PROTEÇÃO DE DADOS

50 anos CSM Conselho Superior da Magistratura

NEWSLETTER
OUTUBRO 2026

6

Nesta edição

EDITORIAL

CIBERSEGURANÇA NO LOCAL DE TRABALHO

COMO OS CIDADÃOS DA UE ENCARAM A TRANSFORMAÇÃO DIGITAL

SEATRI OU O ELOGIO DA MÁQUINA QUE NÃO PENSA

FEITO POR HUMANOS

GLOSSÁRIO DE A a Z

XX ENCONTRO ANUAL DO CSM

BOAS & PRÁTICAS

Editorial

A 6.ª edição desta newsletter junta-se ao Mês da Cibersegurança Europeia, que se assinala anualmente, desde 2012, no mês de outubro, e traz para as suas páginas o tema da cibersegurança, com base num Eurobarómetro Especial sobre a cibersegurança no local de trabalho que deu o sinal de partida para as celebrações deste ano. Os resultados do questionário feito aos trabalhadores dos 27 Estados-Membros da UE são reveladores da necessidade de passar da teoria à prática e do que ainda falta fazer às organizações.
A cibersegurança é uma componente importante do regime de proteção de dados, impondo o RGPD e a Lei n.º 59/2019, de 8 de agosto, exigências significativas em termos de segurança dos dados pessoais. Trata-se de uma obrigação de resultado, mas os responsáveis pelo tratamento têm de demonstrar que fizeram tudo o que estava ao seu alcance para adotar as medidas técnicas e organizativas adequadas ao risco, avaliado em função das características do tratamento de dados.
Esta edição aborda também a transformação digital, analisando como os cidadãos da UE encaram as políticas digitais e quais devem ser as prioridades futuras. Esta informação, muito recente e publicada no passado mês de setembro, provém de um Eurobarómetro cujos resultados apelam a uma leitura atenta.
Como grande novidade, temos um artigo assinado por João G. Ferreira, do ALTEC/CSM, sobre uma ferramenta de pseudonimização de decisões judiciais sem recurso a inteligência artificial. A não perder!
Por último, não podia faltar a rubrica "Feito por Humanos", em que falamos de encarregados de proteção de dados. Prosseguimos igualmente o nosso Glossário de A a Z, a descodificar os termos de que se ouve falar frequentemente, mas que nem sempre se apreende o seu real significado.

Boa leitura!
Clara Guerra



Cibersegurança no local de trabalho

Três em cada quatro trabalhadores enfrentam ciberameaças no local de trabalho, de acordo com os resultados de um novo Eurobarómetro, que foi publicado pela Comissão Europeia a 30 de setembro último, a assinalar o início do Mês da Cibersegurança Europeia, que se assinala no mês de outubro nos 27 Estados-Membros da UE.

Este Eurobarómetro sobre cibersegurança no local de trabalho pretendeu apurar do conhecimento e da preparação dos trabalhadores da UE sobre vários tópicos de cibersegurança com que se podem confrontar no contexto profissional. Foi coordenado pela Comissão e assentou num questionário realizado em todos os EM durante abril e maio de 2026, sendo as médias da UE27 apuradas em função da população total de cada país. Foram realizadas 25.747 entrevistas.

O phishing foi a mais comum ciberameaça no local de trabalho, com 39% dos trabalhadores a reportar mensagens fraudulentas ou websites desenhados para roubar dados ou ganhar acesso não autorizado. Os trabalhadores também reportaram tentativas de roubar dados pessoais (18%) e palavras-passe (16%), ataques de malware (17%) e esquemas fraudulentos com IA generativa (15%).

Os resultados do Eurobarómetro indicam haver um fosso entre a consciencialização por parte dos trabalhadores e a prática diária. Enquanto 83% afirmam que as potenciais consequências de ciberataques são graves, apenas 48% dizem conseguir reconhecer um vídeo falso gerado por IA. De uma maneira geral, 18% dizem que a sua organização não sofreu qualquer ciberataque, de que tenham conhecimento.

Os trabalhadores reconhecem os comportamentos de risco, designadamente em relação ao phishing e à gestão de palavras-passe. Entre aqueles que usam sistemas e ferramentas digitais no trabalho, 76% afirmam que clicar num link sem verificar o remetente é arriscado, enquanto 74% admitem que usar a mesma palavra-passe na conta pessoal e na conta profissional é um risco e 69% reconhecem que partilhar nas redes sociais informação relacionada com o trabalho coloca riscos.

