método de desbloqueio:
  - "Utilizar uma palavra-passe para desbloquear a unidade" e introduza uma palavra-passe forte;
  - "Utilizar o meu smart card para desbloquear a unidade", e introduza o smart card e respetivo PIN (recomendado para magistrados e oficiais de justiça que possuam cartão profissional com certificado digital).
- Guarde a chave de recuperação num local seguro;
- Selecione a opção "Encriptar apenas o espaço em disco utilizado" para maior rapidez, ou "Encriptar a unidade completa" para proteção total;
- Escolha o modo de encriptação compatível com outros dispositivos, caso pretenda utilizar o disco em diferentes versões do Windows;
- Confirme e inicie a encriptação. O processo pode demorar alguns minutos, consoante a capacidade da unidade.

Estas medidas asseguram que a informação armazenada em dispositivos amovíveis permanece protegida, mesmo que o suporte físico seja perdido ou acedido indevidamente. ■

*** Recomendação sobre o uso de *smart card* para encriptar**

O uso do *smart card* para desbloquear unidades BitLocker garante autenticação multifator (cartão físico + PIN).
As chaves privadas permanecem armazenadas de forma segura no chip, impossibilitando cópia ou extração.
Esta opção é recomendada em ambientes de trabalho judicial por oferecer maior proteção e conformidade com as políticas institucionais de segurança.

FICHA TÉCNICA
Newsletter #4
Janeiro 2026

EDIÇÃO
Serviço de Proteção de Dados do CSM

DESIGN E PAGINAÇÃO
Luísa Castelo dos Reis
Sardine & Carbone, Lda

DISTRIBUIÇÃO
no website do CSM
por email e através do Iudex

CONTACTOS
epd@csm.org.pt
www: csm.org.pt
T. +351 213 220 020