PROTEÇÃO DE DADOS

CSM
Conselho Superior da Magistratura

NEWSLETTER
MAIO 2025

3

Nesta edição

Editorial

A 3.ª edição desta newsletter traz uma imagem renovada e conteúdos alargados em matéria de proteção de dados pessoais, incluindo as novidades do trabalho do CSM. Assinala-se o 7.º aniversário da aplicação do RGPD e apresenta-se a nova Encarregada da Proteção de Dados.

Os direitos dos titulares dos dados surgem nesta edição em grande destaque: por um lado, o direito a ser esquecido através da fixação pelo CSM de prazos de conservação para o apagamento de dados judiciais online; por outro, pela mão da jurisprudência europeia recente, o direito de retificar os dados relativos à identidade de género e o direito de acesso como instrumental do direito a não ficar sujeito a uma decisão individual automatizada.

Neste contexto, mostra-se a estreita ligação entre a proteção de dados e o desenvolvimento e utilização de sistemas de IA, em especial quanto às obrigações de transparência que impendem sobre os prestadores e implementadores daqueles sistemas, enquanto responsáveis pelo tratamento de dados, e o exercício dos direitos dos titulares.

Também se dá conta das últimas notícias sobre a publicação das decisões judiciais na base de dados do CSM e sobre o seu alargamento aos Tribunais de Primeira Instância.

'Feito por humanos' é o nome de uma rubrica que agora se inicia e que vai dar a conhecer algumas curiosidades, históricas ou atuais, em torno de um Número e de uma Palavra, relacionados com a proteção de dados pessoais.

Por fim, aborda-se a cibersegurança na ótica do utilizador, com alguns lamirés práticos e um glossário de termos técnicos trocados por miúdos. A continuar em futuras edições.

Boa leitura!
Clara Guerra

CSM
Conselho Superior da Magistratura

Nova Encarregada da Proteção de Dados

O CSM tem uma nova Encarregada da Proteção de Dados (EPD/DPO), Clara Guerra, que veio substituir a juíza de direito Sofia Wengorovius, que desempenhou as funções de EPD do Conselho ao longo de seis anos e entendeu ser agora o momento de regressar ao seu trabalho no tribunal.
Clara Guerra foi Consultora coordenadora da Comissão Nacional de Proteção de Dados, onde trabalhou cerca de 28 anos e adquiriu vasta experiência no domínio da proteção de dados pessoais, incluindo no contexto da atividade inspetiva nacional e europeia. Foi também representante da CNPD em diferentes fóruns europeus e internacionais, tendo exercido a presidência de alguns deles por eleição dos seus pares.
Durante vários anos, foi docente de Proteção de Dados Pessoais, como assistente convidada, na Escola de Lisboa da Faculdade de Direito da Universidade Católica Portuguesa, bem como em cursos de pós-graduação e de formação de executivos na UCP e na Universidade Autónoma de Lisboa.
Por ocasião da cessação de funções de Sofia Wengorovius, o CSM aprovou por unanimidade, na sua sessão plenária de 6 de maio, um louvor à anterior EPD como reconhecimento público pela «forma como superiormente exerceu as exigentes funções de EPD» e pelo «relevante contributo [que deu] no incremento das políticas de proteção de dados neste Conselho, tendo estado na génese do respetivo Gabinete». ■