Contudo, de novo, este proclamado conhecimento frequentemente falha quando traduzido para a aplicação quotidiana. Enquanto 72% dos trabalhadores dizem conseguir identificar emails suspeitos, apenas 54% afirmam verificar o remetente antes de abrir os links e somente 50% dizem que bloqueiam sempre o computador antes de deixar a estação de trabalho.

Hábitos básicos de ciberhigiene são comuns, mas inconsistentes entre os trabalhadores, sendo crescentemente robustos com a idade. Na verdade, a consciencialização dos ciber-riscos também aumenta significativamente com a idade, evidenciando a necessidade de ações de sensibilização dirigidas a jovens trabalhadores até aos 24 anos.

Mais formação e preparação para as organizações

Resulta também deste Eurobarómetro que as organizações precisam de estar melhor preparadas para os ciberataques. De facto, apesar de a maioria dos trabalhadores acreditar que a sua organização é eficaz na proteção contra ciberataques, apenas metade das organizações aplicam medidas de cibersegurança essenciais e um quarto planeia adotá-las.

Seis em cada dez trabalhadores (60%) afirmam ter recebido formação em cibersegurança no ano anterior, embora a participação tenha uma queda abrupta quando se trata de organizações mais pequenas. Ao mesmo tempo, 85% dos trabalhadores estão interessados em melhorar as suas capacidades de cibersegurança, mas 26% indicam a falta de tempo como principal obstáculo a alcançar esse objetivo.

Os dados relativos às respostas de trabalhadores em Portugal são, de uma maneira geral, próximos da média dos 27 EM da UE. Isso mesmo é evidente no que diz respeito às questões sobre exposição ao cibercrime e à fraude e sobre as capacidades e a formação em cibersegurança. Todavia, quanto à perceção dos riscos de cibersegurança, evidenciam-se nas respostas portuguesas percentagens bem superiores à média EU27.

A vice-presidente da Comissão Europeia para a Soberania Tecnológica, Segurança e Democracia, Henna Virkkunen, disse a propósito destes resultados: «O Eurobarómetro de hoje mostra que a consciencialização sobre cibersegurança é elevada. Mas compreender o risco não é o mesmo que estar preparado para ele (…). Isto é um lembrete para cada cidadão, cada empregador e cada organização de que temos de partir da consciencialização para a ação. A Comissão está a trabalhar para reforçar as capacidades, melhorar a preparação e apoiar medidas de cibersegurança mais robustas em toda a Europa. Boa ciberhigiene (…) tem de fazer parte da prática de todos os dias». ■

Como os cidadãos da UE encaram a transformação digital



A Comissão Europeia coordenou um Eurobarómetro Especial sobre a Década Digital 2026 (572), que apresenta as perspetivas e as opiniões dos cidadãos europeus sobre alguns aspetos-chave da transformação digital nos 27 Estados-Membros. Com base em entrevistas realizadas entre fevereiro e março deste ano, este Eurobarómetro focou-se nas prioridades para as futuras políticas digitais e na utilização e desenvolvimento da inteligência artificial. Os resultados foram apresentados no último mês de setembro.

É de salientar que, neste Eurobarómetro, a proteção de dados e a privacidade surgem no centro das atenções dos cidadãos da UE em várias das respostas dadas, constituindo-se como uma preocupação quando está em risco este direito fundamental e sendo motor de opções mais seguras e garantísticas.

A grande maioria dos cidadãos europeus (79%) considera que a política digital deve ser uma alta prioridade para o futuro da UE. No que toca às prioridades estratégicas, os europeus defendem que a Europa se deve posicionar como um líder digital global. Nesse contexto, 85% apoiam investimentos em infraestruturas desenvolvidas na Europa, enquanto 82% apoiam uma redução da dependência de países fora da União. Acresce que 58% mudariam para um fornecedor de serviços europeu, mesmo a custo mais elevado.

Os cinco fatores mais relevantes que sustentam a mudança para um fornecedor europeu são, para os respondentes, uma maior segurança e confiança (50%), melhor proteção de dados pessoais (49%), regras mais claras de proteção dos consumidores (39%), dependência reduzida de países fora da UE (33%) e apoio à economia e à competitividade da UE (30%).

