



VERISIGN™



RESUMEN DE LA INDUSTRIA DE NOMBRES DE DOMINIO EN INTERNET

VOLUMEN 8 – NÚMERO 2 – MAYO DE 2011

INFORME DE VERISIGN SOBRE DOMINIOS

COMO OPERADOR DE REGISTRO GLOBAL PARA .COM Y .NET, VERISIGN SUPERVISA EL ESTADO DE LA INDUSTRIA DE NOMBRES DE DOMINIO A TRAVÉS DE DIVERSAS INVESTIGACIONES ESTADÍSTICAS Y ANALÍTICAS. COMO LÍDER EN EL SUMINISTRO DE INFRAESTRUCTURA DIGITAL PARA INTERNET, VERISIGN PROPORCIONA ESTE RESUMEN DE INFORMACIÓN PARA DESTACAR A LOS ANALISTAS DE LA INDUSTRIA, LOS MEDIOS Y LAS EMPRESAS SOBRE IMPORTANTES TENDENCIAS EN LOS NOMBRES DE DOMINIO REGISTRADOS, INCLUYENDO INDICADORES DE DESEMPEÑO Y LAS OPORTUNIDADES DE CRECIMIENTO.

RESUMEN EJECUTIVO

El primer trimestre de 2011 finalizó con una base de más de 209,8 millones de nombres de dominio registrados entre todos los Dominios de Primer Nivel (TLD), lo que representa un aumento de 4,5 millones de nombres de dominio, o del 2,2% con respecto al cuarto trimestre de 2010. Los registros crecieron en 15,3 millones, o el 7,9%, con respecto al año anterior.

La base de Dominios de Primer Nivel con Códigos de Países (ccTLD) fue de 81,7 millones de nombres de dominio, lo que constituye un aumento del 2,1% trimestre tras trimestre y del 5,1% año tras año.¹

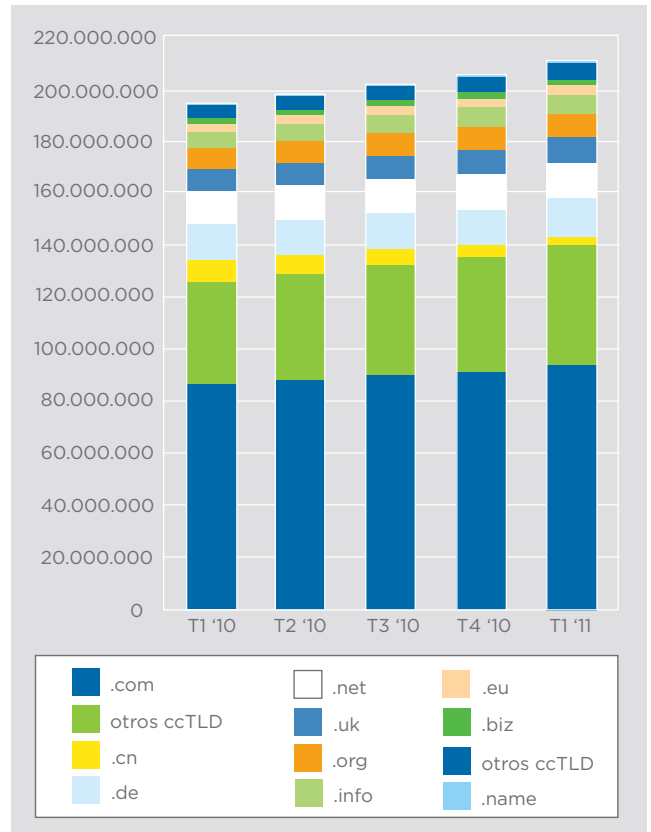
Los TLD .com y .net experimentaron un crecimiento agregado en el tercer trimestre, superando un total combinado de 108 millones de nombres de dominio registrados. Los nuevos registros de dominio .com y .net sumaron 8,3 millones durante el trimestre. Esto representa un crecimiento del 9,2% año tras año en cuanto a nuevos registros, y un aumento del 2,7% con respecto al cuarto trimestre.

