

CENTR Jamboree

Berlim, 6 a 8 de maio de 2026

.pt

ÍNDICE

Introdução.....	3
Regulação, Compliance e Governança da Internet.....	4
Segurança, Resiliência e Continuidade de Negócio.....	6
Inteligência Artificial e o Futuro dos Domínios.....	7
Analytics, Retenção e Crescimento	9
Marketing.....	9
Operação e Negócio	11
Conclusão	13

Introdução

Entre os dias 6 e 8 de maio de 2026, o .PT participou no CENTR Jamboree 2026, realizado em Berlim, encontro anual que reuniu representantes de *registries* europeus, parceiros tecnológicos, especialistas do setor e membros da comunidade da Internet para discutir os principais desafios e tendências que moldam a evolução do ecossistema dos nomes de domínio.

A participação do .PT neste evento voltou a refletir o nosso compromisso com a cooperação internacional, a partilha de conhecimento e o acompanhamento das transformações tecnológicas, operacionais e regulatórias que impactam a comunidade dos ccTLDs. O programa deste ano evidenciou um setor em profunda evolução, marcado pela crescente relevância da inteligência artificial, pela intensificação das exigências regulatórias europeias, pela necessidade de reforço da segurança e resiliência das infraestruturas digitais e pela crescente adoção de modelos de gestão suportados em dados.

O .PT integrou ativamente o programa do evento através da participação de Ana Cunha na sessão “Standardizing Registry Lock Across TLDs”, juntamente com Eric Skoglund (Internetstiftelsen) e Leanne Kenny (Markmonitor). Nesta sessão foi apresentado o trabalho desenvolvido pelo grupo CENTR Registry Lock para a criação de uma solução harmonizada de Registry Lock aplicável a diferentes TLDs, bem como os desenvolvimentos em curso com vista à apresentação de uma proposta de extensão EPP junto da IETF.

Para além desta intervenção, representantes do .PT acompanharam os trabalhos dos diferentes Working Groups do CENTR, bem como diversas sessões dedicadas a temas de relevância estratégica para os *registries* europeus, incluindo governação da Internet, *compliance*, DNS Abuse, continuidade de negócio, *analytics*, retenção de clientes, marketing e os impactos da inteligência artificial na descoberta de conteúdos e na gestão dos nomes de domínio.

As secções seguintes apresentam os principais temas e conclusões recolhidos ao longo das diversas sessões e grupos de trabalho.

Regulação, Compliance e Governação da Internet

A sessão “Trusted Flagger”, apresentada por Charlotte Stausholm, incidiu sobre o papel crescente dos mecanismos de *trusted flagging* no combate a conteúdos e atividades ilícitas online, num contexto marcado pela aplicação do Digital Services Act e pelo reforço das expectativas regulatórias relativamente aos prestadores intermediários de serviços digitais. A apresentação destacou a importância da cooperação entre prestadores de serviços digitais, autoridades competentes e entidades reconhecidas como *trusted flaggers*, bem como os desafios associados à escalabilidade, proporcionalidade e transparência dos mecanismos de *trusted flagging*.

Foi igualmente salientado que os *registries* e *registrars* estão cada vez mais inseridos neste ecossistema de mitigação de riscos digitais, sendo expectável um aumento dos pedidos de atuação célere relativamente a domínios associados a fraude, phishing ou outras formas de DNS Abuse. A sessão reforçou a necessidade de existência de processos internos claros, critérios objetivos de avaliação e canais de cooperação eficientes entre as diferentes partes envolvidas.

A sessão “TCCM in Action: Strengthening Multistakeholder Internet Governance in a post-WSIS+20 world”, apresentada por Charles Noir, centrou-se na evolução dos debates internacionais em matéria de governação da Internet e no posicionamento do Technical Community Coalition for Multistakeholderism (TCCM) no contexto do processo WSIS+20. Foi destacado como principal desenvolvimento o reconhecimento explícito do TCCM no *draft* dos *outcomes* do WSIS+20, considerado um passo relevante para consolidar o papel da comunidade técnica no modelo *multistakeholder* de governação da Internet.