RGPD - 7 anos de aplicação

Assinalou-se, a 25 de maio, o aniversário da aplicação do Regulamento (UE) 2016/679 - Regulamento Geral sobre a Proteção de Dados (RGPD), instrumento que veio dar uma visibilidade sem precedentes ao direito fundamental à proteção de dados pessoais.
São 7 anos de um novo regime jurídico, uniformizado e diretamente aplicável em todos os Estados-Membros do Espaço Económico Europeu (EEE), que inclui os países da UE e a Islândia, o Liechtenstein e a Noruega. O RGPD substituiu as anteriores legislações nacionais que transpunham a Diretiva de Proteção de Dados, de 1995.
O RGPD aplica-se, com algumas exceções, ao setor privado e ao setor público, incluindo aos tribunais.
Embora assente na matriz fundadora e nos princípios basilares da proteção de dados, forjados no Conselho da Europa e na OCDE a partir dos anos 70 do século XX, o RGPD traz novos conceitos, alarga o leque de direitos, amplia as obrigações de transparência, reforça as obrigações de subcontratação, codifica boas práticas, incorpora instrumentos típicos de autorregulação, altera o modelo de supervisão para um controlo ex post e introduz um regime sancionatório dissuasor.
Além disso, o RGPD veio satisfazer as aspirações de longa data das empresas multinacionais com a criação do sistema de balcão único no EEE, que levou à criação de um mecanismo de cooperação e coerência entre as autoridades nacionais de proteção de dados, sob a batuta do Comité Europeu para a Proteção de Dados, um novo órgão da UE, independente e dotado de personalidade jurídica.
Outra grande novidade que tornou o RGPD numa legislação de referência internacional é o alargamento do seu âmbito de aplicação territorial a tratamentos de dados realizados fora da União e a empresas sem estabelecimento na UE, desde que ofereçam bens e serviços a titulares na UE ou controlem o seu comportamento.
Procurando ser tecnologicamente neutro, para poder sobreviver ao dinamismo da inovação e à voragem dos desenvolvimentos técnicos, o RGPD adota uma abordagem baseada no risco, exigindo sempre uma análise casuística.
Nestes 7 anos, desde 2018, que o CSM tem trabalhado na adequada implementação do RGPD, tem promovido a formação dos magistrados judiciais neste domínio e tem tido a preocupação em integrar a proteção de dados no desenvolvimento dos seus novos projetos. A criação do Serviço de Proteção de Dados demonstra bem o nível de investimento do CSM na conformidade com o RGPD. ■

CSM
Conselho Superior da Magistratura

Direito ao apagamento no Portal CITIUS

Em 10.12.2024, o CSM aprovou as conclusões do grupo de trabalho relativas à fixação de prazos de conservação das publicações online de dados dos processos judiciais, designadamente no Portal CITIUS, para assegurar a conformidade com os princípios previstos no RGPD.

Na ausência de norma legal que determine um prazo máximo de conservação dos dados pessoais, é necessário equilibrar a publicidade do processo com os direitos dos cidadãos, observando o princípio da limitação da conservação, reconhecido no artigo 5.º do RGPD e especificamente regulado no artigo 40.º da Lei n.º 34/2009, de 14 de julho, cuja aplicação garante que os dados sejam conservados apenas durante o período necessário para as finalidades para as quais foram tratados.

No âmbito dos processos de insolvência por exemplo, atendendo a que a lei reconhece o direito ao *fresh start*, através da possibilidade de retoma da vida económica e financeira sem estigma ou discriminação, a perpetuação na Internet dos dados das pessoas singulares outrora insolventes não estava a permitir garantir eficazmente esse direito.

No mesmo sentido se manifestou a Provedora de Justiça, numa Recomendação, na sequência de queixas de insolventes, ao pugnar pela necessidade de proceder à remoção de certos atos judiciais do Portal CITIUS, quando os processos se considerem findos para efeitos de arquivo, e aproveitados os dados para efeitos estatísticos.

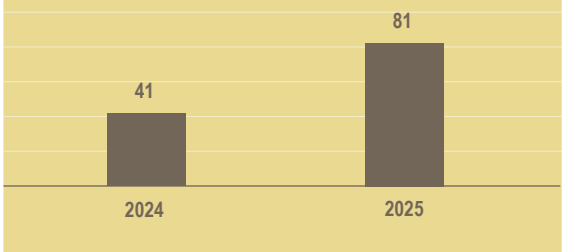
Desde a aprovação desta política de prazos de conservação que aumentou significativamente o número de titulares dos dados a exercer o seu direito ao apagamento (direito a ser esquecido), previsto no artigo 17.º do RGPD.

