



VERISIGN™



# DOSSIÊ SOBRE A INDÚSTRIA DE DOMÍNIOS NA INTERNET

VOLUME 8 – EDIÇÃO 2 – MAIO DE 2011

## RELATÓRIO DA VERISIGN SOBRE DOMÍNIOS

COMO OPERADOR GLOBAL DE REGISTROS PARA DOMÍNIOS .COM E .NET, A VERISIGN MONITORA A SITUAÇÃO DO SETOR DE NOMES DE DOMÍNIOS COM BASE EM UM SÉRIE DE PESQUISAS ESTATÍSTICAS E ANALÍTICAS. COMO LÍDER NO FORNECIMENTO DE INFRAESTRUTURA DIGITAL PARA A INTERNET, A VERISIGN DISPONIBILIZA ESTE DOSSIÊ A FIM DE DESTACAR PARA OS ANALISTAS DO SETOR, A MÍDIA E AS EMPRESAS AS TENDÊNCIAS MAIS IMPORTANTES DO REGISTRO DE DOMÍNIOS NA INTERNET, INCLUINDO OS PRINCIPAIS INDICADORES DE DESEMPENHO E AS OPORTUNIDADES DE CRESCIMENTO.



**SUMÁRIO EXECUTIVO**

O primeiro trimestre de 2011 encerrou com uma base de mais de 209,8 milhões de nomes de domínios registrados entre todos os Nomes de Domínios de Primeiro Nível (TLDs), um aumento de mais de 4,5 milhões de nomes de domínios, ou 2,2% em comparação com o quarto trimestre de 2010. Houve um aumento de 15,3 milhões, ou 7,9%, em relação ao ano anterior.

A base de Domínios de Primeiro Nível com Códigos de Países (ccTLDs) registrou totalizou 81,7 milhões de domínios, um aumento de 2,1% de um trimestre a outro, e de 5,1% de um ano a outro.<sup>1</sup>

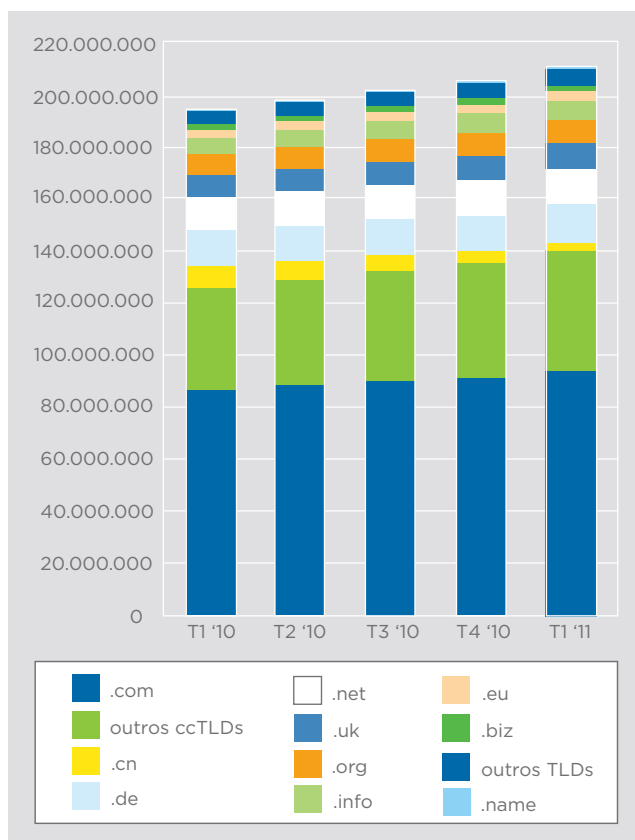
Os TLDs .com e .net apresentaram crescimento absoluto no primeiro trimestre, ultrapassando um total combinado de 108 milhões de nomes de domínios registrados. Novos registros de domínios .com e .net totalizaram 8,3 milhões durante o trimestre. Isso representa um crescimento de 9,2% em novos registros de um ano a outro, e um aumento de 2,7% em relação ao quarto trimestre.