A apresentação identificou igualmente as principais áreas de foco do TCCM para 2026, incluindo o reforço da governação *multistakeholder* da Internet, a manutenção de uma Internet aberta, interoperável e resiliente, e o reforço da participação em fóruns internacionais como a ITU, IGF e ICANN. Foi ainda sublinhada a necessidade de maior coordenação entre atores técnicos e decisores políticos, numa fase em que as discussões sobre soberania digital, cibersegurança e regulação da Internet assumem crescente relevância geopolítica.

A sessão “DENIC’s Journey Towards NIS2 Implementation” abordou o percurso da DENIC na implementação da Diretiva NIS2, evidenciando os desafios operacionais, jurídicos e organizacionais associados ao novo quadro regulatório europeu. Entre os principais aspetos destacados estiveram a necessidade de adaptação de processos internos, a definição de mecanismos de verificação e validação de dados e o reforço da coordenação entre equipas técnicas, operacionais e jurídicas.

A DENIC apresentou igualmente vários “lessons learned” resultantes do processo de implementação, salientando a importância de processos estruturados, do envolvimento transversal das equipas internas e da definição de *milestones* claras. Foram ainda referidos os desafios relacionados com a operacionalização dos novos requisitos de verificação, incluindo volumes significativos de pedidos de validação e a necessidade de automatização progressiva de procedimentos. Algumas das métricas partilhadas ilustraram o impacto operacional do processo.

A sessão “When regulation meets reality” promoveu uma reflexão particularmente prática sobre as dificuldades de implementação concreta das obrigações legais associadas à NIS2 e à publicação de dados de registo. A apresentação utilizou o caso sueco para demonstrar a tensão existente entre os objetivos regulatórios de transparência, rastreabilidade e segurança e as limitações decorrentes da proteção de dados pessoais e da realidade operacional dos *registries*.

Entre os principais pontos debatidos estiveram os impactos da remoção de dados pessoais do WHOIS, a crescente complexidade dos pedidos de acesso a dados e a dificuldade em equilibrar requisitos legais potencialmente contraditórios. Foi ainda sublinhado que a implementação prática da regulação depende fortemente do contexto nacional, da interpretação das autoridades competentes e da maturidade operacional de cada *registry*, o que conduz a abordagens distintas entre ccTLDs europeus.

A sessão “Compliance Management as a Science, Craft, and Art”, apresentada por Declan McDermott, abordou o *compliance* não apenas como um exercício jurídico ou formal, mas como uma disciplina transversal que exige equilíbrio entre interpretação regulatória, gestão operacional e cultura organizacional. A apresentação destacou que a crescente complexidade regulatória obriga os *registries* a desenvolver abordagens cada vez mais estruturadas, documentadas e colaborativas entre equipas técnicas, jurídicas e de gestão.

Foi igualmente enfatizada a importância de mecanismos internos claros de *governance*, documentação de processos, *accountability* e gestão de risco, bem como a necessidade de transformar *compliance* num elemento integrado da estratégia organizacional e não apenas numa obrigação reativa. A sessão sublinhou ainda que a maturidade de *compliance* dos *registries* será cada vez mais relevante num contexto marcado por NIS2, DORA, DSA e crescente escrutínio regulatório europeu.

A sessão “Abuse and the importance of registrant verification” focou-se na relevância crescente da validação e verificação de dados de titulares como instrumento essencial de mitigação de DNS Abuse. Os oradores apresentaram exemplos práticos sobre mecanismos de verificação, análise de risco e impacto operacional de medidas preventivas no combate a phishing, malware e fraude online. Neste âmbito, destaca-se como problemática a utilização de proxy services, que o .se procurou endereçar incluindo nos seus TC’s a seguinte referência: “The information must be completed and correct. Information provided with the intention to shield the identity can be considered as incorrect”.

A discussão evidenciou igualmente as tensões existentes entre requisitos regulatórios, experiência do utilizador e eficácia operacional, sobretudo num contexto em que os *registries* enfrentam expectativas crescentes relativamente à qualidade e fiabilidade dos dados de registo. Foi reforçada a ideia de que a validação de dados deverá assumir um papel cada vez mais central na estratégia de prevenção de abuse, em articulação com os requisitos decorrentes da NIS2 e de futuras iniciativas europeias.