De acordo com o Eurobarómetro, os cidadãos europeus são a favor de uma maior cooperação entre os Estados-Membros para reforçar a cibersegurança (91%), para promover a educação digital (88%), para reforçar a regulação das plataformas online (84%) e para construir uma infraestrutura digital independente europeia (83%).

Para os próximos 10 anos, os cidadãos europeus priorizam como objetivos digitais da UE proteger a privacidade e a segurança (92%), tornar as ferramentas digitais mais acessíveis para toda a gente (89%) e usar as ferramentas digitais para simplificar a vida às pessoas e aos negócios (86%).

Quanto às plataformas online, as questões que mais afetam os cidadãos da UE são: notícias falsas e desinformação (53%); má utilização de dados pessoais (47%); insuficiente proteção das crianças (41%); discurso de ódio (26%) e vendedores online em que não se pode confiar (26%).

Proteger as crianças online surge como uma das grandes preocupações com 92% dos europeus a considerar ser uma elevada prioridade digital.

Questionados especificamente sobre a matéria, 87% dos respondentes concordam que a manipulação online é uma ameaça à democracia.

Sobre as tecnologias com impacto mais positivo nos próximos 10 anos, os cidadãos europeus elegeram as tecnologias de saúde digital (55%), as tecnologias digitais verdes (50%) e a conetividade à Internet mais rápida (42%).

Utilização de IA

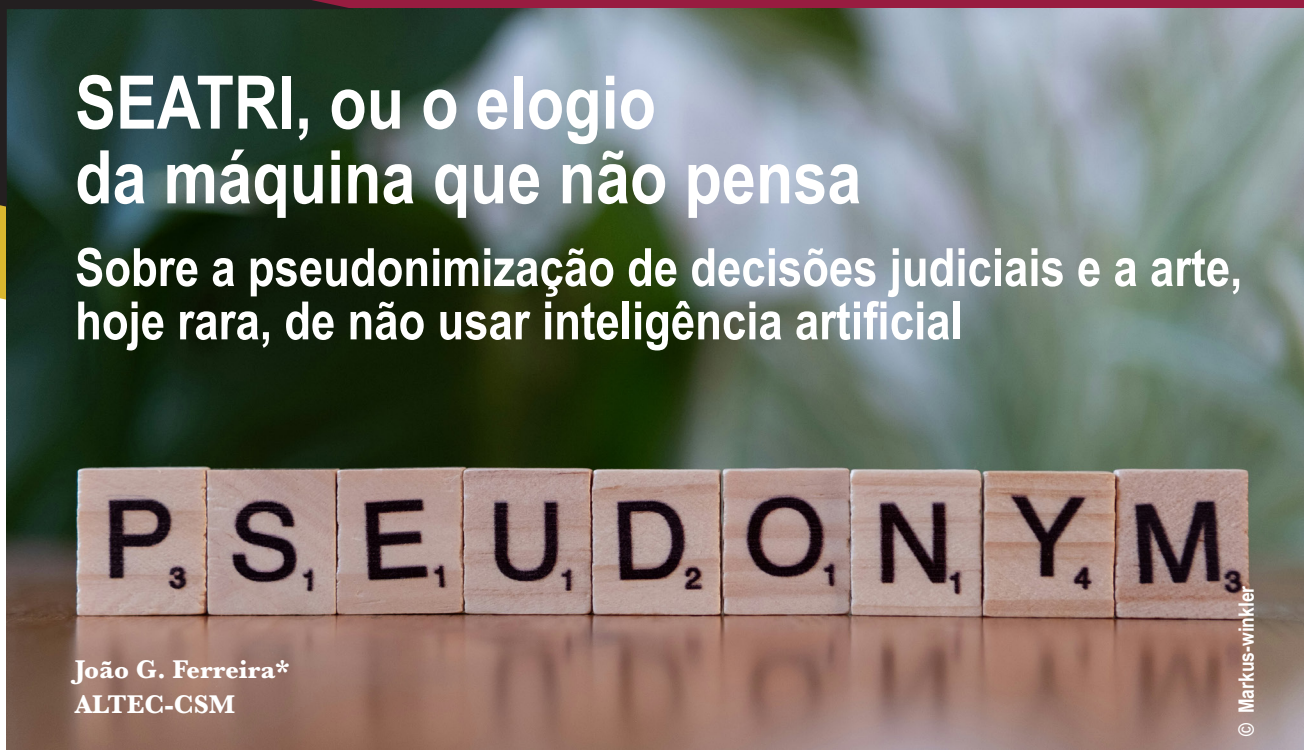
Mais de metade dos cidadãos da UE usam ferramentas de IA generativa: 59% usam-nas na sua vida pessoal e 49% no seu trabalho ou estudos. No entanto, 80% dos cidadãos europeus consideram que o desenvolvimento da inteligência artificial deve ser cuidadosamente regulado por uma questão de segurança, mesmo que isso atrase quem desenvolve a IA.