A ordem dos maiores TLDs em termos de tamanho da base mudou em relação ao quarto trimestre, já que o domínio .uk (Reino Unido) passou de quinto para o quarto lugar, derrubando .org da quarta para a quinta posição. Outra mudança foi o declínio do domínio .cn (China), que passou de sétimo para o nono maior, possibilitando o progresso dos domínios .nl (Holanda) e .eu (União Europeia), sendo que cada um destes avançou uma posição, passando a ocupar a oitava e a sétima posição, respectivamente.

Os maiores TLDs em termos de tamanho de base foram, na ordem, .com, .de (Alemanha), .net, .uk, .org, .info, .nl, .eu, .cn e .ru (Rússia).

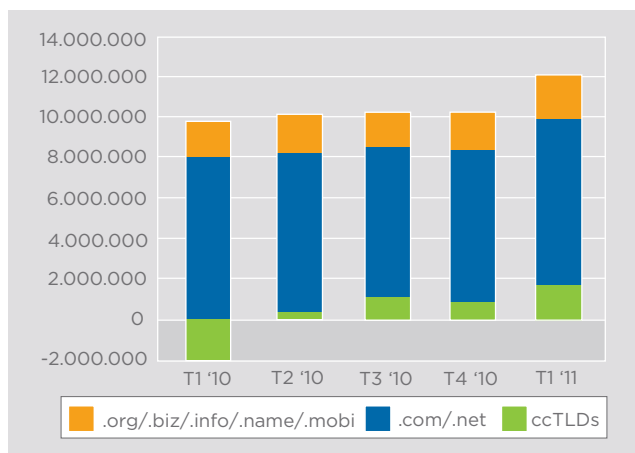
**Total de Domínios Registrados**

Fonte: Zooknic, abril de 2011; Verisign, maio de 2011



**Crescimento de Novos Registros**

Fonte: Zooknic, abril de 2011; Verisign, maio de 2011; Relatórios Mensais da ICANN



<sup>1</sup> Os dados de gTLD e ccTLD mencionados neste relatório são estimativas, no momento deste relatório, e são sujeitos a mudanças ao se receber dados mais completos.

### CLASSIFICAÇÃO DE CCTLDS

O número total de nomes de domínios ccTLD registrados foi de aproximadamente 81,7 milhões no primeiro trimestre de 2011, com um incremento de 1,6 de nomes de domínios, ou um aumento de 2,1%, comparado ao quarto trimestre. Isso representa um aumento de aproximadamente 4,0 milhões de nomes de domínios, ou 5,1%, em comparação com o ano passado.<sup>2</sup>

Entre os 20 maiores ccTLDs, a Holanda, o Brasil, a Itália, a Austrália, a França, os Estados Unidos e o Canadá excederam, cada um, 4% de um trimestre a outro. No último trimestre, quatro dos vinte maiores superaram este patamar.

Os ccTLDs do Canadá e da Austrália foram os únicos, entre os 20 maiores, que superaram o crescimento anual de 20%. No último trimestre, quatro entre estes 20 superaram este patamar.

Há mais de 240 extensões de ccTLDs em todo o mundo, com os dez maiores ccTLDs abrangendo 61% de todos os registros.