No terceiro dia, dedicado aos Working Groups, a sessão “ETSI standardisation: Takedown requests and access to e-evidence”, apresentada pela EUROPOL, incidiu sobre os trabalhos de normalização técnica desenvolvidos pelo ETSI relativamente a pedidos de *takedown* e acesso a *e-evidence*. Foi explicado que os standards ETSI TR 104 126 e ETSI TR 104 144 pretendem criar mecanismos claros, consistentes, seguros e eficientes para submissão e tratamento de pedidos por autoridades competentes, incluindo pedidos relacionados com nomes de domínio.

A EUROPOL clarificou que estes standards têm natureza técnica e operacional, não criando, por si só, obrigações jurídicas de atuação ou resposta por parte dos *registries*. A legitimidade do pedido continuará sempre dependente do enquadramento legal aplicável. Foi ainda referido que a Comissão Europeia está a promover *webinars* regulares sobre o novo sistema associado ao Regulamento e-Evidence, cuja aplicação prática deverá iniciar-se a partir de agosto.

A sessão “Preparing for e-Evidence Regulation”, conduzida por Peter Koch, centrou-se nos preparativos operacionais e organizacionais associados à entrada em vigor do Regulamento e-Evidence. Foram abordados aspetos relacionados com ajustamentos internos de processos, interação com autoridades competentes e desafios associados ao acesso a sistemas descentralizados e ao tratamento de pedidos transfronteiriços.

A apresentação evidenciou que, apesar de ainda existirem incertezas práticas e jurídicas, os *registries* já se encontram a preparar procedimentos internos e canais de comunicação dedicados para acomodar o novo quadro europeu. Foi igualmente sublinhada a importância de alinhamento entre equipas técnicas e jurídicas, bem como da manutenção de diálogo próximo com autoridades nacionais.

Na sessão “Post-WSIS+20: ccTLDs & Internet Governance”, os participantes refletiram sobre o atual momento da governação da Internet e os desafios associados à preservação do modelo *multistakeholder*. A intervenção do .de destacou sobretudo uma reafirmação de confiança no modelo atual, defendendo que o mesmo continua funcional e adequado. Já o .se alertou para o facto de não ser possível assumir como garantida a continuidade deste equilíbrio institucional e político.

O .ca destacou igualmente a relevância destas discussões para o relacionamento entre *registries* e governos nacionais, defendendo que os ccTLDs podem assumir um papel relevante na promoção e defesa dos princípios *multistakeholder* junto das autoridades públicas. Foi ainda referido que continuam sem existir decisões internas sobre o futuro financiamento do IGF global, refletindo alguma incerteza quanto à sustentabilidade futura de determinados fóruns internacionais de governação da Internet.

Por fim, a sessão “EU Policy Update”, apresentada por Polina Malaja, abordou os principais desenvolvimentos regulatórios europeus relevantes para os *registries*. No âmbito do Digital Omnibus, destacou-se o apoio do Conselho Europeu à criação de um mecanismo único de reporte de incidentes de cibersegurança, bem como as reservas relativamente ao eventual aumento para 96 horas do prazo de notificação de violações de dados pessoais. Foram igualmente debatidas preocupações quanto à nova definição de dados pessoais e à necessidade de clarificação por parte do EDPB sobre como proceder à pseudonimização e anonimização de dados.

Relativamente ao Cybersecurity Act 2.0, foi referido que o comentário do CENTR se encontra em preparação e que a versão final do diploma apenas deverá ser publicada em 2027. Quanto à regulação financeira, foi indicado que a proposta FiDA continua bloqueada nos trólogos, sem perspectiva de alterações relevantes nas disposições que impactam os *registries*. Foram ainda partilhadas atualizações sobre o PSR e discutidas expectativas regulatórias futuras, confirmando a crescente interligação entre cibersegurança, proteção de dados e supervisão regulatória europeia.