O CSM já recebeu, até 20 de maio, um total de 122 pedidos de apagamento de dados pessoais do Portal CITIUS no âmbito de processos de insolvência. ■

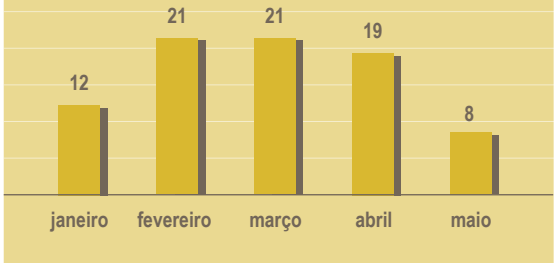
Saber+
Política de prazos de conservação da publicação dos dados dos atos judiciais

Recomendação n.º 3/A/2024 da Provedora de Justiça

Nº Total de Pedidos de apagamento de dados do Portal CITIUS



Nº de Pedidos de apagamento de dados em 2025



CSM
Conselho Superior da Magistratura

Pseudonimização e publicação das decisões judiciais

O CSM constituiu este ano um grupo de trabalho para a elaboração de critérios uniformes de seleção das decisões judiciais a publicar *online* pelos Tribunais de Primeira Instância e pretende, nesse contexto, ajustar as técnicas de pseudonimização a aplicar a toda a jurisprudência nacional.

Constituído por presidentes de nove comarcas, por dois assessores do GAVPM e pelo Serviço da Proteção de Dados do CSM, esse grupo de trabalho apresentou as suas conclusões em abril.

Com o propósito assumido pelo CSM de iniciar a publicação *online*, de forma sistemática e crescente, das decisões judiciais da Primeira Instância, tornou-se necessário adaptar os critérios anteriormente aprovados, desde logo os critérios de seleção das decisões, na impossibilidade, por ora, de se adotar um critério de seleção negativa, à semelhança do que acontece nos tribunais superiores.

Além disso, foi também elaborada uma proposta de refinamento dos critérios de tratamento, apresentação e publicação da decisão, especificando-se as técnicas de pseudonimização a aplicar, de modo a conciliar a publicidade e a legibilidade da jurisprudência com os direitos das pessoas singulares, cujos dados pessoais constam das decisões e que gozam da proteção conferida pelo RGPD.

As regras de pseudonimização propostas seguem de perto as recentes orientações da CEPEJ (Comissão Europeia para a Eficiência da Justiça) do Conselho da Europa, de dezembro de 2024. Acresce que, sendo o CSM o coordenador nacional do Identificador Europeu de Jurisprudência (ECLI – *European Case Law Identifier*), a seleção dos dados pessoais a ofuscar tem de observar certas regras na composição do identificador da decisão.

Atualmente, a proposta final de atualização dos critérios de seleção e publicação das decisões e respetivas técnicas de pseudonimização está em fase de discussão, com previsão de aprovação pelo CSM para breve.

A partir de setembro prevê-se o arranque, numa fase piloto, da publicação de decisões selecionadas de Primeira Instância. Em janeiro de 2026, prevê-se a publicação plena das decisões de todas as Comarcas na base de dados de jurisprudência do CSM reformulada.

Numa fase inicial, o Serviço da Proteção de Dados do CSM ficará a assegurar um serviço de apoio (*helpdesk*) aos tribunais, com o objetivo de auxiliar na aplicação prática dos critérios de pseudonimização e na utilização da ferramenta designada por "anonimizador". ■

Glossário de A a Z

Adware

é um software (frequentemente malicioso) que se instala automaticamente sem conhecimento do utilizador, à boleia de programas gratuitos que são descarregados da Internet, e exibe anúncios não solicitados no computador ou no dispositivo móvel, com base na sua atividade online, nomeadamente através do acesso ao histórico do navegador e à localização. O acesso a estas informações pode ser vendido a terceiros, além do rendimento obtido pelos criadores de adware cada vez que instalam o software, exibem anúncios ou o utilizador clica num anúncio.

[fonte: www.kasperski.com.br]

Ataque

tentativa para destruir, expor, alterar, incapacitar, obter acesso não autorizado a um ativo ou fazer uso não autorizado.

[fonte: www.enisa.europa.eu]

Autenticação

é um processo de verificação de identidade. É usado para verificar a identidade de utilizadores, de dispositivos e de outras entidades num sistema informático.