#### Principais Operadores de Registro de ccTLD por Base de Nomes de Domínios, Primeiro trimestre de 2011

Fonte: Zooknic, abril de 2011

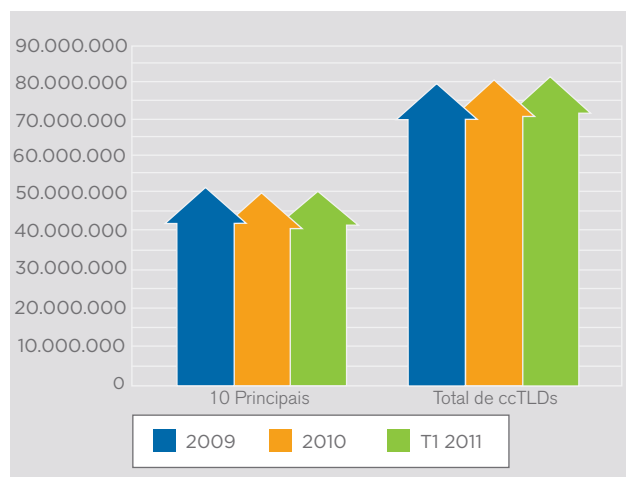
- |                         |                    |
|-------------------------|--------------------|
| 1. .de (Alemanha)       | 6. .ru (Rússia)    |
| 2. .uk (Reino Unido)    | 7. .br (Brasil)    |
| 3. .nl (Holanda)        | 8. .ar (Argentina) |
| 4. .eu (União Europeia) | 9. .it (Itália)    |
| 5. .cn (China)          | 10. .pl (Polónia)  |

### DINÂMICA DE .COM/.NET

A taxa de renovação dos domínios .com/.net do primeiro trimestre de 2011 foi de 73,8%, uma alta em relação aos 72,7% do quarto trimestre. De um trimestre a outro, as taxas de renovação podem variar alguns pontos percentuais em qualquer direção, com base na composição da base “a expirar” e na contribuição de distribuidores autorizados específicos.

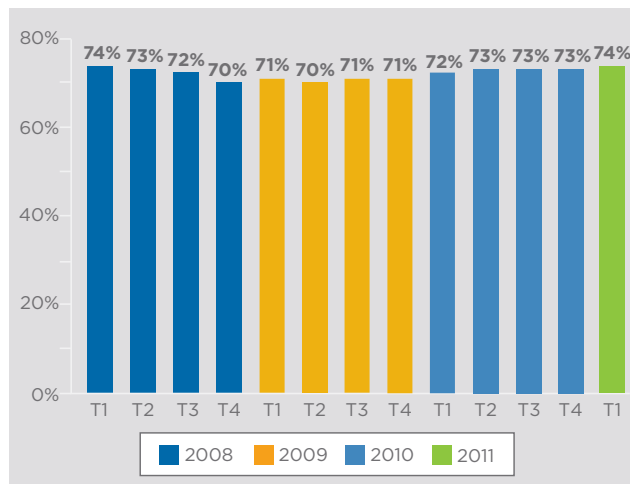
### Classificação de ccTLDs

Fonte: Zooknic, abril de 2011



### Com/.Net - Taxas de Renovação

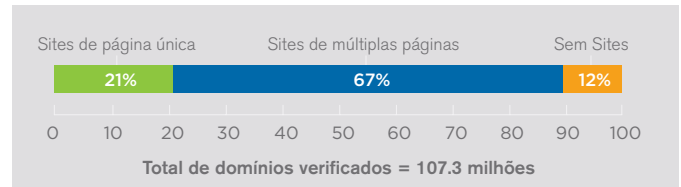
Fonte: Verisign, maio de 2011



2 Alguns sistemas de registro ccTLD ofereceram programas promocionais durante o primeiro trimestre.

## Web sites .Com/.Net

Fonte: Verisign, janeiro de 2011



Um importante fator para as taxas de renovação é se um nome de domínio está ou não associado a um Web site, visto que os nomes de domínios associados a Web sites têm maior probabilidade de serem renovados. A Verisign estima que 88% dos domínios .com e .net estão associados a um Web site. Isso significa que um usuário final que visita tal nome de domínio encontra um Web site. Os Web sites podem ainda ser descritos como de múltiplas páginas ou de página única. Sites de página única incluem páginas em construção, páginas de anúncios e páginas estacionadas, além de páginas estacionadas que geram receita com publicidade on-line.