El orden de los TLD más importantes en términos del tamaño de su base cambió en comparación con el cuarto trimestre, ya que .uk (Reino Unido) pasó del quinto al cuarto puesto entre los TLD más grandes, desplazando al dominio .org del cuarto al quinto lugar. Además, .cn (China) cayó del séptimo al noveno puesto, lo que permitió que tanto .nl (Países Bajos) y .eu (Unión Europea) avanzaran un puesto para ocupar el séptimo y el octavo lugar, respectivamente.

Los TLD más grandes en cuanto al tamaño de su base fueron, en orden decreciente, .com, .de (Alemania), .net, .uk, .org, .cn, .info, .nl (Países Bajos), .eu (Unión Europea) y .ru (Rusia).

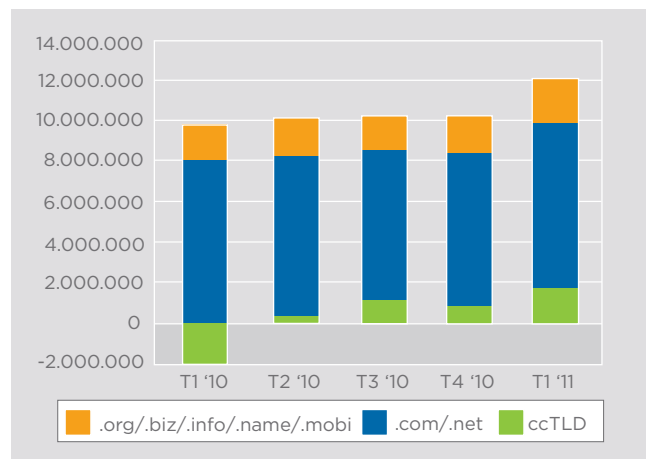
Total de Nombres de Dominio Registrados

Fuente: Zooknic, abril de 2011; Verisign, mayo de 2011



Crecimiento de Nuevos Registros

Fuente: Zooknic, abril de 2011; Verisign, mayo de 2011; Informes mensuales de ICANN



¹ Los datos acerca de gTLD y ccTLD mencionados en este informe son estimativos hasta la fecha del presente documento y pueden sufrir alteraciones a medida que se reciban datos más completos.

CLASIFICACIÓN DE LOS CCTLD

En total, los registros de ccTLD fueron aproximadamente 81,7 millones en el primer trimestre de 2011, con el agregado de 1,6 millones de nombres de dominio, o un aumento del 2,1% en comparación con el cuarto trimestre. Esto representa un aumento de casi 4 millones de dominios, o del 5,1% con respecto al año anterior.²

Entre los 20 primeros ccTLD, tanto los Países Bajos, como Brasil, Italia, Australia, Francia, los Estados Unidos y Canadá tuvieron un crecimiento superior al 4% trimestre tras trimestre. En el último trimestre, cuatro de los 20 dominios más importantes alcanzaron esa cifra.

Australia y Canadá fueron los únicos 20 ccTLD más importantes cuales tuvieron un crecimiento superior al 20% año tras año. En el último trimestre, cuatro de los 20 dominios más importantes alcanzaron esa cifra.

Existen más de 240 extensiones de ccTLD en el mundo, pero los 10 primeros ccTLD representan el 60% de todos los registros.

Principales Operadores de Registro de ccTLD por Base de Nombres de Dominio, primer trimestre de 2011

