



**ICANN**  
ANNUAL GENERAL

**63**

**BARCELONA**

20-25 October 2018



# ÍNDICE

TECH DAY \_\_\_\_\_ **1**

DNSSEC \_\_\_\_\_ **5**





## ICANN 63

20-25 DE OUTUBRO, 2018 – BARCELONA, ESPANHA

Entre 20 e 25 de outubro teve lugar em Barcelona, Espanha, o ICANN 63, fórum que reúne os mais diversos grupos de pessoas com interesse na Governação da Internet e com especial incidência na governação e funcionamento do sistema de DNS, um dos principais pilares para o bom funcionamento da internet global.

Como já é habitual, o .pt acompanhou com elevado interesse os fóruns que decorreram neste evento, com especial destaque para o Tech Day e para o DNSSEC Workshop.



## ICANN 63 EM NÚMEROS



## ICANN 63 - TECH DAY

A abertura do Tech Day pautou-se pela apresentação por parte da CentralNic sobre a utilização de um programa de Big Bounty que tem como finalidade tornar as aplicações públicas mais seguras, atribuindo prémios a quem encontrar bugs ou fragilidades de segurança.

Depois foi a vez do .CAT explicar como tem vindo a usar, desde 2012, a privacidade por defeito para os seus contactos e, por isso, cumpria, desde logo, os requisitos do RGPD, sendo assim um dos primeiros TLD's a ter iniciativas deste género.

De seguida foi apresentado um estudo que demonstra o quão fácil ainda é injetar tráfego nas zonas de DNS e como este problema tem merecido pouca atenção, deixando assim as portas abertas a agentes maliciosos.

O workshop contou ainda com apresentações dedicadas à gestão de rede. Neste âmbito, um dos temas em discussão foi a implementação da tecnologia anycast, nomeadamente sobre como tirar partido desta tecnologia. Sobre este tema a CIRA, registry canadiano, fez um ponto de situação sobre o seu projeto de um gateway de Internet doméstico, que controla o tráfego doméstico malicioso, protegendo a internet no geral. Por fim, foi referida a evolução das firewalls, que deixaram de ser apenas bloqueadores de portas e protocolos e passaram a interpretar o tráfego que a elas chega.



A segunda parte do Tech Day iniciou com o registry australiano, auDA, a apresentar o seu projeto de migração entre sistemas de registos, que decorreu no ano passado e que fez com que o registry migrasse de um fornecedor de aplicação para outro sem qualquer impacto no registry.



De seguida foi a vez do anfitrião, o .ES, fazer uma apresentação sobre a sua infraestrutura. O .ES está integrado no Ministério da Economia espanhol e, para além do registo de nomes de domínio, tem também valências de NREN, fornecendo computação e outros recursos ao Governo e a universidades espanholas.

A apresentação seguinte referiu um projeto que se dedica à construção de um HSM aberto, para que todos, não só possam construir o seu próprio, como verificar se existe alguma característica de espionagem no hardware que têm.

O painel terminou com uma apresentação por parte do registry inglês, a Nominet, sobre como construir uma nuvem de anycast recorrendo a fornecedores cloud, um trabalho que se mostrou difícil no início, mas que a Nominet conseguiu resolver através de uma empresa que recorria a fornecedores e que conseguia criar uma nuvem anycast.

A última sessão do Tech Day iniciou com uma apresentação sobre as atualizações ao protocolo RDAP. De seguida o SSAC do ICANN apresentou mais uma sessão de sensibilização sobre os ataques homográficos com recurso a domínios IDN, uma problemática que continua bastante atual.

Seguiu-se uma apresentação sobre as medições feitas durante o processo de rotação da chave da raiz. A rotação da chave da raiz correu bem no geral, tendo havido apenas quatro registos de problemas, mas que não se consegue perceber se estão diretamente ligados à rotação. Neste momento a

ICANN está a começar a preparar a próxima rotação, sendo que se espera que esta aconteça brevemente.