[fonte: www.coursera.org]

CSM
Conselho Superior da Magistratura

A proteção de dados e a IA

A inteligência artificial (IA) veio para ficar. O universo de ficção científica que retemos na memória dos livros e do cinema deu lugar a uma realidade atual, simultaneamente promissora e perigosa, e com indubitável influência crescente nas nossas vidas. Não se trata de magia, mas de matemática. E agora também de direito, através da regulação europeia sobre IA (RIA), em vigor desde o ano passado e com aplicação faseada entre 2025 e 2027.

Mas falar de IA é falar também de proteção de dados, porque a IA se alimenta de dados e sempre que a conceção, desenvolvimento ou utilização de sistemas de IA envolverem o tratamento de dados pessoais, também se aplica o RGPD ou os regimes especiais de proteção de dados. Isso mesmo é afirmado no Considerando 10 do RIA, quanto às obrigações dos prestadores ou dos responsáveis pela implantação de sistemas de IA enquanto responsáveis pelo tratamento de dados.

Também é clarificado no RIA que os titulares dos dados continuam a usufruir de todos os direitos e garantias que lhes são conferidos pelo direito da União, incluindo os direitos relacionados com as decisões exclusivamente automatizadas, devendo os sistemas de IA permitir o exercício dos direitos dos titulares e facilitar a sua aplicação efetiva.

É neste contexto que o recente acórdão do Tribunal de Justiça, que se pronunciou a título prejudicial, no caso austríaco D&B, ganha uma importância acrescida. Chamado a pronunciar-se sobre a interpretação de normas do RGPD relativas ao exercício do direito de acesso (alínea h) do n.º 1 do artigo 15.º) e ao direito a não ficar sujeito a uma decisão individual automatizada (artigo 22.º), o Tribunal entende que o titular dos dados tem o direito à explicação sobre o funcionamento do mecanismo subjacente à decisão automatizada de que essa pessoa foi objeto e sobre o resultado a que essa decisão conduziu.

De acordo com o Tribunal, o titular dos dados pode exigir que, a título de informações úteis relativas à lógica subjacente à decisão, lhe seja explicado através de informações pertinentes e de forma concisa, transparente, inteligível e de fácil acesso, o procedimento e os princípios concretamente aplicados para explorar, por via automatizada, os dados pessoais relativos a essa pessoa para obter um determinado resultado.

Tal não significa que lhe seja dada uma *explicação complexa sobre os algoritmos utilizados ou a divulgação dos algoritmos na íntegra.* No entanto, o Tribunal afirma que a complexidade das operações a realizar no âmbito de uma decisão automatizada não pode exonerar o responsável pelo tratamento do seu dever de explicação (cf. pontos 60 e 61 do acórdão).

O TJUE reitera, aliás, remetendo para jurisprudência anterior, que o titular dos dados tem o direito de verificar a exatidão dos dados que lhe dizem respeito, e de que estes são tratados de forma lícita.

O TJUE conclui que estas obrigações de transparência que impendem sobre os responsáveis pelo tratamento de dados são essenciais para a garantia de outros direitos, em particular do direito de o titular, perante uma decisão que se baseia exclusivamente num tratamento automatizado e que o afete significativamente, manifestar o seu ponto de vista e contestar a decisão.

Sobre a invocação do segredo comercial para não prestar informações aos titulares dos dados, o TJUE declara que o responsável pelo tratamento é obrigado a comunicar essas informações alegadamente protegidas à autoridade de controlo de proteção de dados ou ao órgão jurisdicional competente, aos quais incumbe fazer a ponderação entre os direitos e os interesses em causa para determinar o alcance do direito de acesso.

Daqui decorre claramente que, no desenvolvimento e utilização de sistemas de IA, dos quais venham a resultar decisões individuais automatizadas, incluindo a definição de perfis, é essencial ter em conta a obrigação de fornecer as informações necessárias, em linguagem acessível, quanto à lógica subjacente a esse tratamento de dados, de modo a facilitar e a permitir o efetivo exercício dos direitos pelos respetivos titulares dos dados.