Fuente: Fuente: Zooknic, abril de 2011

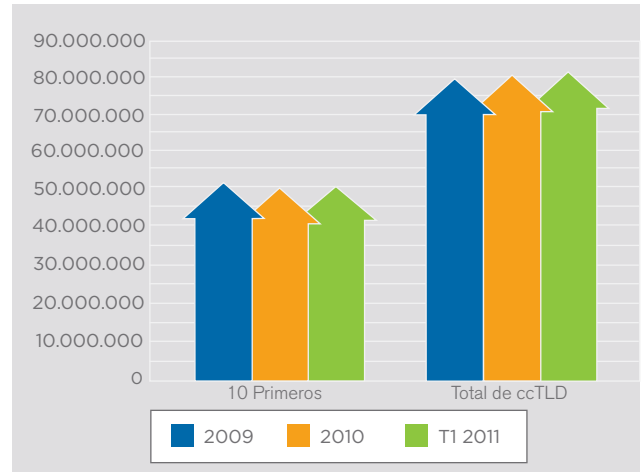
- | | |
|------------------------|--------------------------|
| 1. .de (Alemania) | 6. .ru (Federación Rusa) |
| 2. .uk (Reino Unido) | 7. .br (Brasil) |
| 3. .nl (Países Bajos) | 8. .ar (Argentina) |
| 4. .eu (Unión Europea) | 9. .it (Italia) |
| 5. .cn (China) | 10. .pl (Polonia) |

DINÁMICA DE .COM/.NET

La tasa de renovación de .com/.net para el primer trimestre fue del 73,8%, en comparación con el 72,7% del cuarto trimestre. Las tasas de renovación trimestre tras trimestre pueden tener una variación de unos pocos puntos porcentuales en cualquier sentido, basada en la composición de la base en vías de expirar y en la contribución de distribuidores autorizados específicos.

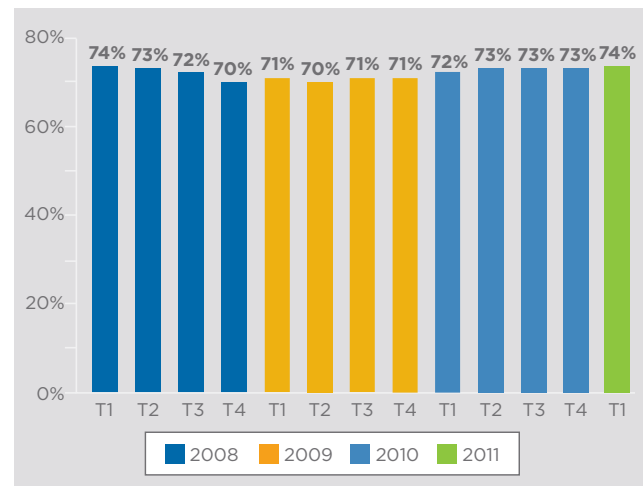
Clasificación de ccTLD

Fuente: Fuente: Zooknic, abril de 2011



.com/.net - Tasas de Renovación

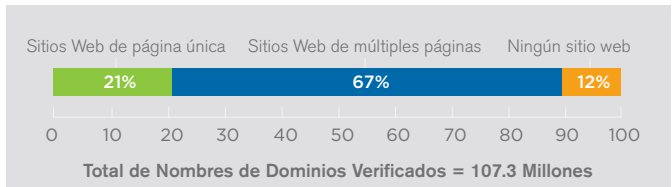
Fuente: Verisign, mayo de 2011



² Algunos registros de ccTLD realizaron programas de promoción durante el primer trimestre.

Sitios .Com/.Net

Fuente: Verisign, enero de 2011



El hecho de que un nombre de dominio esté o no asociado a un sitio Web es un factor clave para las tasas de renovación, pues los nombres de dominio asociados a sitios Web tienen una mayor probabilidad de renovación. Verisign estima que el 88% de los nombres de dominio .com y .net están asociados a un sitio Web, lo que quiere decir que un usuario final que busca este nombre de dominio encontrará un sitio Web. Estos sitios Web pueden ser descritos como de múltiples páginas o de página única. Los sitios de página única incluyen sitios en construcción, páginas de anuncios y páginas estacionadas, además de las páginas estacionadas que generan ingresos a partir de la publicidad en línea.

El promedio de consultas diarias al Sistema de Nombres de Dominio (DNS) de Verisign durante el trimestre fue de 57 mil millones, con un pico de hasta 67 mil millones. En comparación con el mismo período de tiempo en 2010, tanto el promedio diario y como el pico crecieron un 6%.

