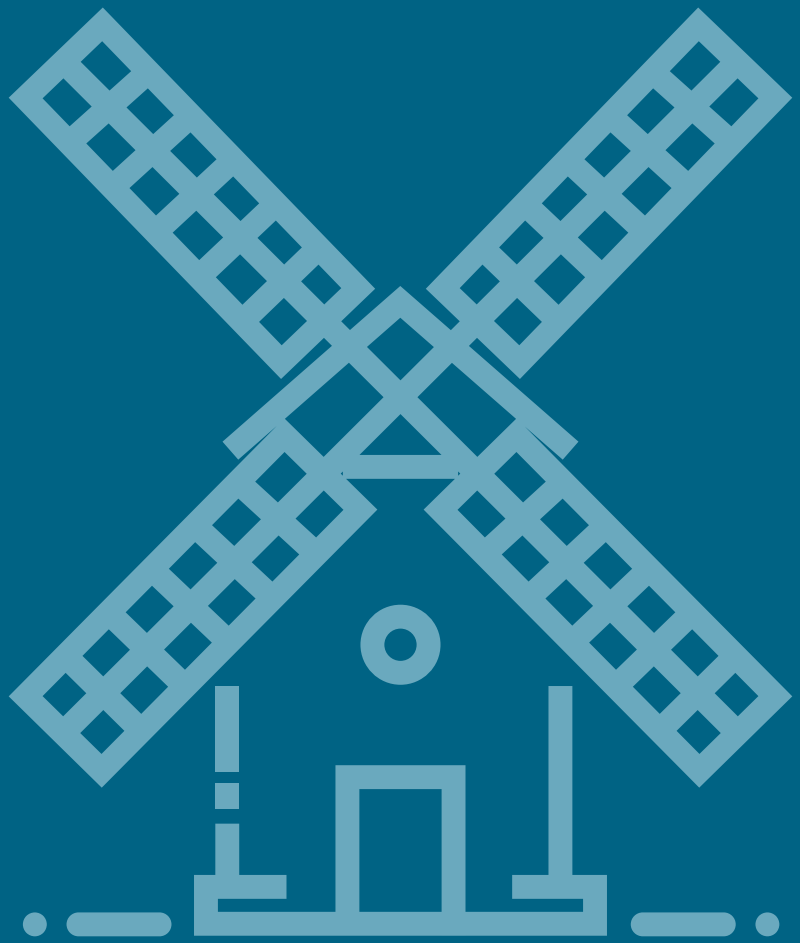
RELATÓRIO CENTR JAMBOREE 2019

27 a 29 de maio, Amesterdão - Holanda

Council of European National
Top-Level Domain Registries

ÍNDICE



INTRODUÇÃO

De 27 a 29 de maio decorreu o CENTR Jamboree 2019, em Amesterdão. Mais de 200 participantes e seis grupos de trabalho – administrativo, I&D, jurídico, marketing, técnico e segurança – reuniram-se para discutir as tendências no mundo dos ccTLD's. O Jamboree é um dos principais eventos do CENTR. Decorre durante três dias e promove a partilha de experiências entre os grupos de trabalho que habitualmente se reúnem de forma independente.

Disponibilizamos, nos pontos que se seguem, algumas das conclusões que destacamos das sessões em que o .PT participou.

O PAPEL DOS REGISTRIES NOS CONTEÚDOS ILEGAIS ONLINE

Não se levantam dúvidas relativamente ao facto dos conteúdos online ilegais diminuírem a confiança na internet como veículo de difusão da informação e plataforma de oportunidades económicas. Nesta medida, e face à importância da sua atividade para o bom funcionamento da rede, os registries têm-se mostrado empenhados em contribuir para uma melhor abordagem a este problema, participando ativamente na busca de uma solução.

A problemática dos conteúdos online ilegais e da sua necessária remoção da internet como forma eficaz de obstar à sua disponibilização na rede reveste-se de particular complexidade pois, se por um lado a determinação de "conteúdo ilegal" está dependente de uma análise casuística e da qualificação conferida pelo ordenado jurídico nacional, por outro lado têm cabimento dentro deste conceito diversos ilícitos, como a venda de bens contrafeitos (*fake shops*) ou disponibilização de conteúdos protegidos por direitos de propriedade intelectual, incumbindo a diferentes entidades poderes de fiscalização e investigação consoante a matéria em apreço (p. ex. órgãos de polícia criminal, tribunais judiciais, centros de arbitragem, autoridade de inspeção, entre outras).