A proteção de dados pessoais está intrinsecamente ligada ao desenvolvimento da IA, adotando ambos os regulamentos uma abordagem baseada no risco, além de partilharem conceitos, ferramentas e salvaguardas. O quadro legal da IA remete para uma interação constante com o regime jurídico de proteção de dados, pelo que dificilmente poderemos dissociar um do outro. ■

Saber+

Acórdão de 27 de fevereiro de 2025
D&B, C-203/22, ECLI:EU:C:2025:117

Regulamento (UE) 2024/1689
Regulamento da Inteligência Artificial (RIA)

CSM
Conselho Superior da Magistratura

Feito por humanos

O número
1981

Ano em que foi aberto à assinatura o primeiro instrumento jurídico internacional de proteção de dados. No dia 25 de janeiro, dez Estados-Membros do Conselho da Europa, incluindo Portugal, assinaram a Convenção 108, relativa à proteção das pessoas singulares em relação ao tratamento automatizado dos seus dados pessoais. A Convenção foi também aberta à adesão de Estados não-Membros. Em Portugal, a Convenção 108 foi ratificada em 1993 e entrou em vigor em 1 de janeiro de 1994. O texto do tratado foi modernizado em 2018, dando lugar à Convenção 108+, que conta atualmente com 55 Estados Parte.

A Palavra
Algoritmo

Processo de resolução de um problema constituído por uma sequência ordenada e bem definida de passos que, em tempo finito, conduzem à solução do problema ou indicam que, para o mesmo, não existe soluções.

Do latim medieval algorithmus, de algorismus com adaptação ao grego ἀριθμός 'número'.

"algoritmo", in Dicionário da Língua Portuguesa. Academia das Ciências de Lisboa. Disponível em https://dicionario.acad-ciencias.pt/pesquisa/algoritmo

[consultado em 12/05/2025]

Jurisprudência

Retificação da identidade de género em registo público

Em 13 de março de 2025, o Tribunal de Justiça da UE proferiu um acórdão, declarando que o artigo 16.º do RGPD, que prevê o direito de o titular dos dados obter do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito, deve ser interpretado no sentido de que impõe a uma autoridade nacional incumbida da manutenção de um registo público que retifique os dados pessoais relativos à identidade de género de uma pessoa singular quando esses dados não cumpram o princípio da exatidão, reconhecido no artigo 5.º, n.º 1, alínea d), do RGPD.

Este caso surge na sequência da queixa de um titular dos dados que havia solicitado, junto de um registo público, ao abrigo do artigo 16.º do RGPD, a retificação do seu género de 'feminino' para 'masculino' e a alteração do seu nome próprio, tendo juntado para o efeito os atestados médicos de especialistas, pretensão essa que lhe foi negada por não ter provado a realização de cirurgia de mudança de sexo.

O TJUE remete para jurisprudência constante do Tribunal Europeu dos Direitos Humanos, que protege, ao abrigo do artigo 8.º da CEDH (equivalente ao artigo 7.º da Carta), a identidade de género de uma pessoa, como um elemento constitutivo e um dos aspetos mais íntimos da sua vida privada. Esta disposição engloba o direito de cada pessoa estabelecer os pormenores da sua identidade de ser humano, o que inclui o direito das pessoas transgénero ao desenvolvimento pessoal e à integridade física e moral, bem como ao respeito e ao reconhecimento da sua identidade de género, sendo que esse reconhecimento não pode estar subordinado à realização de uma cirurgia não desejada pela pessoa.

Embora o TJUE admita restrições ao direito de retificação, ao abrigo do artigo 23.º do RGPD, estas só poderão ocorrer através de medida legislativa e nas condições legalmente exigidas, e não por mera prática administrativa. De qualquer modo, o Tribunal de Justiça entende que aquela prática não é necessária ou proporcional, podendo o atestado médico constituir-se como um elemento de prova bastante.

