SERVICIOS DE CONSULTORÍA RELACIONADO CON EL DOMINIO .CO

Autores:

Jim Prendergast

Michael Palage

Antonio García Zaballos

Olga Cavalli

Mayo 2019

Indice general

1. Parte 1 (Ref: 2.2.1):

Identificar las principales tendencias internacionales y potenciales futuros cambios del mercado de nombres de dominio en el nivel superior -TLD-; haciendo énfasis en aquellos relacionados con los códigos de país a nivel global y en la región de Latinoamérica y el Caribe

1.1. Análisis de internet en la región latinoamericana y comparativa en el ámbito global

Consideraciones generales

Hay alrededor de 4.156 millones de usuarios de Internet en todo el mundo, lo que representa alrededor del 54% de la población mundial. La región de América Latina tiene una mayor penetración que el promedio mundial, con aproximadamente 440 millones de usuarios de Internet. La región aún muestra problemas relacionados con la calidad del acceso al servicio de Internet.

El impacto de los servicios móviles ha influido en la penetración de Internet y se vuelve relevante para evaluar este impacto. Ha habido un rápido crecimiento en los servicios de banda ancha móvil con suscripciones de banda ancha móvil en todo el mundo que superan 50 por cada 100 habitantes.

Hay dos factores principales que tienen un impacto en la conectividad internacional entre América Latina y América del Norte, uno son los cables submarinos que conectan ambas regiones, el otro son los puntos de intercambio de tráfico de Internet (IXP) que tienen un impacto en la calidad del servicio, la latencia, precios y disponibilidad a nivel local.

La transición de IPV6 evoluciona a una velocidad menor a la esperada, existen asimetrías entre los países de la región y también en comparación con las economías desarrolladas.

Existe una creciente interconexión de redes a través de los puntos de intercambio de intercambio de tráfico de Internet (IXP) que también desempeñan un papel relevante en la reducción de los precios finales de las tarifas de acceso a Internet, promoviendo las conexiones entre pares y el intercambio de contenido a nivel local. Al mismo tiempo, los Content Delivery Networks (CDN) entregan contenido directamente a los IXP, evitando el tránsito a través de redes ya instaladas.

Existen nuevas regulaciones nacionales impulsadas por el posible impacto de la ciberseguridad y la privacidad en la economía nacional. Las regulaciones y leyes a nivel nacional pueden tener un impacto global dado la conectividad de Internet más allá de las fronteras de los países. DNSSEC proporciona una manera de evitar algunos de los problemas de seguridad relacionados con el Sistema de nombres de Dominio, agregando seguridad al permitir que el navegador web verifique la información del DNS y confirme que no ha sido alterada. El Informe de ICANN sobre DNS en América Latina destaca el hecho de que solo Brasil en .br tiene más del 25% de sus dominios bajo administración con DNSSEC habilitado y México con .mx tiene un 5%. Parece haber una falta de demanda de este servicio o falta de conocimiento de los beneficios positivos para la seguridad relacionados con su uso.

Los informes recientes emitidos por la industria del dominio de Internet indican que el mercado global de dominios se estima en 348 millones en todos los TLD registrados. El número de dominios registrados crece cada año a un ritmo más lento. El informe de estadísticas de CENTR indica que a partir de enero de 2019, se ha registrado la tasa interanual más baja del 3,7%.

Hubo aproximadamente 154.3 millones de registros de nombres de dominio ccTLD al final del cuarto trimestre de 2018, con un aumento de aproximadamente 5.0 millones de registros de nombres de dominio, o 3.4 por ciento, en comparación con el tercer trimestre de 2018.

Las estadísticas de LACTLD y ICANN muestran una tasa de crecimiento de un promedio del 6% desde 2010, que está relativamente cerca del crecimiento global del dominio del 8%. En el caso de .co, se ha observado un aumento mayor de los registros de dominio en función de una estrategia comercial y de marketing diferente. Existen variadas modalidades de administración de los ccTLD regionales, muchas de ellas que no tienen carácter comercial.

Convertirse en un registrador acreditado en América Latina y el Caribe no es una tarea fácil, y algunos de ellos tampoco son sostenibles en el tiempo. El número de registradores acreditados por ICANN en la región está disminuyendo cada año.

El impacto del proceso de nuevos gTLD fue muy bajo en América Latina y el Caribe. Solo hubo 24 solicitudes de nuevos gTLD entre más de 1900 en todo el mundo. Dentro de las 24 solicitudes, ocho eran marcas de TLD, dos geográficas y el resto eran generales.

Se estima que existen unos 28,000 IDN asociados con la región, registrados en en el segundo nivel de ccTLDs.