Segurança, Resiliência e Continuidade de Negócio

A sessão “Public awareness on web and e-mail security” foi apresentada por Kristian Hansen (Punktum dk, Dinamarca) e Pamela Davidsson (Internetstiftelsen, Suécia), e abordou duas iniciativas nórdicas complementares para promover a adoção de boas práticas de segurança na internet.

A apresentação dinamarquesa centrou-se no Sikkerpånettet.dk, uma ferramenta gratuita de avaliação de segurança lançada em 2020, baseada no motor holandês internet.nl. A ferramenta permite a qualquer proprietário de um domínio .dk testar a segurança do seu site, servidor de e-mail e ligação à internet, recebendo uma pontuação e orientações concretas sobre como corrigir as falhas detetadas. O projeto enquadra-se numa estratégia mais ampla da Dinamarca para tornar a zona .dk a mais segura do mundo, recorrendo a consultas públicas, incentivos aos registradores e parcerias com entidades institucionais e do setor privado. Desde o lançamento foram realizados cerca de 400 mil testes individuais, o que é considerado um resultado expressivo para um país de 6 milhões de habitantes. Os próximos desenvolvimentos incluem a simplificação da experiência de utilização, a adoção do motor atualizado do internet.nl e uma análise mais aprofundada por setores como banca, municípios e PMEs.

A componente sueca apresentou o Internetkollen.se, solução equivalente operada pela Suécia, que monitoriza continuamente os domínios mais críticos das zonas .se e .nu. Até 2025, o sistema baseava-se na ferramenta Hardenize; em 2026 migrou igualmente para o motor internet.nl. Os dados recolhidos em abril de 2026 revelam que apenas 36% dos domínios críticos à sociedade estão bem configurados a nível web, com variações significativas entre setores — os jornais e os bancos apresentam os melhores resultados, enquanto municípios, universidades e o setor das telecomunicações ficam claramente abaixo da média. A Suécia disponibiliza ainda estes dados através do kolada.se, uma plataforma que permite comparar a maturidade digital dos municípios suecos ao longo do tempo.

A sessão “A Business Continuity Playbook v2”, apresentada por Dirk Jumpertz (TLD ISAC), abordou as boas práticas associadas à preparação e manutenção de planos de continuidade de negócio em organizações responsáveis por infraestruturas críticas. A apresentação incidiu sobre a necessidade de revisão periódica dos planos, identificação de dependências críticas e definição clara de responsabilidades durante situações de crise. Foi igualmente salientada a importância da realização de exercícios regulares como forma de validar procedimentos e reforçar a preparação das equipas.

A sessão “From Chaos to Clarity: Mastering Crisis Management through Realistic Exercise Training”, apresentada por Catharina Ankre (Internetstiftelsen), Kristof Tuyteleers (DNS Belgium) e Dirk Jumpertz (TLD ISAC), focou-se na utilização de exercícios de simulação como ferramenta de preparação para cenários de crise. Os oradores partilharam experiências adquiridas através de exercícios realizados no contexto do TLD ISAC, destacando a importância de recriar situações realistas de elevada pressão para testar processos de tomada de decisão, coordenação interna e comunicação entre equipas.

As discussões demonstraram que a gestão de crise e a continuidade de negócio assumem uma relevância crescente para os *registries*, não apenas devido ao aumento das ameaças cibernéticas, mas também em consequência das exigências regulatórias associadas à NIS2 e à crescente dependência das organizações relativamente a infraestruturas digitais críticas.

Inteligência Artificial e o Futuro dos Domínios

A sessão “How domains remain relevant in the age of AI”, apresentada por Michiel Henneke (SIDN) e Lars Jensen (ShortDot), abordou o impacto da inteligência artificial no ecossistema dos nomes de domínio e a forma como os ccTLDs poderão continuar a desempenhar um papel relevante num contexto de crescente utilização de ferramentas de IA generativa. Os oradores recordaram que, ao longo dos anos,

os domínios foram sucessivamente considerados ameaçados pelo surgimento dos motores de pesquisa, das redes sociais, das aplicações móveis e dos *marketplaces*, sem que isso tenha comprometido o seu crescimento sustentado.