A média de consultas diárias ao Sistema de Nomes de Domínios da Verisign (DNS) foi de 57 bilhões durante o trimestre, com um pico que chegaram aos 67 bilhões. Comparado ao mesmo período de 2010, a média diária cresceu 6%, e o pico também aumentou na mesma proporção.

O crescimento contínuo das consultas ao DNS é proveniente tanto dos impulsionadores normais de tráfego – mais especialmente, o aumento contínuo no uso global da Internet – quanto dos cada vez mais poderosos ataques de negação de serviço (DDoS) dirigidos contra todas as partes da infraestrutura crítica da Internet. Estes aumentos, consequência de fontes benignas e de fontes mal-intencionadas, exigem inovação e investimentos agressivos por parte dos operadores de infraestrutura, para atender à demanda crescente. Para a Verisign, isso significa a implementação do Projeto Apolo, a qual levará a um crescimento de mil vezes no nível atual de 4 trilhões de consultas para gerenciar 4 quatrilhões de consultas por dia em 2020.

## CRESCENTES AMEAÇAS À NAVEGAÇÃO SÃO DETERMINANTES PARA O SUCESSO DOS NOVOS TLDS

Com todas as expectativas em torno dos Domínios Genéricos de Primeiro Nível (gTLDs) e a expansão do Sistema de Nomes de Domínios (DNS) em escala global, é importante que a comunidade global da Internet não perca de vista as crescentes e reais ameaças cibernéticas que este sistema enfrenta. A defesa bem-sucedida contra estas ameaças será de extrema importância para que se garanta a estabilidade continuada e o crescimento da infraestrutura do DNS.

Durante muitos anos, o DNS tem sido o ponto mais importante numa batalha de alto risco entre os que conduzem ciberataques e os tecnólogos, que são responsáveis por manter a segurança e a estabilidade da infraestrutura. Os combatentes de ambos os lados entendem bem o fato de que o DNS é a fonte de estabilidade da comunicação pela Internet. Caso fique comprometido, toda a Internet estará em risco.

Na última década, a arma escolhida pelos criminosos cibernéticos - a negação de serviços distribuídos (DDoS) - tem se tornado mais comum e produzido efeitos mais destrutivos.

Os ataques DDoS ocorrem quando os agressores utilizam PCs sem proteção que foram “escravizados” por meio de códigos maliciosos para superar um único alvo com o tráfego da Internet. O que torna os ataques tão pífidos é que frequentemente imitam o tráfego normal enquanto sobrecarregam a capacidade dos seus alvos, fazendo com que fiquem off-line. Segundo o Sexto Relatório sobre Segurança da Infraestrutura

Mundial da Arbor Networks (Arbor Networks Worldwide Infrastructure Security Report VI), a Internet testemunhou o primeiro ataque DDoS de 100 gigabits por segundo (gbps), em 2010, superior ao recorde de 10 gbp, em 2005.

Para situar estes dados, vale mencionar que 100 gbps equivalem a 10 vezes a capacidade de qualquer circuito discreto backbone de IP, sendo grande o suficiente para derrubar quase todas as redes no planeta. Este dado não passou despercebido pelos administradores de redes. De fato, [pesquisas sobre a questão de DDoS](#) solicitadas pela Verisign, e realizadas em março de 2011, revelaram que quase três entre cada quatro tomadores de decisões na área de TI que trabalham para empresas que não possuem um plano de solução para o alívio do DDoS planejam fazer a implementação nos próximos 12 meses.

Para tornar a situação ainda pior, os TLDs sempre foram, e sempre serão, tanto alvos quanto meios condutores em potencial para alguns dos ataques cibernéticos mais importantes. Derrubar ou manipular um TLD poderá trazer problemas para milhões de sites, e centenas de milhões de usuários, simultaneamente. Da mesma forma, ataques sobre Domínios de Primeiro Nível com Códigos de Países (ccTLDs) poderiam paralisar países inteiros, sendo, portanto, uma tática perigosa tanto para os ciberterroristas patrocinados pelo Estado como também para outros cibercriminosos.