É entendimento comum entre os registries dos ccTLD's europeus que, na qualidade de operadores técnicos do sistema DNS, não lhes cabem competências de fiscalização do conteúdo dos websites associados aos nomes de domínio registados ou de apreciação da legalidade desses mesmos conteúdos. Não obstante, e compreendendo o seu papel neste contexto, os registries europeus têm introduzido mecanismos mais rigorosos de análise da veracidade dos dados disponibilizados pelos registrants que se têm provado verdadeiramente eficazes, uma vez que, por norma, quem regista domínios para fins ilícitos não usa informações pessoais corretas.

Alguns registries europeus têm, inclusivamente, desenvolvido e aplicado novas tecnologias e mecanismos jurídico-administrativos que envolvem uma avaliação sumária aos conteúdos associados aos nomes de domínio registados (.nl e .eu) ou a notificação das autoridades competentes após a identificação de conteúdos ilícitos (.dk).

OS REGISTRIES EUROPEUS COMO PRESTADORES INTERMEDIÁRIOS DE SERVIÇOS DA SOCIEDADE DA INFORMAÇÃO

Relativamente a este tema está em causa a possível consideração dos registries de ccTLD's europeus como prestadores intermediários de serviços da sociedade da informação à luz da Diretiva 200/31/CE, de 8 de junho de 2000, habitualmente designada por Diretiva sobre o comércio eletrónico.

Com o crescente enfoque sobre como lidar com os conteúdos online ilegais, o papel dos prestadores intermediários de serviços da sociedade da informação e a sua responsabilidade em impedir a disponibilização daqueles conteúdos tem adquirido especial relevância, pelo que, e nesta medida, importa perceber se os registries deverão ou poderão ser considerados prestadores intermediários.

Embora não seja claro em que medida a Diretiva exclui a responsabilidade dos registries como prestadores intermediários, provável consequência da sua antiguidade e de alguma desadequação à realidade atual, tem sido interpretação unânime entre os registries europeus que estes não deverão ser assim qualificados, enquadrando a sua atividade na isenção de responsabilidade consagrada no art. 12º da Diretiva, pois face às suas competências técnicas, apenas são responsáveis por facultar o acesso a uma rede de comunicações

("*simples transporte*"), não estando na origem dessa transmissão, não selecionando o destinatário da mesma e não modificando as informações objeto de transmissão, o mesmo será dizer, não sendo responsáveis pelos conteúdos disponibilizados online.

Não obstante, o crescente envolvimento dos registries na eliminação de conteúdos online ilegais da internet através da remoção intencionada dos nomes de domínio correspondentes poderá dificultar a defesa de posição diversa à sua qualificação como prestadores intermediários de serviços da sociedade da informação aquando da próxima revisão legislativa europeia sobre esta matéria.

A EXPERIÊNCIA DOS REGISTRIES EUROPEUS COM O REGULAMENTO (UE) 2017/2394, DE 12 DE DEZEMBRO DE 2017

O Regulamento (UE) 2017/2394, de 12 de dezembro de 2017, relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de proteção dos consumidores, apresenta novos desafios aos registries e seus registrars na medida em que vem reforçar os poderes conferidos às autoridades competentes nacionais, responsáveis pela aplicação da legislação da União Europeia de proteção dos interesses dos consumidores, para agirem sobre os nomes de domínio registados.

Esta nova regulamentação vem admitir diretamente a possibilidade das autoridades competentes poderem solicitar aos prestadores de serviços de internet, operadores de telecomunicações, registos e entidades gestoras de nomes de domínio e prestadores de serviços de alojamento, a prestação de todas as informações que considerem pertinentes à investigação, bem como o poder de ordenar o registo ou a remoção de um nome de domínio podendo, inclusivamente, demandar o registo de um domínio sob a sua titularidade.

É convicção generalizada entre os registries que esta lei pode apresentar-se como uma verdadeira vantagem, particularmente no que respeita ao tratamento dos conteúdos online ilegais, uma vez que existirá uma autoridade que está legalmente habilitada a fiscalizar o conteúdo dos websites e a dar ordem de remoção dos nomes de domínio associados.