1.1.1. Internet en el mundo y en la región de América Latina y el Caribe.

Hay alrededor de 4.156 millones de usuarios de Internet en todo el mundo, lo que representa alrededor del 54% de la población mundial. En los países en desarrollo, todavía hay espacio para el crecimiento, con el 45% de las personas que utilizan Internet. En los 47 países menos adelantados (PMA) del mundo, cuatro de cada cinco personas (80%) todavía no utilizan Internet.[1]

La región latinoamericana tiene una mayor penetración que la mundial. La región tiene una penetración promedio de Internet del 67%, con aproximadamente 440 millones de usuarios de Internet. La mayor penetración de Internet por país se muestra en el siguiente gráfico, con Ecuador (81%), Argentina (78.6%) y Chile (77%) con las cifras más altas..[2]

Penetración de Internet en América Latina
Fuente: Statista and Internet World Stats

Como se indica en el Informe sobre el estado de la banda ancha en América Latina de la CEPAL, el uso de Internet ha crecido en América Latina y el Caribe: el 56% de

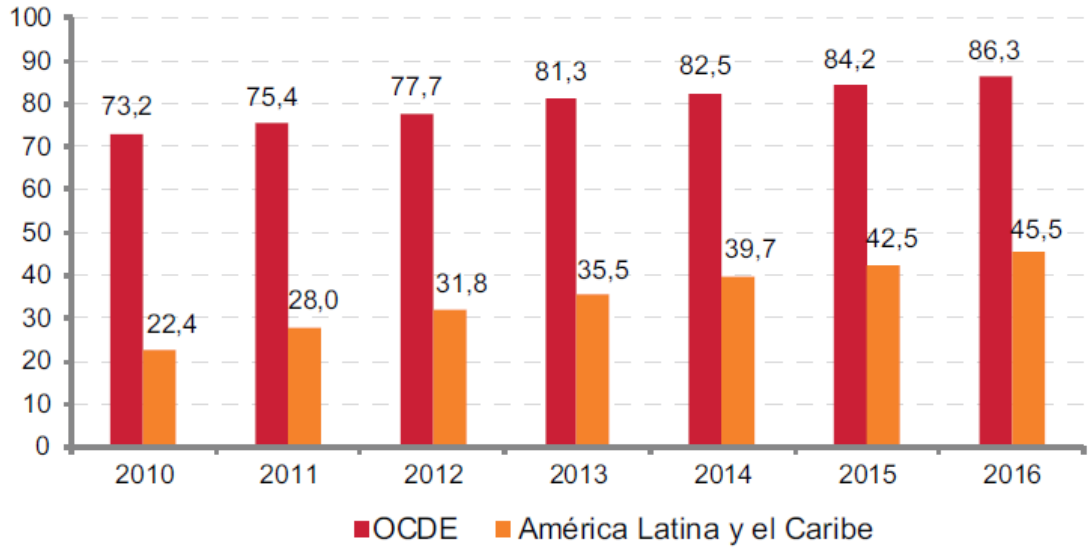
[1] Source: ITU State of the Information Society Report 2018.
[2] Source: Statista and Internet World Stats - https://www.internetworldstats.com/south2.htm

sus habitantes usó la red en 2016, lo que representa un aumento de 36 puntos porcentuales en una década. El informe indica que, en términos de relación con la asequibilidad, en 2010 se requirió asignar aproximadamente el 18% del ingreso promedio mensual para contratar un servicio de banda ancha fija de 1Mbps, mientras que a noviembre de 2017 esa cifra era solo del 1,2%.

La región aún muestra problemas relacionados con la calidad del acceso al servicio de Internet y la equidad en su acceso. Ecuador y Argentina tienen el 15% de sus conexiones con velocidades superiores a un promedio de 15 Mbps. La comparación de estas cifras con los 10 países más avanzados muestra que el 50% de las conexiones son superiores a 15 Mbps.

En términos de hogares conectados a Internet, el informe muestra un aumento del 103% entre 2010 y 2016, ya que más de la mitad de los hogares aún carecen de acceso a Internet.

Puede ser útil comparar estas cifras con regiones más desarrolladas del mundo. En relación con los países de la OCDE, el estudio de la CEPAL muestra una reducción significativa en la brecha entre ese grupo y los países de América Latina y el Caribe. El siguiente gráfico muestra esta reducción. La diferencia de penetración entre las dos regiones, que fue de 50.8 puntos porcentuales (p.p.) en 2010, se redujo a 40.8 en 2016.