Os maiores obstáculos citados pelos respondentes ao desenvolvimento de IA são preocupações de privacidade (39%), receio de informação não rigorosa (36%) e preocupações sobre questões éticas ou má utilização das ferramentas de IA (32%).

Sobre prioridades para o desenvolvimento de IA, os cidadãos da UE concordam com mais IA sustentável (78%), com mais IA para melhores serviços públicos (76%) e com mais ferramentas de IA detidas pela UE (74%). ■

SEATRI, ou o elogio da máquina que não pensa

Sobre a pseudonimização de decisões judiciais e a arte, hoje rara, de não usar inteligência artificial



João G. Ferreira*
ALTEC-CSM

I. Uma confissão

Vivemos num tempo em que tudo tem inteligência artificial. As torradeiras têm inteligência artificial; as escovas de dentes também; há frigoríficos que meditam sobre o conteúdo das suas prateleiras. Nenhum produto ousa chegar ao mercado sem o selo mágico, porque o mercado perdoa tudo menos a sobriedade.

É neste cenário que devo uma confissão que roça a imprudência: o Conselho Superior da Magistratura ensaia, em fase beta, uma ferramenta de anonimização de decisões judiciais que não usa inteligência artificial. Nem muita, nem pouca: rigorosamente nenhuma. O SEATRI (Sistema Eletrónico de Anonimização dos TRIbunais), desenvolvido no ALTEC (Apoio Logístico à Tramitação de Elevada Complexidade), lê acórdãos e sentenças, deteta nomes, moradas, números de identificação e cerca de três dezenas de outras categorias de dados pessoais, propõe pseudónimos, submete tudo a revisão humana e devolve um documento pronto a publicar - sem que o documento alguma vez saia do computador de quem o trata. E fá-lo com as tecnologias menos glamorosas do catálogo: expressões regulares, dicionários e aritmética. A escolha não é um atraso de vida, mas uma decisão de engenharia: precisamente onde a Justiça toca os dados pessoais dos cidadãos, a ausência de inteligência é, paradoxalmente, a opção mais inteligente.

II. Publicar sem expor

O CSM balizou esse caminho com minúcia invulgar: a deliberação do Plenário de 11 de abril de 2023, atualizada em 2 de junho de 2025, fixa os dados a ofuscar e a técnica aplicável a cada categoria. Os magistrados e os autores citados como doutrina mantêm-se - anonimizar o juiz seria uma inovação curiosa em matéria de transparência. Várias categorias pedem ofuscação apenas parcial: no endereço eletrónico preserva-se o domínio, no IBAN sobrevive o «PT50», na data de nascimento fica o ano, na morada mantém-se o tipo de via. O leitor ficará a saber que o réu morava numa travessa; em qual, isso já não. Some-se a escala - milhares de decisões por ano, com dezenas de páginas cada - e o problema pedia uma ferramenta. A pergunta séria era outra: que espécie de ferramenta merece que lhe confiemos isto?

III. Cinco razões, e nenhuma é nostalgia

A primeira é a confidencialidade. Um acórdão por anonimizar é o objeto mais sensível de todo o circuito de publicação; para um modelo remoto o tratar, o documento teria de ir ter com ele. O SEATRI inverte a premissa: o documento nunca sai do computador do utilizador. Toda a cadeia corre localmente, dentro do navegador: não há nuvem, não há subcontratantes, não há transferência nenhuma - é o artigo 25.º do RGPD tomado como planta arquitetónica. O leitor desconfiado pode desligar o cabo de rede a meio do trabalho: o SEATRI prossegue, imperturbável; o que, em 2026, não se pode dizer de quase nada.