Por outro lado, verifica-se que a maioria dos Estados-Membros ainda não legislou internamente sobre esta matéria, nomeadamente especificando como se operará a remoção e o registo de nomes de domínio por ordem da autoridade competente e a favor desta, ou se uma entidade com poderes delegados pela autoridade competente poderá igualmente ordená-lo. Torna-se, pois, urgente a resposta a estas questões considerando que o Regulamento será plenamente eficaz a partir de janeiro de 2020.

LITIGÂNCIA NOS REGISTRIES EUROPEUS

CASO .JP

Recentemente o .jp confrontou-se com um litigio (atípico) sobre um nome de domínio, envolvendo duas partes interessadas que, em simultâneo, mas separadamente, desencadearam os procedimentos legais necessários à remoção e posterior transferência do domínio.

O primeiro processo a ser iniciado foi interposto pelo detentor de um direito de propriedade intelectual anteriormente constituído sobre o nome registado, que pretendia a transferência da sua titularidade, o segundo foi desencadeado pela Autoridade Tributária japonesas que notificou o registry para a execução do domínio para venda judicial e liquidação de uma dívida fiscal do registrant.

Perante a inexistência de um litígio anterior, o registry deveria proceder imediatamente à execução do nome de domínio por ordem da Autoridade Tributária japonesa, porém, no cenário apresentado, e de acordo com a legislação aplicável, o registry não poderá atuar sobre o nome de domínio (p. ex. transferi-lo ou removê-lo) enquanto o processo instaurado pelo legítimo detentor do direito anterior correr os seus termos.

Por ora, o nome de domínio permanece "congelado", não tendo sido executado a favor da Autoridade Tributária, uma vez que o registry considerou que sendo o direito sobre cada nome registado sob. jp determinado pelas Regras de Registo, não existia enquadramento legal que permitisse a imediata venda judicial do nome de domínio. Contudo, a titularidade do domínio também não foi transferida para o detentor do direito de propriedade intelectual, uma vez que ainda não há decisão sobre este litígio.

CASO .NZ

O registry de .nz identificou que uma identidade norte-americana prestadora de serviços de registo e alojamento de nomes de domínio procedia, recorrentemente, à recolha, ao uso e à conservação indevida dos dados pessoais associados a nomes de domínio de .nz disponíveis para consulta através do diretório WhoIs.

A entidade visada procedeu à criação de base de dados paralelas com os dados pessoais recolhidos através do sistema WhoIs, violando as regras de boa utilização desta ferramenta (p. ex. o volume de queries autorizado), e tendo ainda sido possível ao registry confirmar a venda destas bases de dados a diferentes interessados, sem o consentimento dos respetivos titulares dos dados.

O processo judicial está ainda a correr os seus termos num tribunal norte-americano.

QUESTÕES E DISCUSSÕES TÉCNICAS

DNSSEC

Foi adotado recentemente um novo standard para a adoção de DNSSEC, designado de CDS/CDNSKEY, que permite a passagem do DS record diretamente entre a zona do domínio e a zona do TLD usando apenas DNS, sem ser necessário passar pelos sistemas de registo do TLD. O domínio de topo suíço (.ch) já implementou este standard. Para se ter um domínio com DNSSEC neste TLD basta agora adicionar alguns registos à zona após a assinatura da mesma, sendo que posteriormente o TLD pesquisa na zona por este tipo de registos e, caso os mesmos sejam válidos, passa a publicar os registos DS na sua zona de forma a que a cadeia DNSSEC esteja completa.

Também no âmbito do DNSSEC, o .lu demonstrou como conseguiu aumentar substancialmente o número de domínios com DNSSEC na sua zona. Para tal foi necessário adicionar o serviço de DNS autoritativo para domínios .lu ao conjunto de serviços disponibilizados pelo TLD. Assim, os registos de domínios .lu puderam passar a ser feitos através deste novo serviço. Desta forma foi possível adicionar ao serviço de DNS autoritativo, de forma simples e rápida, a assinatura DNSSEC dos domínios provisionados nele, sendo um serviço *out-of-the-box* que qualquer domínio que use este serviço poderá ter.