Penetración de Internet en los hogares de América Latina y el Caribe en comparación con los países de la OCDE - Fuente: CEPAL basada en datos de la UIT y la OCDE
(Los datos de OCDE no incluyen México y Chile)

1.1.2. Impacto de las comunicaciones móviles en la penetración de internet

El Informe de la ITU sobre el Estado de la Internet Society muestra un progreso continuo en la conectividad y el uso de las TIC. La cantidad de suscripciones móviles-celulares en todo el mundo ahora supera la población mundial, aunque muchas personas, especialmente en países en desarrollo, todavía no usan un teléfono móvil[3].

El impacto de los servicios móviles ha influido en la penetración de Internet y se vuelve relevante para evaluar este impacto. Ha habido un rápido crecimiento en los servicios de banda ancha móvil con suscripciones en todo el mundo que superan los 50 por cada 100 habitantes.

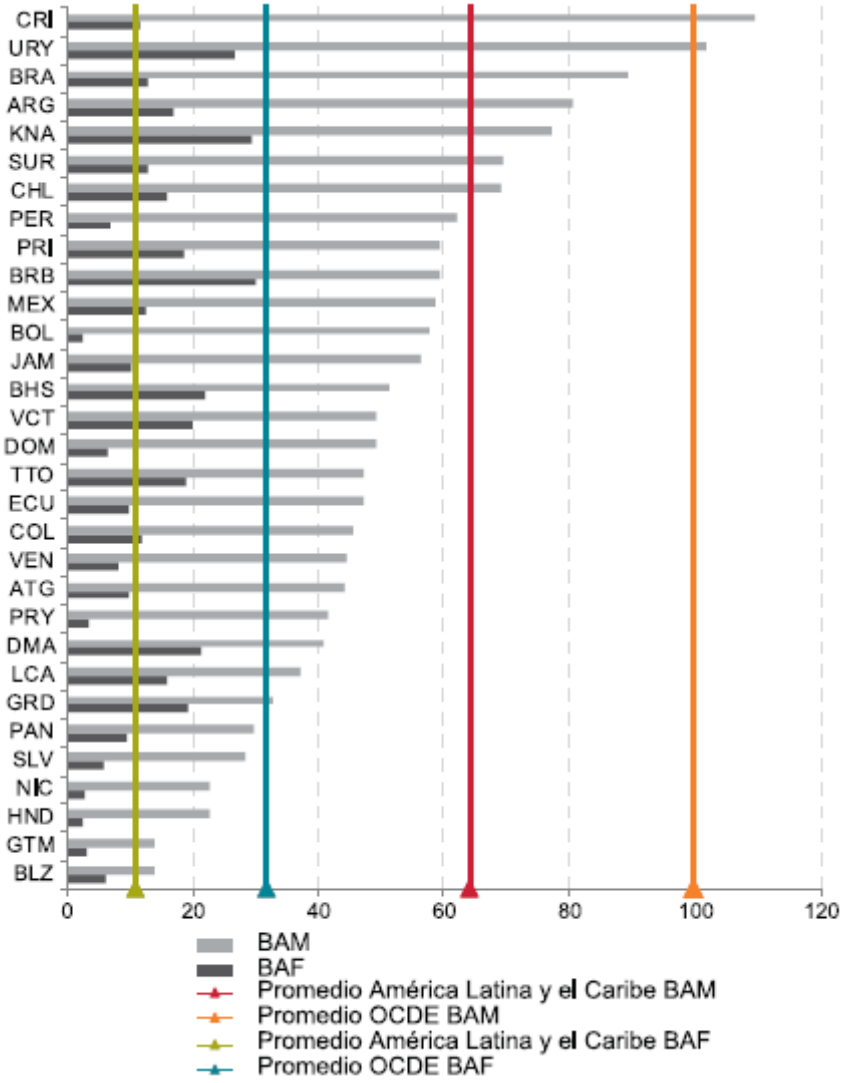
En el informe de la CEPAL, el nivel de penetración de Internet del acceso de banda ancha móvil (BAM) en comparación con el acceso de banda ancha fija (BAF) es mayor. En 2107 BAM alcanzó el 64% y BAF el 11%. La brecha entre los países de la región y los países de la OCDE es de 21% en BAF y 35,5 BAM.[4]

Los datos compilados por la UIT muestran que hay el doble de suscripciones de banda ancha móvil por cada 100 habitantes en los países desarrollados en comparación con los países en desarrollo, mientras que la brecha entre los países en desarrollo más conectados y los países menos avanzados ha aumentado en los últimos años.

El siguiente gráfico muestra la penetración de Internet de banda ancha fija y móvil por país, en comparación con la penetración promedio en los países OCDE.