A segunda é o determinismo. Um modelo generativo é, por construção, probabilístico; num domínio em que um único nome esquecido constitui uma violação de dados pessoais, essa criatividade é um passivo. O motor do SEATRI não alucina nem tem dias maus: um número de nove dígitos ou

é um NIF ou não é - o dígito de controlo decide. E quando erra, erra de forma reproduzível: corrige-se a regra e o erro não volta. Depurar uma rede neuronal parece-se menos com engenharia e mais com o interrogatório de uma testemunha evasiva.
A terceira é a fundamentação. Cada deteção tem justificação enunciável: o padrão que correspondeu, o vocabulário processual ao lado, a validação matemática que confirmou. «O modelo achou que sim» não é fundamentação; e os juristas, que passam a vida a exigi-la aos outros, dificilmente aceitariam menos de uma máquina.
A quarta é a disponibilidade. Toda a solução assente num serviço remoto - e já existiam, meritórias e pioneiras - paga a física da própria arquitetura: filas, janelas de manutenção e o inevitável «serviço indisponível, tente novamente». O SEATRI nunca dirá tal coisa, pela razão singela de que não tem serviço que possa estar indisponível: responde no próprio computador, todas as vezes.
A quinta é a mais terrena: o custo. Um serviço de inteligência artificial cobra-se ao pedido, à página, ao token; uma política pública de publicação de jurisprudência mede-se aos milhares de documentos. O SEATRI corre no computador que já está em cima da secretária, e o custo marginal de cada documento é zero: a diferença entre publicar o que o orçamento permite e publicar o que a transparência exige.
Resta a objeção séria: e os nomes que escapam? A resposta está no desenho, não na sorte: a heurística de contexto reconhece um nome desconhecido pela companhia que mantém - «o arguido», «a testemunha», «residente em» - e, na dúvida, a ferramenta lista em vez de calar: o candidato incerto aparece ao revisor, desativado, mas visível. A revisão humana não é enfeite regulamentar: há riscos que só um humano vê, como o do «mosaico», que identifica sem um único nome; o próprio RGPD o recorda no considerando 26 - a pseudonimização reduz o risco, não o extingue. O SEATRI não decide: assiste; a autoridade final é do revisor.

IV. Como funciona, em quatro atos

Primeiro, a extração: o documento (PDF, Word, Excel ou texto simples) é lido localmente e a estrutura reconstruída, porque anonimizar bem começa por ler bem. Segundo, a deteção em camadas: padrões com validação matemática (um candidato a NIF só é aceite se o dígito de controlo o confirmar), dicionários onomásticos tolerantes a acentos e gralhas (o «João Manuel Silva» da página 3 e o «Silva» da página 41 recebem o mesmo pseudónimo) e pontuação por contexto jurídico. Terceiro, os pseudónimos: determinísticos, numerados e consistentes - ARGUIDO.1, TESTEMUNHA.2 -, com as técnicas parciais cumpridas à letra; o mapa entre originais e pseudónimos fica apenas no computador do utilizador, cifrável com uma frase-passe (AES-GCM): reversível para quem de direito, ilegível para todos os outros. Quarto, a revisão e a entrega: o revisor valida, ignora, funde e reclassifica; a exportação troca cirurgicamente os vãos de texto no próprio ficheiro Word, preservando a formatação; e, antes de entregar, a ferramenta desconfia de si própria - compara o resultado com o original e varre cabeçalhos, rodapés, notas e até a miniatura de pré-visualização, exigindo confirmação humana se encontrar o que quer que seja.

V. O oleiro e o barro

O SEATRI não nasceu num laboratório de informática; nasceu da leitura de acórdãos. A ideia e o primeiro protótipo - coisa que não se diz todos os dias de um desembargador - pertencem a António Gomes; a conceção e os testes couberam a ele e a João A. Ferreira, ambos juízes desembargadores do ALTEC. Não existe controlo de qualidade mais rigoroso do que um desembargador com um acórdão verdadeiro na mão e a expectativa serena de que a máquina não lho estrague. A fase beta que agora decorre existe precisamente para encontrar defeitos, e vai encontrá-los; fica desde já registada a previsão, para poupar trabalho aos críticos.
Fique claro, para desfazer mal-entendidos confortáveis: este artigo não é um manifesto contra a inteligência artificial - seria, vindo de mim, uma hipocrisia notável. A maior parte do que o ALTEC constrói assenta fortemente em inteligência artificial; o SEATRI é, nesse portefólio, a exceção deliberada. E devo ao leitor a ironia completa: o próprio SEATRI foi desenvolvido com auxílio de inteligência artificial - na escrita do código, nos testes, na caça aos defeitos. A ferramenta que não pensa foi construída com a ajuda de uma que pensa; e a diferença, que é toda a diferença, está no sítio onde cada uma trabalha. A inteligência artificial ajudou a construir o cofre, mas não ficou com a chave. No núcleo do tratamento de dados pessoais de um acórdão exige-se previsibilidade, verificabilidade e confinamento local; e estas três palavras, hoje, ainda se escrevem sem redes neuronais.
O SEATRI não aprende, não conversa, não promete. Lê, conta, confere e sublinha. Não telefona para casa, porque não tem casa para onde telefonar. E quando termina, entrega a última palavra a quem sempre a teve e a deve continuar a ter: o juiz.
Num tempo em que as torradeiras têm opiniões, talvez seja esta a verdadeira inovação. ■