Foram ainda reportados, por três registries, diversos incidentes com DNSSEC, que ocorreram durante os últimos meses. Estes incidentes estão todos relacionados com as assinaturas geradas e com *bugs* nos softwares que fazem a geração das assinaturas. Foi, assim, mais uma vez levantada a questão de como fazer *upgrades* ao software e de como validar se está tudo ok com o software atualizado. No final as conclusões foram semelhantes: é necessário testar os *upgrades* de diversas formas e ter sistemas de monitorização especialmente treinados para detetar as falhas de forma eficiente.

DNS Hijacking

O tema do DNS Hijacking continua na ordem do dia, já que cada vez existem formas mais criativas de sequestro de tráfego. A Netnod, que opera o *root server* e é também um fornecedor de serviços de secundário de DNS tanto para TLD's como para empresas, deparou-se recentemente com um problema com o seu *root server* que passou pela publicação errada de um *glue record* deste servidor e que levou ao desvio de tráfego legítimo para servidores maliciosos. Este desvio foi feito com o objetivo de conseguir capturar passwords de um site específico, de forma a, futuramente, poder-se impersonificar as pessoas neste site. O problema surgiu principalmente devido ao deficiente funcionamento do sistema de gestão de registos do TLD usado, o .net, que permitia a publicação de registos por um utilizador indevido. Esta situação ficou resolvida removendo o registo malicioso no TLD e corrigindo o software do registry sendo que, para prevenir questões semelhantes, é necessário reforçar os pontos de monitorização. A Netnod pensa ter sido um ataque direcionado, que poderia ter tido consequências bastante maiores.

Foi também discutido o caso de um ataque de *DNS Hijacking* do qual um operador sueco foi alvo e que impactou a atividade de um dos seus clientes. O perpetrador deste ataque, recorrendo a diversas técnicas, conseguiu, de forma silenciosa, modificar os *glue records*, roubar as credenciais de acesso aos sistemas de delegação da zona e, por fim, obter total controlo sobre o domínio, através da redelegação dos NS e alteração dos registos DNSSEC (DS).

Migração de TLD's para Cloud Pública

Um dos temas em destaque tem sido a migração de diversos TLD's de Cloud Privada para sistemas em Cloud Pública, como por exemplo AWS. Até ao momento apenas dois TLD's moveram os seus sistemas de registo para Cloud Pública, no entanto este tema desperta cada vez mais o interesse dos mesmos. Nesta migração, existem, no entanto, questões que ficam por responder, como são exemplo as questões de soberania e de segurança dos dados.

DoH (DNS over HTTPS)

Foi recentemente criado um *standard* que despertou a atenção dos responsáveis pelos motores de busca e que faz com que a resolução de domínios deixe de ser *plain* texto típica e que passe a ser feita por HTTPS, que é um protocolo bastante usado pelos motores de busca. Assim, os responsáveis pelos motores de busca começaram a mover a resolução de nomes do sistema operativo para a própria aplicação, o que tem gerado bastante polémica por diversos motivos, entre eles a falta de controlo por parte do ISP dos *resolvers* usados em DoH e a quebra dos bloqueios de DNS, que são muitas vezes impostos ao nível dos *resolvers* locais mas que são quebrados com o uso de resolvers DoH, que muitas vezes não são *resolvers* locais e não obedecem às ordens de bloqueio da mesma forma.

Deteção de falsas webshops

Websites de lojas falsas ou de produtos contrafeitos são bastante populares, mas podem ser bastante prejudiciais para o TLD em termos de prestígio. Desta forma, e para detetar este tipo de websites, o .be desenvolveu um sistema baseado em várias métricas que estes websites apresentam, de forma a, futuramente, poder tomar medidas contra os mesmos. Este modelo de deteção está ainda em análise, sendo que brevemente haverão mais novidades.

SEGURANÇA

Os projetos mais discutidos neste âmbito foram os relativos à gestão de um sistema de segurança de informação e continuidade de negócio (ISO/IEC 27001 e 22301) e ao esforço de conformidade com a Diretiva NIS.

Além disso, a CIRA (registry do .ca) apresentou um projeto sobre o desenvolvimento de um *home-gateway* seguro, de fácil utilização e configuração para um utilizador comum, que pretende evitar que sejam colocados dipositivos IoT vulneráveis na internet de forma inadvertida.

Foi ainda interessante a partilha, por parte de um elemento da Polícia Holandesa, da operação levada a cabo em 2017, que terminou com a detenção dos elementos por detrás do "Hansa Market", um dos principais mercados negros à data a operar na Darkweb.