El crecimiento continuo de consultas al DNS proviene tanto de los generadores de tráfico normales (más notablemente el crecimiento continuo del uso de Internet en todo el mundo) como de los ataques distribuidos de denegación de servicio (DDoS), cada vez más potentes y frecuentes, que se efectúan contra la infraestructura crítica de Internet. Estos aumentos, tanto provenientes de fuentes benignas como de fuentes maliciosas, requieren de una innovación y una inversión agresiva en la parte de los operadores de la infraestructura para satisfacer esta demanda creciente. Para Verisign, esto hace referencia al Proyecto Apollo, el cual permitirá aumentar 1000 veces la capacidad del nivel actual de 4 billones de consultas, para pasar a gestionar 4 trillones de consultas diarias para el año 2020.

LAS AMENAZAS CRECIENTES A LA NAVEGACIÓN POR INTERNET SON CLAVE PARA EL ÉXITO DE LOS NUEVOS TLD

A pesar de todo el entusiasmo que rodea a los nuevos Dominios Genéricos de Primer Nivel (gTLD) y de la expansión del Sistema de Nombres de Dominio (DNS), es importante que la comunidad global de Internet no pierda de vista las amenazas cibernéticas concretas y crecientes a las que se enfrenta ese sistema. Defenderse con éxito de esas amenazas será fundamental para asegurar la continuidad de la estabilidad y el crecimiento de la infraestructura del DNS.

Durante muchos años, el DNS ha sido el epicentro de una batalla en la que hay mucho en juego entre los saboteadores cibernéticos y los tecnólogos responsables de mantener la seguridad y la estabilidad de la infraestructura. Los combatientes de ambos bandos comprenden demasiado bien que el DNS es el eje de la comunicación por Internet. Si éste se ve comprometido, toda la Internet está en riesgo.

En la última década, el uso del arma favorita de los delincuentes informáticos (los ataques de denegación de servicio distribuido (DDoS)) ha aumentado tanto en frecuencia como en carga útil destructiva.

Los ataques DDoS suceden cuando los agresores utilizan PCs sin protección que han "esclavizado" usando un código malicioso para sobrecargar un objetivo con tráfico de Internet. Lo que hace que estos ataques sean tan insidiosos es que a menudo imitan el tráfico normal mientras sobrecargan la capacidad de sus víctimas, dejándolos efectivamente offline. De acuerdo con el Sexto informe anual sobre seguridad de la infraestructura a nivel mundial de Arbor Networks, la

Internet ha sido testigo del primer ataque DDoS de 100 gigabit-por-segundo (gbps) en 2010, muy superior al récord de 10 gbps establecido en 2005.

Para poner esa cifra en perspectiva, cabe decir que 100 gbps equivalen a 10 veces la capacidad de cualquier circuito discreto de red troncal IP, y es lo suficientemente grande como para abrumar a casi todas las redes del planeta, a excepción de unas pocas. Esta cifra no ha pasado desapercibida para los administradores de redes. [La investigación sobre los DDoS](#) encargada por Verisign y realizada en marzo de 2011 descubrió que casi tres de cada cuatro responsables de tomar decisiones en materia de TI que trabajan para empresas que no cuentan con una solución para disminuir los DDoS, planean implementar una en los próximos 12 meses.

Para empeorar las cosas, los TLD siempre han sido (y siempre serán) tanto víctimas como posibles canales de algunos de los ataques informáticos más graves. Hacer caer o manipular un TLD puede causar estragos en millones de sitios y cientos de millones de usuarios en el acto. Y los ataques a ciertos TLD con Códigos de países pueden paralizar a naciones enteras, y constituyen una táctica peligrosa empleada tanto por terroristas informáticos con auspicio estatal como para otros delincuentes informáticos.

Éstas son las realidades con las que deben lidiar todos los operadores de TLD (incluso aquellos que son pequeños y nuevos) al trabajar para brindar servicios a distribuidores autorizados, usuarios finales que registran el nombre de dominio y consumidores que confían en ellos.