A principal mensagem transmitida foi a de que a inteligência artificial poderá não representar uma ameaça ao ecossistema dos domínios, mas antes um fator de aceleração da economia digital. Ao reduzir significativamente as barreiras à criação de websites, produtos digitais, automações e pequenos negócios online, a IA poderá contribuir para o surgimento de um maior número de identidades digitais, aumentando consequentemente a necessidade de registo de domínios. Neste contexto, foi reforçada a importância dos domínios enquanto elementos de confiança, reputação, soberania digital e presença própria na Internet.

A sessão “The Future of Domain Names in the Age of AI: A Cooperative International Research on GeoTLDs Supported by ICANN Grants”, apresentada por Beatriz Guzmán e Josep Masoliver (.cat), incidiu sobre os potenciais impactos dos motores de pesquisa baseados em inteligência artificial na visibilidade dos nomes de domínio. O projeto apresentado procura analisar a forma como diferentes modelos de linguagem, incluindo ChatGPT, Gemini e Perplexity, tratam diferentes TLDs e se existem diferenças significativas relativamente aos resultados obtidos através dos motores de pesquisa tradicionais.

Foi introduzido o conceito de *visibility gap*, utilizado para descrever situações em que domínios com bom posicionamento nos motores de pesquisa convencionais apresentam menor relevância ou visibilidade em plataformas baseadas em IA. O estudo encontra-se ainda numa fase inicial, mas poderá contribuir para compreender de que forma os *registries* deverão adaptar as suas estratégias de presença digital à evolução dos mecanismos de descoberta de conteúdos online.

A sessão “AI policies across CENTR ccTLDs” promoveu uma troca de experiências entre vários *registries* relativamente à adoção de políticas internas sobre inteligência artificial. Foram debatidas abordagens distintas quanto à utilização de ferramentas de IA generativa, mecanismos de *governance* interna, avaliação de risco e necessidade de criação de *guidelines* para colaboradores. A discussão demonstrou que a maioria dos *registries* ainda se encontra numa fase inicial de definição estratégica, mas já reconhece a necessidade de enquadramento interno claro para utilização segura e responsável destas tecnologias.

Foi igualmente discutido o impacto potencial do AI Act e de futuras iniciativas regulatórias europeias sobre os *registries*, nomeadamente no que respeita à utilização de IA em processos de deteção de DNS Abuse, automação de verificações e apoio à tomada de decisão. Alguns participantes salientaram a importância de equilibrar inovação, eficiência operacional e mitigação de riscos associados à transparência, enviesamento algorítmico e proteção de dados.

A sessão “AmalA – Suspicious Domain Detection System in .es” apresentou a solução desenvolvida pelo *registry* espanhol para deteção de domínios potencialmente abusivos através de técnicas de inteligência artificial. O sistema combina análise comportamental, modelos preditivos e indicadores de risco para identificar registos suspeitos numa fase precoce, permitindo reforçar os mecanismos de prevenção e mitigação de DNS Abuse. A apresentação evidenciou o crescente interesse dos *registries* na utilização de ferramentas de IA para apoiar atividades de monitorização, classificação de risco e resposta a incidentes.

Analytics, Retenção e Crescimento

A sessão “From Metrics to Meaning: Redefining Registrar Engagement Through Analytics”, apresentada por Priyadarshini Tiwari (.IE), demonstrou como a utilização de *analytics* avançado pode contribuir para fortalecer o relacionamento entre *registries* e *registrars*. Foi apresentado um portal desenvolvido em Power BI que disponibiliza métricas de crescimento, retenção, transferências e *benchmarking*, permitindo transformar dados operacionais em informação útil para suporte à tomada de decisão.

A apresentação evidenciou uma tendência crescente entre os *registries* para evoluírem de operadores essencialmente técnicos para parceiros estratégicos dos seus ecossistemas, disponibilizando não apenas infraestruturas críticas, mas também conhecimento analítico e ferramentas de apoio ao negócio.