* Engenheiro; Consultor no Conselho Superior da Magistratura / ALTEC



Feito por humanos

O número

6207

Encarregados da proteção de dados (EPDs) notificados à Comissão Nacional de Proteção de Dados (CNPD) à data de 30 de setembro de 2026. Entre estes, 1233 EPDs foram designados por entidades públicas e 4974 desempenham funções no setor privado.

O total de EPDs registados na CNPD tem vindo a crescer continuamente. No final do ano de aplicação do RGPD, em 2018, havia 1916 EPD notificados. Em 2019, atingiram-se as 2925 notificações ativas e, em 2020, superou-se a fasquia dos 3 mil EPD (3474).

Nos cinco anos seguintes, o número de EPD notificados à CNPD registou um aumento de cerca de 500 novas notificações por ano, cifrando-se em 5954 no final de 2025.

Neste momento já foi ultrapassada a barreira dos 6 mil EPD.

A palavra

Violação
(de dados pessoais)

Uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento

(Definição constante do artigo 4.º, ponto 12), do Regulamento (UE) 2016/679 - RGPD)



XX Encontro Nacional do CSM

O XX Encontro Anual do CSM, sob o tema "Refletir o passado. Projetar o futuro", traz uma vez mais a proteção de dados pessoais para os debates. Assim, no próximo dia 20 de novembro, o Painel IV discutirá "Os caminhos da inovação na tecnologia e na organização judiciária". Nesse contexto, o tópico da proteção de dados estará presente pela mão da Encarregada de Proteção de Dados do CSM.

Este Encontro Anual é duplamente especial, não só porque acontece na celebração dos 50 anos da consagração constitucional do Conselho, mas também porque decorre em paralelo e em sintonia com a Judiciary Tech Summit, um evento internacional coorganizado pelo CSM e pela Faculdade de Direito da Universidade de Lisboa.

Ambos os eventos têm lugar no Pavilhão de Portugal, em Lisboa, num dos edifícios mais emblemáticos da arquitetura contemporânea portuguesa. Projetado pelo arquiteto Álvaro Siza Vieira (com a colaboração de Eduardo Souto Moura nos espaços expositivos interiores) e engenharia de António Segadães Tavares, foi inaugurado a 22 de maio de 1998 como pavilhão oficial de Portugal na EXPO'98.

O seu elemento mais icónico é a imponente pala de betão pré-esforçado que, assente em dois pórticos de betão, vence um vão monumental e dá forma a uma ampla praça com vista para o rio, também chamada Praça Cerimonial.

O Pavilhão de Portugal recebeu o Prémio Valmor e o Prémio Municipal de Arquitetura em 1998 e, em 30 de março de 2010, foi classificado como Monumento de Interesse Público.

O monumento passou em 2015 para a alçada da Universidade de Lisboa, que procedeu à requalificação total do espaço. Reabriu a 30 de abril de 2025, transformado num polo dedicado à ciência, à cultura, à inovação e a eventos académicos.

Ponha já na sua agenda e vá ficando a par das novidades:

- **Encontro Anual do CSM:** 19 e 20 de novembro. As inscrições já estão abertas.
- **Judiciary Tech Summit:** 17 a 20 de novembro. Brevemente ficará disponível o programa final e serão abertas as inscrições, em website próprio do evento. ■

50 anos CSM Conselho Superior da Magistratura

Glossário de A a Z



Gestão de identidades

É o processo centralizado para gerir as identidades dos utilizadores e os privilégios de acesso que detêm. Requer o registo e o controlo de identidades dentro de uma organização e a aplicação de políticas de governação de identidades. Basicamente, a identidade digital do utilizador é o perfil que o identifica quando usa a rede, enquanto o acesso se refere às permissões que o utilizador tem atribuídas quando se autentica. Em conjunto, formam uma parte importante sobre como o utilizador interage com a tecnologia. É a forma como o computador sabe que é mesmo uma determinada pessoa que está a tentar autenticar-se e não outra pessoa qualquer.