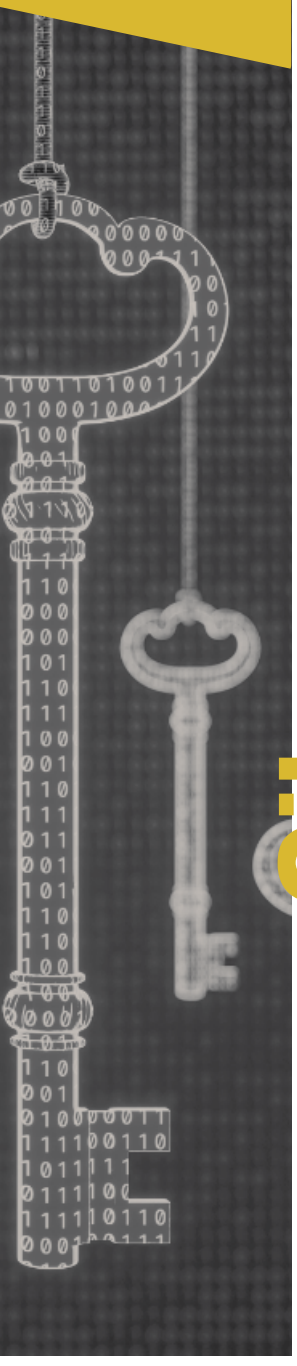
O acórdão conclui que, para efeitos do exercício do direito de retificação de dados relativos à identidade de género constantes de um registo público, podem ser exigidos elementos de prova pertinentes, mas nunca pode a garantia do direito ficar dependente, por meio de prática administrativa, da apresentação de prova de cirurgia de mudança de sexo. ■

Saber+

Acórdão de 13 de março de 2025
Caso Deldits, C-247/23, ECLI:EU:C:2025:172

CSM
Conselho Superior da Magistratura

Cibersegurança



Boas & Práticas

O regime jurídico de proteção de dados contém normas específicas relativas à segurança dos tratamentos de dados pessoais. Impõe às organizações a adoção de medidas técnicas e organizativas adequadas, em função do risco que cada tratamento de dados pode representar para os direitos e liberdades dos titulares.
Daí que a cibersegurança seja uma componente essencial da proteção de dados, já que o nosso quotidiano se organiza sobretudo no ciberespaço, seja na vida privada ou na vida profissional, seja como meros titulares de dados ou como utilizadores de aplicações e sistemas de informação.
Contribuir para garantir a segurança da informação é, assim, uma missão de todos. E como o saber não ocupa lugar, aqui ficam alguns lamirés sobre cibersegurança, de cariz prático, para reforçar a sua cultura de proteção de dados e melhor defender a sua privacidade.

A sua palavra-passe ainda é “123456”?

Pode parecer exagero, mas continua a ser uma das palavras-passe mais utilizadas no mundo. O mesmo se pode dizer de datas de aniversário ou mesmo da palavra ‘password’. Só que as palavras-passe dão acesso a informação pessoal, por vezes, de grande sensibilidade, pelo que uma palavra-passe tão óbvia ou simples representa um risco significativo de terceiros conseguirem aceder a esses dados. Por isso, o simples gesto de escolher uma palavra-passe pode transformar-se numa fragilidade crítica.

Porquê?

- Palavras-passe fracas ou repetidas são facilmente quebradas por ataques automatizados.
- Usar a mesma palavra-passe em vários serviços significa que uma única violação de dados pode comprometer tudo.

Sugestões

- Use palavras-passe longas e imprevisíveis (mínimo 12 caracteres).
- Crie frases memoráveis (ex.: Tr0c0@Minha5enha!TodosOsMeses).
- Nunca reutilize palavras-passe entre serviços diferentes.
- Altere imediatamente a sua palavra-passe se suspeitar que ela foi exposta.
- Evite guardar palavras-passe no navegador de Internet (browser), porque são frequentemente alvo de ataques. Quando lhe surge aquela janela a perguntar se quer guardar a palavra-passe (password), assinale a opção ‘não’ ou ‘nunca guardar’.
- Não confie em serviços “gratuitos” na nuvem para guardar senhas; nesses casos, o produto pode ser o utilizador e os seus dados.
- Altere as palavras-passe predefinidas de fábrica nos dispositivos que adquire (ex.: routers Wi-Fi, câmaras IP, NAS, impressoras). Estas credenciais são públicas e frequentemente exploradas em ataques automáticos.