Na sessão “Nothing is as old as yesterday’s News – The Journey towards Live Data”, Alexander Maryhofer (nic.at) apresentou a evolução da organização para modelos de monitorização e *reporting* baseados em dados em tempo real. Foram discutidos os benefícios operacionais associados à disponibilização de informação permanentemente atualizada, bem como os desafios técnicos relacionados com a integração de múltiplas fontes de dados e a garantia da qualidade da informação disponibilizada.

A sessão “Measurement of DNS Abuse”, apresentada por Michel Hausding (SWITCH), incidiu sobre a importância da medição consistente e comparável dos fenómenos de DNS Abuse. Foram discutidos diferentes indicadores e metodologias de recolha e análise de dados, bem como os desafios associados à harmonização de métricas entre *registries*. A apresentação reforçou a importância de abordagens suportadas por dados para compreender tendências, avaliar medidas de mitigação e apoiar a definição de políticas de prevenção.

A sessão “Renewal Indicators Task Force”, apresentada por Clemens Moritz (nic.at), Sebastian Castro (.IE) e Thyman Wabeke (SIDN), incidiu sobre um estudo colaborativo envolvendo cerca de 40 milhões de domínios distribuídos por vários ccTLDs. O objetivo consistiu em identificar padrões associados à renovação e retenção de domínios, tendo sido concluído que fatores como a antiguidade do domínio e a sua ligação ao mercado local tendem a aumentar significativamente a probabilidade de renovação. A iniciativa destacou-se sobretudo pelo elevado nível de cooperação e *benchmarking* entre *registries* na análise de desafios comuns.

A apresentação da DNS Belgium sobre estratégias de crescimento e retenção demonstrou como a utilização de dados comportamentais pode contribuir para melhorar os resultados em mercados maduros. Foi partilhado um caso prático relacionado com a recuperação de domínios em quarentena, onde a identificação da janela temporal mais adequada para contacto permitiu alcançar resultados positivos em termos de recuperação de registos. A sessão reforçou a importância crescente da retenção e da gestão do ciclo de vida dos clientes como componentes centrais das estratégias de crescimento dos *registries*.

Marketing

A sessão do Working Group de Marketing com o tema “What can registries do for the IDNs they manage – and why IDNs matter for ccTLDs?”, conduzida por Regina Filipová Fuchsová do .eu e Dijana Milutinović

do .rs, referiu que os IDNs são essenciais para a construção de uma Internet multilingue e inclusiva, mas a sua adoção e gestão eficaz variam significativamente entre os ccTLDs. Esta sessão explorou as medidas práticas, políticas e estratégicas que os *registries* podem adotar em conjunto para reforçar os IDNs que gerem, desde a melhoria da implementação técnica e da experiência do utilizador, até ao aumento da sensibilização, da confiança e da adoção. Regina Filipová Fuchsová referiu que todos os anos é lançado o IDNWorldReport.eu, que foi apresentado após o CENTR Jamboree e está disponível [aqui](#). Discutiu-se depois as barreiras à comunicação de IDNs, tendo sido identificadas as seguintes: dificuldade em explicar o domínio, sendo que em português muitas palavras percebem-se na mesma, por exemplo, com ou sem acento; Não é uma prioridade para as marcas, tendo o .br dado o exemplo do Banco Itaú que não usa o IDN. Discutiu-se de seguida o que se pode fazer para melhorar a utilização de IDNs. Dijana Milutinović referiu que promovem os IDNs através de *hackathons* e incentivam a utilização de IDNs como fator de diferenciação em campanhas publicitárias. O .br e o .pt falaram sobre a LusNIC, que pode ser um exemplo para países que falam a mesma língua (ex. Cirílico).

Na parte do tour de *table*, diversos *registries* referiram as suas taxas de crescimento, designadamente: .cat - 4,19%; .hu - 3.2%; .no - 1,05%; .ee - 5.31%; .se: 1,2%; Verisign - 3,7%; .ca - 3,3%; .lv - 2.6%.