[fonte: www.iso.org]

Hacktivism

Atividade que ocorre quando ativistas sociais ou políticos usam tecnologia informática para tomar posição em defesa das suas causas. "Hacking" (em Inglês) significa invadir ou piratear o computador de alguém, e "ativismo" diz respeito à pro-

Cibersegurança
Boas & Práticas



Desta vez abordamos um tópico muito importante e que constitui uma das ameaças mais recorrentes nos dias de hoje, sendo responsável pela partilha de dados pessoais com terceiros desconhecidos, com base em técnicas sofisticadas de engenharia social que levam as pessoas a cair em logros e a permitir ataques às suas contas de utilizador pessoais ou a sistemas informáticos das organizações onde trabalham.
Para o efeito, recorremos como fonte a um guia público do Centro Nacional de Cibersegurança, atualizado em 1 de agosto de 2024, e a ilustrações da ENISA - Agência para a Cibersegurança da UE sobre o tema.

À Pesca de dados

O ***phishing*** é um tipo de ataque em que se usam técnicas de engenharia social para capturar informação sensível de uma vítima através de email. Um agente de ameaça que utilize este tipo de ataque procura enganar os recetores de emails para que estes disponibilizem informação sensível através do clique em anexos e/ou URL maliciosos ou da partilha de dados em páginas fraudulentas. Para o efeito, o atacante simula uma marca credível ou personifica alguém de confiança.
Quando esta técnica é utilizada através de SMS, dá pelo nome de ***smishing*** e, por telefone (voz), de ***vishing***.
Esta técnica também pode ser usada através de mensagens instantâneas em aplicações de redes sociais.

O que fazer

- Não clicar em anexos ou links de emails, de mensagens instantâneas ou de SMS suspeitos;
- Quando se é contactado, confirmar a veracidade do endereço de email, do perfil ou do número de telefone de origem;
- Avaliar sempre a oportunidade dos conteúdos de emails, de mensagens instantâneas, de SMS ou de telefonemas;

moção de uma perspetiva social ou política. "Hacktivism" é uma combinação das duas. A maioria dos ataques informáticos tem como alvo organizações governamentais ou empresariais, mas também outro tipo de entidades relevantes, tais como grupos religiosos, traficantes de droga, terroristas ou pedófilos. Os métodos usados são muito variados, tal como a gravidade e a legalidade das suas ações. Frequentemente, os hacktivistas cometem cibercrimes, como quando lançam ataques de negação de serviço (DoS, denial-of-service) para interromper os serviços, os quais podem resultar em avultados prejuízos para as organizações.

[fonte: www.fortinet.com/uk]

Identidade digital

No seu nível mais básico, método pelo qual cada um se identifica perante um sítio Web, um serviço da Internet, uma rede de computadores ou outro utilizador em linha. Atualmente há muitas formas de o fazer, usando elementos como nomes do utilizador, palavras-passe, números de identificação pessoal (PIN) e certificados digitais.

[fonte: www.apdsi.pt]

- Não partilhar dados pessoais ou seguir instruções sem verificar noutras fontes a veracidade do pedido – por exemplo, junto do gestor de conta do Banco ou de um superior hierárquico;
- Desconfiar de mensagens com erros formais de linguagem, mas também não confiar em todas as mensagens apenas porque não apresentam erros formais de linguagem;
- Nas organizações, realizar simulações de ataques de *phishing* e *smishing*, e eventualmente de *vishing*, de modo a aumentar a sensibilização e os níveis de atenção a estes meios;
- Não partilhar dados sensíveis nas redes sociais porque essa prática pode fornecer informação a possíveis atacantes que queiram realizar *spear phishing (phishing* dirigido a uma pessoa específica);
- Denunciar junto dos responsáveis de segurança informática da organização ou junto das autoridades sempre que se é alvo ou vítima de um ataque deste tipo;
- Estar atento e não se deixar persuadir sem reflexão por solicitações autoritárias, promessas ou pedidos urgentes. ■



FICHA TÉCNICA
Newsletter #6 outubro 2026

EDIÇÃO
Serviço de Proteção de Dados do CSM
Clara Guerra, Filipe Matias e Luísa Pedroso

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