Foi você que pediu um ficheiro cifrado?

Ainda bem, porque cifrar ficheiros é simples e fundamental para proteger a sua informação. Um ficheiro cifrado torna muito mais difícil, ou mesmo impossível, que terceiros leiam o seu conteúdo. Se os ficheiros contêm informação particularmente sensível, seja de natureza profissional ou pessoal, há motivos acrescidos para os cifrar. Isto aplica-se tanto ao envio de ficheiros por e-mail ou mensagens, como ao transporte em dispositivos de armazenamento, nomeadamente pens USB ou discos externos.

Porquê?

- Se perder uma pen USB sem ficheiros cifra-

CSM
Conselho Superior da Magistratura

Cibersegurança

dos, qualquer pessoa pode facilmente aceder e fazer qualquer tipo de uso da informação ali contida, incluindo publicamente, sem que possa ter qualquer controlo sobre a situação.

- Se enviar ficheiros não cifrados por e-mail, corre o risco de este ser reencaminhado, ou intercetado e acedido em caso de violação da conta de correio eletrónico.
- Mesmo que utilize plataformas de mensagens cifradas, os ficheiros perdem a proteção assim que chegam ao destinatário.
- Há múltiplas pessoas e entidades, públicas e privadas, nacionais e estrangeiras, envolvidas na cadeia de transmissão de um e-mail ou mensagem, pelo que há um risco significativo de os seus ficheiros poderem ser lidos se não forem cifrados.

Sugestões:

- Cifre sempre os ficheiros com conteúdo sensível, sigiloso ou confidencial.
- Guarde cópias de segurança dos ficheiros antes de os cifrar.
- Evite enviar documentos sensíveis como anexos desprotegidos, cifre os ficheiros ou utilize plataformas seguras da instituição.
- Utilize ferramentas de compressão com cifragem integrada, que permitam proteger ficheiros ou pastas com palavras-passe seguras e algoritmos reconhecidos.
- Verifique sempre o endereço de e-mail do destinatário antes de enviar informação sensível.
- Não inclua dados confidenciais no assunto do e-mail nem no corpo da mensagem, mantenha essa informação apenas nos anexos cifrados.

O que pode fazer:

- Comprima e cifre os seus ficheiros:
  - Utilize ferramentas gratuitas, de software livre, tais como, entre outras, 7-Zip, PeaZip ou Keka. Provavelmente, um destes programas já está instalado no seu computador.
  - Ative a opção "Encriptar nomes de ficheiros" para proteger também a lista de conteúdos.
  - Defina uma palavra-passe longa, única e complexa (veja o lamiré anterior).
  - Se o ficheiro for apenas para transporte pessoal, guarde a palavra-passe num local seguro, exclusivamente do seu conhecimento, e separado do dispositivo de armazenamento.
  - Envie a palavra-passe por um canal diferente:
  - Se enviar o ficheiro por e-mail, envie a palavra-passe por SMS ou por outro serviço de mensagens.
  - Nunca utilize o mesmo meio para enviar o ficheiro e a palavra-passe.
  - Combine previamente com o destinatário o procedimento de envio e acesso.

Se pretende enviar ficheiros do seu e-mail institucional para o e-mail institucional do destinatário, pode utilizar as funcionalidades de cifragem já disponíveis nos computadores da sua organização. Estas permitem enviar mensagens seguras de forma simples e eficaz, garantindo que tanto o conteúdo da mensagem como os anexos são totalmente cifrados.

Como fazer:

- Ao redigir uma nova mensagem de e-mail, vá ao separador "Opções" e selecione "Encriptar" / "Encriptar" ou "Não reencaminhar".
- A opção "Não Reencaminhar" é a mais recomendada, pois além de cifrar a mensagem, impede que seja copiada, impressa ou reenviada a terceiros não autorizados.
- Estas funcionalidades garantem que o conteúdo da mensagem e os anexos estão cifrados, exigindo a autenticação do destinatário para aceder à informação. ■

FICHA TÉCNICA
Newsletter#3

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