Seguiu-se uma sessão com o tema “*Relaunching a TYPO3 website: Agency collaboration & key learnings*”, conduzida por Melanie Schütte do .de, que apresentou perspectivas práticas sobre a seleção de sistemas CMS, a definição de funções e fluxos de trabalho, bem como as vantagens e desvantagens de trabalhar com agências externas. Na imagem que se segue, é possível ver uma comparação entre três possíveis ferramentas:



À pergunta “Porquê escolher o TYPO3?”, a oradora referiu a estabilidade e suporte para arquiteturas complexas e que não se tratava de encontrar uma nova ferramenta, mas sim de manter uma relação de longo prazo com a agência.

***Nota:** O TYPO3 é um sistema de gestão de conteúdos livre. Escrito em PHP e corrido em MySQL, TYPO3 é usado para a criação de sites de porte médio até portais grandes.*

No que diz respeito à *timeline* de desenvolvimento do projeto, iniciou em junho e terminou em dezembro. Em termos de *key learnings*, foram identificados os seguintes: 1) O DNA importa: a estrutura TYPO3 ajudou a poupar tempo; 2) Menos é mais: passaram de 1400 para 100 páginas; 3) Fator humano: o sucesso depende do envolvimento das equipas internas.

Esta sessão foi particularmente relevante para o .PT, tendo em consideração que estamos a realizar os trabalhos preparatórios para o novo website.

A próxima reunião do grupo de Marketing será em conjunto com o grupo de Business Operations & Processes, nos próximos dias 24 e 25 de setembro, em Ljubljana.

Operação e Negócio

A sessão “RDAP – What is it for? Tailormade lookup services at .no”, apresentada por Unni e Marit (.no), demonstrou o potencial do Registration Data Access Protocol (RDAP) como plataforma para disponibilização de serviços de consulta mais flexíveis e personalizados. Foi evidenciado que o RDAP permite efetuar pesquisas estruturadas com base em diferentes critérios, como o nome de domínio, o número de organização ou o número de identificação pessoal, disponibilizando mecanismos avançados de filtragem e automatização através de uma API REST. A apresentação destacou ainda as vantagens desta tecnologia para os *registrars*, nomeadamente o acesso a funcionalidades de pesquisa mais completas e a possibilidade de integração direta nas suas próprias plataformas, reforçando o papel do RDAP como sucessor natural do WHOIS e como ferramenta de modernização dos serviços de consulta de dados de registo. Existe ainda o potencial de criar acessos específicos para polícias e outras entidades competentes com permissões adequadas às suas necessidades, contudo existem diversas questões de *compliance* que teriam de ser acauteladas.

As três apresentações dedicadas à faturação eletrónica proporcionaram uma visão complementar sobre a implementação dos novos requisitos europeus, combinando o enquadramento legal com exemplos práticos de adoção por diferentes *registries*. O SK-NIC (.sk) apresentou a evolução do pacote legislativo VAT in the Digital Age (ViDA) e o respetivo calendário de implementação na União Europeia, destacando igualmente o papel da rede PEPPOL como infraestrutura comum para a troca de documentos eletrónicos. A DNS Belgium (.be) partilhou a sua experiência prática na implementação da faturação eletrónica, evidenciando a importância do planeamento antecipado, da colaboração entre as equipas financeira e tecnológica e da integração com soluções especializadas. Por sua vez, o .PT apresentou o enquadramento nacional e a arquitetura tecnológica adotada para assegurar a conformidade com a legislação portuguesa, demonstrando que dispõe já de uma solução plenamente operacional. Em conjunto, as três apresentações evidenciaram que a faturação eletrónica constitui uma transformação estrutural para os *registries*, exigindo preparação atempada, integração entre sistemas e uma estreita articulação entre as áreas financeira e tecnológica.

Na sessão “New Dashboard in .ES – From MicroStrategy to Power BI”, Alejandro Cañas Nieto (Red.es / Dominios.es) apresentou o processo de modernização da plataforma de *Business Intelligence* do *registry* espanhol, assente na migração do MicroStrategy para o Microsoft Power BI. Foram abordados os desafios associados à migração, à validação dos dados e à racionalização dos *dashboards*, tendo sido reduzido o número de relatórios disponibilizados, sem perda de informação relevante. A apresentação demonstrou igualmente a intenção de alargar a utilização da plataforma a todas as áreas da organização, incluindo operações, segurança, apoio ao utilizador e área jurídica, reforçando a importância da utilização de dados fiáveis e atualizados como suporte à gestão operacional e à tomada de decisão.