Esta são as realidades que todos os operadores de registro de TLD - até mesmo aqueles que são novos e de pequeno porte - enfrentam enquanto buscam servir os distribuidores autorizados, usuários finais e consumidores que deles dependem.

### **FORTALECENDO OS PILARES DE DISPONIBILIDADE E INTEGRIDADE**

Entre os três pilares da segurança da informação - confidencialidade, integridade e disponibilidade - o maior foco da comunidade DNS tem sido a questão da integridade, com o uso de DNSSEC pelo mundo. A DNSSEC aborda este problema dos chamados ataques "man in the middle" - nas quais os invasores falsificam dados DNS - permitindo sua autenticação. À medida que

a DNSSEC passa a ser utilizada com mais frequência em toda a Internet, estes tipos de ataque devem diminuir significativamente.

Com a implementação de DNSSEC ao nível do servidor-raiz, e nos principais gTLDs e ccTLDs como, .com, .net, .org e muitos outros, a integridade avança um grande passo. No entanto, embora a integridade seja importante para que o DNS funcione de maneira confiável e sem problemas, outro componente da segurança da informação - a disponibilidade - poderá ser ainda mais fundamental.

Quando uma rede ou TLD se torna indisponível, mesmo por um curto período de tempo, há um efeito de redução, pois quando não responde às solicitações, as portas para a loja ficam fechadas e os consumidores vão a outro lugar. Por este motivo, a preservação da disponibilidade deve sempre ser uma das mais altas prioridades - especialmente para os operadores de TLD. E embora existam muitos problemas que podem causar indisponibilidade da rede, os ataques DDoS são um dos mais significativos e imprevisíveis. A pesquisa DDoS mencionada acima revelou que nove entre dez pessoas entrevistadas (87%) classificaram a proteção DDoS como muito importante para manter a disponibilidade.

Hoje em dia, há muitas medidas conhecidas de combate aos ataques DDoS (limitação de taxas, uso de firewalls e roteamento de black hole, entre outros) que variam em termos de eficácia e eficiência. Muitas vezes, a primeira linha de defesa - particularmente no caso de operadores de TLD, que mal podem comportar o tempo que leva para mitigar um ataque DDoS depois que ele ocorre - é o provisionamento excessivo ou a construção de mais largura de banda e capacidade de lidar com transações, para ajudar a resistir aos picos exponenciais durante um ataque DDoS.

O provisionamento excessivo é necessário, mas, por si só, não representa um programa completo de redução de DDoS. Os operadores de TLD buscarão desenvolver a capacidade de detectar e reduzir rapidamente os ataques na nuvem antes que cheguem às redes em questão.



Com as mudanças extraordinárias e rápidas nos ataques DDoS que estamos vendo hoje em dia, as táticas mais tradicionais de redução de DDoS, como o provisionamento excessivo de largura de banda, assim como o uso de firewalls e sistema de prevenção contra intrusos (IPS) não são mais suficientes para proteger as redes, as aplicações e os serviços. Para muitos operadores de TLD, os serviços de redução de DDoS de terceiros, oferecidos por especialistas, deveriam ajudar a fechar o vão tecnológico ao defender suas redes contra uma variedade cada vez maior de ameaças e desafios.

Uma das formas com que a Verisign trabalha para ajudar os operadores de rede a enfrentar estes desafios é por meio do Verisign DDoS Protection Services (Serviços de Proteção contra DDoS da Verisign). Com base na experiência da empresa na defesa bem-sucedida da sua infraestrutura DNS global contra DDoS e outros tipos de ataques por mais de dez anos, os Serviços de Proteção contra DDoS da Verisign são serviços "agnósticos" de rede hardware baseados na nuvem, para monitoramento e mitigação de DDoS, que detectam e filtram o tráfego mal-intencionado na nuvem para que nunca chegue à rede. Esta abordagem permite que as equipes de TI mantenham a disponibilidade de aplicações on-

line fundamentais, sem a necessidade de grandes investimentos na infraestrutura ou provisionamento excessivo.