Programas de divulgação responsável e de recompensas

Os programas de divulgação responsável e de recompensas são uma tendência em grande crescimento na comunidade de segurança, sendo inclusivamente já adotados por grandes empresas, como a Google, o Facebook e a Microsoft, e também por alguns ccTLD's, como o .nl e o .eu. Estes programas têm por objetivo criar um ambiente de compensação e de reconhecimento para aqueles que detetem e reportem vulnerabilidades nos seus sistemas.

A EURid apresentou o seu programa de divulgação responsável de vulnerabilidades e de recompensas e identificou as diferenças deste tipo de programas em comparação com as convencionais auditorias de segurança técnicas, bem como as vantagens da adoção e os resultados obtidos até ao momento. O registry do .eu mostrou ainda como começou primeiro por adotar um programa de divulgação responsável (PDR) e passou posteriormente a adotar um programa de recompensas, ou mais conhecido por Bug Bounty (PBB). A principal diferença entre estes programas é que nos PDR não existe qualquer recompensa para quem descobrir alguma vulnerabilidade nos sistemas, já nos PBB são entregues recompensas monetárias, tipicamente tendo em conta a criticidade das vulnerabilidades identificadas.

A diversidade de investigadores de segurança envolvidos e o tempo disponível para testarem as plataformas e sistemas leva a que sejam muitas vezes identificadas vulnerabilidades de segurança fora da caixa, que não seriam identificadas nos testes de segurança convencionais.

Guia de Segurança para ccTLD's – Iniciativa do CENTR

As novas exigências legais, nomeadamente a Diretiva NIS, criam responsabilidades acrescidas para os ccTLD's em termos de segurança da informação e obrigam à aplicação das necessárias medidas técnicas e organizativas para fazer face aos riscos (art. 14.º). Esta legislação e os normativos de segurança e de continuidade de negócio são, muitas vezes vagos, não sendo explícitos nas medidas necessárias nem adequados ao ecossistema de um Domínio de Topo.

Neste sentido, o DENIC (registry do .de) apresentou uma proposta para o desenvolvimento conjunto, no âmbito do CENTR, de um guia de requisitos comuns de segurança específicos para o contexto dos ccTLD's. Neste guia propõe que sejam identificadas as ameaças e riscos associados ao ecossistema de um Domínio de Topo e as medidas necessárias para os mitigar e controlar.

A IMPORTÂNCIA DOS DADOS

Um dos temas que esteve em discussão foi a questão dos dados e a forma como os utilizamos. O desafio consistiu em responder a quatro questões: que dados temos; qual o seu valor; que tipo de serviços podemos desenvolver a partir de dados valiosos; e quais os dados que devemos vender ou disponibilizar gratuitamente.

Os registries têm acesso a diferentes tipos de dados: lista de domínios, detalhes dos registrants, informação sobre NameServer, DNSSEC, IPv4/IPv6, dados dos registrars, transações (WHOIS, registos, atualizações, cancelamentos), informações de segurança, contactos de parceiros e de outras entidades, estatísticas, estudos, entre muitos outros.

A utilização e o acesso a estes dados variam dependendo se somos registry, registrar, registrant ou outra entidade. Mesmo em cada um deles, a utilização também varia de acordo com o objetivo e é trabalhada de forma diferente pelas diferentes equipas (marketing, técnica, I&D). Independentemente de quem sejamos e de em que posição nos encontramos, os dados são valiosos e devem ser trabalhados, já que muitas vezes nos permitem detetar necessidades e desenvolver iniciativas, soluções e serviços para responder às mesmas.

Business Intelligence para registrars

O registry francês, AFNIC, apresentou o modelo de Business Intelligence que disponibiliza aos registrars. Ao longo do percurso para chegar a este modelo percebeu que diferentes registrars apresentavam diferentes necessidades, havendo, no entanto, algumas necessidades comuns a todos, e à medida que a dimensão do registrar aumentava as necessidades também aumentavam. Assim, criou um modelo básico de dashboard a que todos os registrars têm acesso, sendo que existem níveis mais avançados mediante um pagamento adicional.