FORTALECER LOS PILARES DE LA DISPONIBILIDAD Y LA INTEGRIDAD

De los tres pilares de la seguridad de la información (confidencialidad, integridad y disponibilidad), en los últimos tiempos la atención de la comunidad del DNS estuvo centrada fundamentalmente en la integridad, con la implementación de las DNSSEC en todo el mundo. Las DNSSEC tratan el problema de los ataques denominados “man-in-the-middle” (mediante los cuales los atacantes falsifican datos del DNS) permitiendo la autenticación de esos datos. A medida que las

DNSSEC se implementen más ampliamente en toda la Internet, estos tipos de ataques deberían disminuir significativamente.

A través de la implementación de las DNSSEC al nivel del servidor raíz y en los principales gTLD y ccTLD, tales como .com, .net, .org y muchos otros, la integridad del DNS ha dado un gran paso hacia delante. Pero si bien la integridad es muy importante para que el DNS funcione sin problemas y de forma confiable, otro pilar (la disponibilidad) quizás sea aún más fundamental.

Cuando una red o TLD no están disponibles (incluso por poco tiempo), esto puede tener un efecto en cadena, porque cuando no responde a las consultas, las puertas de la tienda se cierran y los consumidores podrían irse a cualquier otro sitio. Por este motivo, la disponibilidad siempre debe ser una de las máximas prioridades; en especial para los operadores de TLD. Y, si bien existen muchos problemas que pueden causar la indisponibilidad de una red, los ataques DDoS se encuentran entre los más significativos e impredecibles. La investigación sobre los DDoS citada más arriba descubrió que casi nueve de cada 10 personas encuestadas (el 87 por ciento) calificaron a la protección contra los DDoS como muy importante para mantener la disponibilidad.

Actualmente, se conocen muchas medidas para contrarrestar los ataques DDoS (limitación de la tasa, firewalls, enrutadores “agujero negro”, etc.) que varían en cuanto a su efectividad y eficiencia. A menudo, la primera línea de defensa (en particular para los operadores TLD, quienes apenas pueden costear el tiempo que toma atenuar el impacto de un ataque DDoS antes de que éste suceda) es el “over-provisioning” (sobreabastecimiento), o generar más capacidad de ancho de banda y de gestión de transacciones de la red para ayudar a resistir los exponenciales picos de volumen que se experimentan durante un ataque DDoS.

El “over-provisioning” es necesario, pero en sí mismo no representa un programa completo de atenuación de los DDoS. Lo ideal sería que los operadores de TLD buscaran desarrollar la capacidad de detectar y reducir rápidamente los ataques en la nube antes de que estos lleguen a sus redes.



Con los cambios extraordinarios y veloces que estamos viendo hoy en los ataques DDoS, las tácticas de atenuación de DDoS tradicionales, como el “over-provisioning” de ancho de banda, los firewalls y el sistema de prevención de intrusos (IPS) ya no alcanzan para proteger a las redes, las aplicaciones y los servicios. En el caso de muchos operadores de TLD, contratar servicios de atenuación de DDoS provistos por expertos especialistas debería ayudarles a sortear la brecha tecnológica permitiéndoles defender a sus redes de una serie cada vez más vasta de amenazas y desafíos.

Una de las formas en las que Verisign está trabajando para ayudar a los operadores de redes a afrontar estos desafíos es a través del Verisign DDoS Protection Services (Servicios de protección contra los DDoS de Verisign). Estos servicios de protección se desarrollaron a partir de la experiencia de la empresa en cuanto a la defensa exitosa de su infraestructura de DNS global contra los DDoS y otros tipos de ataques por más de una década, y son servicios independientes de monitoreo y atenuación de DDoS basado en la nube e independientes de la red y el hardware, que detectan y filtran el tráfico malicioso en la nube, para que éste nunca llegue a la red. Este enfoque permite que los equipos de TI mantengan la disponibilidad de servicios

y aplicaciones en línea fundamentales, sin necesidad de grandes inversiones en infraestructura u “over-provisioning”.

Al igual que lo que sucede con todo lo asociado al lanzamiento de un nuevo gTLD, para alcanzar el Éxito y mantener la estabilidad en el mercado emergente, resulta fundamental contar con buenos socios en materia técnica y con una firme comprensión de la diversidad de amenazas existentes en la actualidad.