Como em tudo que se refere ao lançamento de um novo gTLD, a presença de parceiros fortes na área técnica e um pleno entendimento da situação das ameaças serão muito importantes para se obter êxito e estabilidade neste mercado emergente.

### SAIBA MAIS

Para assinar ou acessar os arquivos contendo os Dossiês Sobre a Indústria de Nomes de Domínios na Internet, visite [www.verisign.com.br/dossiesdominios](http://www.verisign.com.br/dossiesdominios). Envie um e-mail com seus comentários ou dúvidas para [info\\_dominios@verisign.com](mailto:info_dominios@verisign.com).

### SOBRE A VERISIGN

A VeriSign, Inc. (NASDAQ: VRSN) é a fornecedora confiável de serviços de infraestrutura de Internet para o mundo conectado. Bilhões de vezes ao dia, a Verisign ajuda empresas e consumidores de todas as partes do mundo a se comunicar e realizar transações de com segurança. Outras notícias e informações sobre a empresa estão disponíveis no Web site [www.VerisignInc.com](http://www.VerisignInc.com).

#### A Metodologia Zooknic

Para os dados gTLDs cuja fonte é Zooknic, a análise utiliza uma comparação das alterações no arquivo de zona-raiz de nomes de domínios complementada com dados WHOIS em uma amostra estatística dos domínios, que menciona o distribuidor autorizado responsável pelo registro de um determinado nome de domínio e a localização do usuário final. A margem de erro dos dados depende do tamanho da amostra e do tamanho do mercado. Os dados de ccTLD baseiam-se na análise dos arquivos de zona-raiz. Para obter mais informações, acesse [www.zooknic.com](http://www.zooknic.com).

## VerisignInc.com

©2011 VeriSign, Inc. Todos os direitos reservados. VERISIGN, o logotipo da VERISIGN e outras marcas comerciais, marcas de serviço e design são marcas comerciais registradas ou não registradas da VeriSign, Inc. e suas subsidiárias nos Estados Unidos e em outros países. Todas as outras marcas comerciais são a propriedades de seus respectivos titulares.

As declarações contidas neste anúncio que não constituam dados e informações históricos constituem declarações projetadas com significado incluso na Seção 27A do "Securities Act" de 1933 e Seção 21E do "Securities Exchange Act" de 1934. Essas declarações envolvem riscos e incertezas que podem fazer com que os resultados reais da VeriSign sejam materialmente diferentes daqueles declarados ou implícitos em tais declarações projetadas. Os riscos e incertezas potenciais incluem, entre outros, a incerteza de rendimentos e lucratividade futuros, flutuações em potencial dos resultados operacionais trimestrais em função de fatores como aumento da concorrência e pressões de precificação de serviços concorrentes, oferecidos a preços abaixo de nossos preços, e aceitação pelo mercado de nossos serviços já existentes, incapacidade da VeriSign de desenvolver com sucesso e comercializar novos serviços e a incerteza sobre se os novos serviços fornecidos pela VeriSign terão aceitação do mercado ou resultarão em novas receitas. Mais informações sobre fatores potenciais que podem afetar os negócios da empresa e seus resultados financeiros estão nos arquivos da VeriSign na Comissão de Valores Mobiliários, que incluem o Relatório Anual da empresa no Formulário 10-K para o exercício findo em 31.12.10, os relatórios trimestrais no Formulário 10-Q e os relatórios atuais no Formulário 8-K. A VeriSign não se responsabiliza pela atualização de qualquer declaração projetada após a data deste comunicado.