A Punktum dk apresentou igualmente a estratégia de comunicação adotada para preparar os *registrars* para a introdução de novos requisitos contratuais e operacionais, decorrentes de uma mudança de paradigma em que todos os registos passarão a ser efetuados via *registrar*. O processo iniciou-se em outubro de 2025 com uma campanha de comunicação dirigida aos *registrars*, imprensa e redes sociais, complementada por sessões presenciais e online. Numa fase posterior, foram promovidos grupos de trabalho e reuniões dedicadas à análise detalhada das alterações ao contrato de *registrar* e dos novos requisitos aplicáveis, permitindo recolher contributos e esclarecer dúvidas antes da sua implementação. A apresentação evidenciou a importância de uma comunicação contínua, transparente e participativa na gestão de alterações com impacto nos parceiros, destacando o papel do envolvimento dos *registrars* como fator crítico para o sucesso da implementação.

Em conjunto, as sessões dedicadas à operação e negócio evidenciaram uma tendência comum entre os *registries* europeus para a modernização dos seus serviços e processos internos, através da adoção de soluções mais automatizadas, interoperáveis e orientadas por dados. Paralelamente, foi reforçada a importância da comunicação estruturada com os *registrars* e do seu envolvimento antecipado na implementação de novos requisitos, como elemento essencial para uma gestão eficaz da mudança. Temas como a evolução dos serviços de consulta de dados de registo, a implementação da faturação eletrónica, a utilização de plataformas avançadas de *Business Intelligence* e o reforço da colaboração com os parceiros demonstram uma crescente aposta na eficiência operacional, na melhoria dos serviços prestados aos *registrars* e na adaptação aos novos requisitos tecnológicos e regulamentares.

Conclusão

O CENTR Jamboree 2026 confirmou a crescente convergência dos desafios enfrentados pelos *registries* europeus, independentemente da sua dimensão ou contexto nacional. Temas como a implementação da NIS2, a mitigação de DNS Abuse, a validação de dados de titulares, a gestão de crises, a conformidade regulatória e a evolução dos modelos de negócio assumiram um papel central nas discussões realizadas ao longo do evento.

A inteligência artificial destacou-se como um dos temas mais relevantes do programa, quer pelo seu potencial para transformar os mecanismos de descoberta de conteúdos e a visibilidade online, quer pelas oportunidades que oferece ao nível da automação, da análise de risco e da deteção de atividades abusivas. Paralelamente, tornou-se evidente a crescente importância dos dados e da capacidade analítica como suporte à tomada de decisão, à retenção de clientes e à melhoria do relacionamento com *registrars* e restantes *stakeholders*.

As várias sessões demonstraram igualmente que a segurança, a resiliência operacional e a capacidade de adaptação a novos requisitos regulatórios continuarão a constituir prioridades estratégicas para os *registries* nos próximos anos. Neste contexto, a colaboração entre organizações, a partilha de experiências e o desenvolvimento de iniciativas conjuntas revelaram-se elementos fundamentais para responder de forma eficaz a desafios cada vez mais complexos e interligados.

A participação do .PT no CENTR Jamboree 2026 permitiu acompanhar estas tendências, reforçar relações com a comunidade internacional de *registries* e contribuir ativamente para a discussão de temas estratégicos para o futuro do ecossistema DNS, consolidando o posicionamento do .PT como um interveniente empenhado na construção de uma Internet mais segura, resiliente e confiável.

O evento voltou a evidenciar a importância da cooperação entre *registries* e o papel do CENTR enquanto plataforma de referência para a partilha de experiências, desenvolvimento de iniciativas conjuntas e discussão dos desafios tecnológicos, operacionais e regulatórios que moldam o futuro do setor.