Estudo: domínios pessoais vs domínios empresariais

O nic.at levou a cabo um estudo com o objetivo de perceber se um domínio de uma pessoa singular teria um caminho diferente de um domínio de uma empresa. Este estudo percorreu diversas etapas. Primeiro foi necessário identificar se um domínio era pessoal ou empresarial, sendo que tal estimativa foi obtida com base na listagem dos nomes de domínio registados desde 1984. Esta etapa revelou-se bastante mais complexa do que o previsto, mas, após algumas interações, foi possível chegar à conclusão de que os domínios relacionados com nomes têm uma taxa de remoção ligeiramente inferior à dos restantes domínios, sendo que, a longo prazo, estes domínios poderiam gerar maior rentabilidade do que os restantes.

MARKETING | COMUNICAÇÃO

Novas ideias são sempre bem-vindas e estes fóruns de partilha de experiências permitem às equipas de marketing e comunicação trazer algumas, adaptando-as depois ao seu contexto e mercado.

Tal como o .PT, vários registries realizam campanhas de comunicação em parceria com os seus registrars: é o caso do .nl, .ie e .eu. Para além destas campanhas, são diversas as iniciativas que os registries levam a cabo, dirigidas aos registrars: o .si está a desenvolver uma plataforma de comunicação para registrars; o .lt está a organizar vários eventos para registrars; e o .at tem um programa de fidelização exclusivo para registrars.

Em termos de ferramentas de comunicação, os registries estão cada vez mais a apostar no vídeo, no online e nas redes socias.

Deixamos aqui alguns exemplos:

- **.nl:** campanha de vídeo no Facebook sobre uma nova ferramenta de sugestão de nomes de domínio para os websites dos registrars;
- **.be:** aposta em campanhas de Google Ads e Facebook Ads;
- **.ee:** campanha sobre "como registrar um domínio .ee" dirigida a pessoas singulares; campanha nas redes sociais sobre o seu novo portal de leilões;
- **.ru:** vídeo "Internet for everyone", cujo tema principal é a inclusão, uma história sobre a internet, que não é apenas acessível a todos, mas que também pode tornar a vida melhor e mais gratificante;
- **.co:** campanha no Youtube com um influenciador; produção de vídeos para promover o uso e o registo de domínios sob .co;
- **.pl:** foi para a rua e perguntou às pessoas o que sabem sobre a internet. Os vídeos estão agora disponíveis no Youtube;
- **.cat:** tutoriais em vídeo com testemunhos de registrants de .cat;
- **.lt:** cursos online sobre registo de domínios e desenvolvimento de websites.

O .PT tem também vindo a apostar no online. Para além da presença nas redes sociais – Facebook, Instagram, LinkedIn e Youtube – lançou recentemente um novo website, mais intuitivo, simples e próximo de quem o visita. Além disso, tem também realizado campanhas online, em parceria com os seus registrars. Tutoriais, *webinars* e campanhas online não são alheios ao .PT e estão já a ser planeados.

Integração Marketing/I&D

Este ano, e pela primeira vez, decorreu uma sessão conjunta marketing/I&D com o objetivo de perceber de que forma estas equipas podem trabalhar em conjunto. Para o efeito, alguns registries já com alguma experiência nesta área, apresentaram casos de estudo.

A SIDN (registry do .nl), através da SIDN Labs, realizou um estudo sobre IPv6 e percebeu que a sua reduzida adoção estava a prejudicar o clima de inovação holandês. Este facto levou a SIDN a pensar numa forma de incentivar a adoção de IPv6. Um trabalho conjunto entre as equipas de marketing e de I&D levou ao desenvolvimento de um programa que envolve incentivos financeiros para os registrars de nomes de domínio, no sentido de os levar à adoção de IPv6, e que resultou na adoção por parte de 370 registrars. Este programa poderá ser usado também no âmbito da adoção de DNSSEC, sendo que a SIDN tem já em vista o seu desenvolvimento futuro que envolverá validação DANE e a criação de uma ferramenta de verificação de conformidade de nomes de domínio para registrars. O valor estimado para este programa para 2019 é de 1.7 milhões de euros, uma realidade que sabemos um pouco distante para o .PT, no entanto não nos leva a baixar os braços. Pensaremos em programas mais adaptados à nossa realidade, que nos levem a atingir os nossos objetivos também nesta matéria.

dns.pt
dnssec.pt
facebook.com/dns.pt
pt.linkedin.com/in/dnspt

Produção: junho 2019
Grafismo: dns.pt