A última apresentação desta sessão esteve a cargo do registry norueguês, Norid, e focou-se no trabalho que o registry teve que levar a cabo para cumprir as medidas previstas no RGPD, como por exemplo as alterações ao WHOIS por forma a não expor os dados de pessoas singulares titulares de nomes de domínio.



# ICANN | 63 • DNSSEC





## ICANN 63 - DNSSEC

O DNSSEC Workshop iniciou com o habitual ponto de situação sobre a implementação de DNSSEC no mundo. Concluiu-se não ter havido uma evolução significativa face ao último workShop, no entanto há mais dois ccTLD's que tornaram o DNSSEC operacional: .BY e .IT.

De seguida, alguns ccTLDs apresentaram a sua evolução na implementação de DNSSEC. Aqui o .DK e o .DE referiram que a evolução na implementação tem sido constante, quer no número de nomes de domínio assinados quer em termos de validação no país. O .CH demonstrou uma evolução positiva ao nível de domínios assinados e apresentou as mais recentes

atualizações ao sistema de registo de domínios, com a introdução da tecnologia de reconhecimento de CDS. De seguida o .UK apresentou as suas atualizações ao sistema de geração de assinatura, mudando de uma tecnologia HSM closed source para tecnologia BIND. Também o .IT mostrou os sistemas de assinatura que tem usado, apesar de ter tido pouco sucesso ao nível do número de domínios assinados na zona. Sobre este assunto, o .ES referiu que tem ainda alguma dificuldade na implementação de DNSSEC nos domínios que gere. Por fim, foi a vez do .CZ, que apresenta uma das implementações mais completas da Europa, suportando muitos dos algoritmos e tecnologias, como é o caso do CDS. Após este painel, o .BR falou sobre a recente rotação de algoritmo na sua chave KSK, referindo que o processo decorreu sem problemas.



A sessão da manhã terminou um painel dedicado a tecnologias de atualização automática de digest da assinatura e outro dedicado à rotação da chave KSK. No primeiro painel os participantes referiram o sucesso das tecnologias de atualização automática dos registos DS, já que os resultados têm sido bastante positivos. No entanto o registrar GoDaddy apresentou algumas reservas na utilização de tecnologias como estas, visto que fazem bypass ao registrar, não deixando o mesmo controlar esta parte do DNS. No segundo painel foi novamente referido sucesso da rotação da chave KSK, estando já a comunidade a planear a próxima.

A sessão da tarde foi dedicada ao tema da adoção de DANE. Este protocolo de segurança adicional para email, que funciona com a ajuda de DNSSEC, adiciona um certificado na cadeia do DNS. A primeira apresentação referiu que a adoção de DANE, em especial no serviço de email, tem continuado a evoluir favoravelmente e que tem havido um aumento significativo do número de domínios que utilizam esta tecnologia. O .DE apresentou uma penetração lenta face ao tamanho total da zona, sendo que irá trabalhar no sentido de aumentar o número de domínios que utilizam esta tecnologia.

Por último, falou-se do projeto LocalRoot, que tem como objetivo disponibilizar uma cópia local da zona raiz do DNS para reduzir o tráfego para os servidores da raiz. Este projeto tem evoluído com a adição de outras zonas de alto débito e que apresentam poucas alterações, como é o caso da .arpa.





**SAIBA MAIS EM:**

**Relatório CENTR:** <https://centr.org/library/library/external-event/centr-report-on-icann63.html>

**Comunicado do GAC:** <https://gac.icann.org/contentMigrated/icann63-barcelona-communique>



[dns.pt](https://dns.pt)  
[dnssec.pt](https://dnssec.pt)  
[facebook.com/dns.pt](https://facebook.com/dns.pt)  
[pt.linkedin.com/in/dnspt](https://pt.linkedin.com/in/dnspt)

# .pt