CONOZCA MÁS

Para suscribirse o acceder a los archivos del Resumen de la Industria de Nombres de Dominio en Internet, ingrese a www.verisigninc.com/resumenes. Envíe sus comentarios o preguntas por correo electrónico a info_dominios@Verisign.com.

ACERCA DE VERISIGN

Verisign, Inc. (NASDAQ: VRSN) es el proveedor confiable de servicios de infraestructura de Internet para el mundo en red. Miles de millones de veces al día, Verisign ayuda a las empresas y a los consumidores de todo el mundo a comunicarse y conducir sus negocios con confianza. Para obtener más información y noticias sobre la compañía, por favor visite www.VerisignInc.com.

Metodología Zooknic

Para los datos gTLD cuya fuente es Zooknic, el análisis utiliza una comparación de las alteraciones en el archivo de la zona raíz de nombres de dominio complementada con datos WHOIS en una muestra estadística de nombres de dominio que menciona el distribuidor responsable por el registro de un determinado nombre de dominio y la ubicación del usuario final que lo registró. Los datos tienen un margen de error basado en el tamaño de la muestra y el tamaño del mercado. Los datos sobre ccTLD se basan en el análisis de los archivos de la zona raíz. Para más información, visite www.zooknic.com.

VerisignInc.com

©2011 Verisign, Inc. Todos los derechos reservados. VERISIGN, el logotipo de VERISIGN y otras marcas comerciales, marcas de servicio y diseños son marcas comerciales registradas o sin registrar de Verisign, Inc. y sus filiales en los Estados Unidos y en países extranjeros. Todas las demás marcas comerciales pertenecen a sus respectivos propietarios.

Las declaraciones incluidas en este anuncio, y siempre que no sean de tipo histórico o informativo, constituyen declaraciones de previsiones, tal y como se contempla en la Sección 27A de la Ley sobre Valores “Securities Act” de 1933 y en la sección 21E de la Ley de Intercambio de Valores denominada “Securities Exchange Act” de 1934 con sus modificaciones. Estas declaraciones suponen la existencia de dificultades e incertidumbres que podrían causar que los resultados reales de Verisign difieran materialmente de los indicados o implicados en dichas declaraciones de previsiones. Los riesgos e incertidumbres potenciales incluyen, entre otros, la incertidumbre sobre los ingresos y la rentabilidad futuros y las posibles fluctuaciones de los resultados trimestrales, debido a factores tales como el incremento de la competencia, la presión sobre los precios ejercida por servicios ofrecidos por nuestros competidores disponibles a precios menores que los nuestros y los cambios en las prácticas de marketing incluidas aquellas de terceros distribuidores autorizados; la lenta recuperación de la economía; los desafíos a la continua privatización de la administración de Internet; el resultado de desafíos legales o de otro tipo que resulten de nuestras actividades o de las actividades de distribuidores autorizados y usuarios finales; leyes y regulaciones gubernamentales nuevas o vigentes; cambios en la conducta de los clientes; la incapacidad de Verisign para desarrollar y comercializar exitosamente nuevos servicios; la incertidumbre sobre si los nuevos servicios que brinda Verisign lograrán aceptación en el mercado o generarán ingresos; interrupciones en el sistema; las violaciones a la seguridad, los ataques de hackers, virus o actos de vandalismo intencionales en Internet; la incertidumbre acerca de los costos y la duración de servicios transitorios y solicitudes de indemnización relacionadas con las ventas de activos; y la incertidumbre sobre si el Proyecto Apollo logrará sus objetivos establecidos. Más información acerca de los posibles factores que puedan afectar el negocio y los resultados financieros de la empresa se encuentra en la presentación de Verisign ante la Comisión de Valores e Intercambio, que incluye el Informe Anual de la empresa en el Formulario 10-K para el año que terminó el 31 de diciembre de 2010, los informes trimestrales en el Formulario 10-Q y los informes actuales en el Formulario 8-K. Verisign no asume la obligación de actualizar ninguna de las declaraciones proyectadas después de la fecha de este comunicado.