[3] Fuente: ITU - Measuring the Information Society Report 2018
https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf

[4] A los efectos de este análisis y en este informe, la banda ancha fija se considera a velocidades superiores a 256 kbps y 3 Gbps móvile.



Penetración de banda ancha fija y móvil en la región por país en comparación con OCDE
Fuente: CEPAL a partir de datos del IUT y del Observatorio Regional de Banda Ancha (ORBA)[5]

1.1.3. La infraestructura e Internet

No hay Internet sin infraestructura y América Latina y el Caribe tienen una fuerte dependencia del tráfico internacional de Internet, principalmente de los Estados Unidos, no solo porque el contenido se encuentra allí, sino porque la mayoría de los contenidos generados en la región se encuentran almacenados en ese país. .

Hay dos factores principales que tienen un impacto en la conectividad internacional entre América Latina y América del Norte, uno son los cables submarinos que conectan ambas regiones, el otro son los puntos de intercambio de tráfico de Internet

[5] Fuente: https://repositorio.cepal.org/bitstream/handle/11362/43365/1/S1800083_es.pdf

(IXP: Internet Exchange Points) que tienen un impacto en la calidad del servicio de Internet, la latencia, precios y disponibilidad a nivel local.

Otro factor importante para el crecimiento futuro de Internet es la adopción de IPV6, que también es un facilitador de la implementación de Internet de las cosas (IoT: Internet of Things). LACNIC es el Registro Regional de Internet y el administrador de las direcciones IPV6 para la región LAC. La región está implementando lentamente IPV6, pero se puede ver el progreso en algunos países. El despliegue es bastante lento en las organizaciones y no todos los ISP lo ha implementado todavía.[6]

Las razones de los retrasos en la implementación están relacionadas con la infraestructura actual que tiene problemas para la transición a IPv6, incluidas las dificultades operativas y la disminución de la disponibilidad y el costo creciente de las direcciones IPv4.

Estos problemas se irán resolviendo con el tiempo, ya que la mayoría de los ISP irán actualizando su infraestructura progresivamente. Esta mejora de IPV6 se relaciona con la necesidad de mejorar la imagen corporativa; reconocer que la migración a IPv6 sin un mayor crecimiento de IPv4 es la mejor solución económica y la oportunidad para el crecimiento de la base de negocios y clientes.

[6] Fuente: CAF – LACNIC IPV6 Deployment https://www.lacnic.net/innovaportal/file/3083/1/caf-lacnic-ipv6-deployment-social-economic-development-in-lac.pdf

2015	
Pacific Caribbean Cable System (PCCS)	Balboa, Panamá; Cartagena, Colombia; Hudishibana, Aruba; Jacksonville, Florida, EE.UU; Manta, Ecuador; María Chiquita, Panamá; San Juan, Puerto Rico, EE.UU; TeraCora, Curacao; Islas Vírgenes, Reino Unido.
FOS Quellón-Chacabuco	Puerto Chacabuco, Chile; Quellón, Chile.
2016	
GTMO-1	Dania Beach, FL, EE.UU; Bahía de Guantánamo, Cuba.
2017	
Seabras-1	Playa Grande, Brasil; Wall Township, New Jersey, EE.UU.
Monet	Boca Raton, Florida , EEUU; Fortaleza, Brasil; Santos, Brasil.
2018	
ARBR	Las Toninas, Argentina; Playa Grande, Brasil.
BRUSA	Fortaleza, Brasil; Rio de Janeiro, Brasil; San Juan, Puerto Rico, EEUU; Virginia Beach, Virgina, EE.UU.
Kanawa	Kourou, Guyana Francesa; Schoelcher, Martinica.
South Atlantic Cable System (SACS)	Fortaleza, Brasil; Luanda, Angola.
South Atlantic Inter Link (SAIL)	Fortaleza, Brasil; Kiribi, Camerún.
GTMO-PR	Bahía de Guantánamo, Cuba; Punta Salina, PR, EEUU.
2019	
South America Pacific Link (SAPL)	Balboa, Panamá; Colón, Panamá; Jacksonville, FL, EEUU; Makaha, Hawaii, EEUU; Valparaiso, Chile.
EllaLink	Fortaleza, Brasil; Funchal, Portugal; Playa, Cabo Verde; Santos, Brasil; Sines, Portugal.
SABR	Ciudad del Cabo, Sudáfrica; Recife, Brasil.

Lista de cables submarinos en ALC que comenzaron a funcionar desde 2015
Fuente: CEPAL y Observatorio de Banda Ancha.

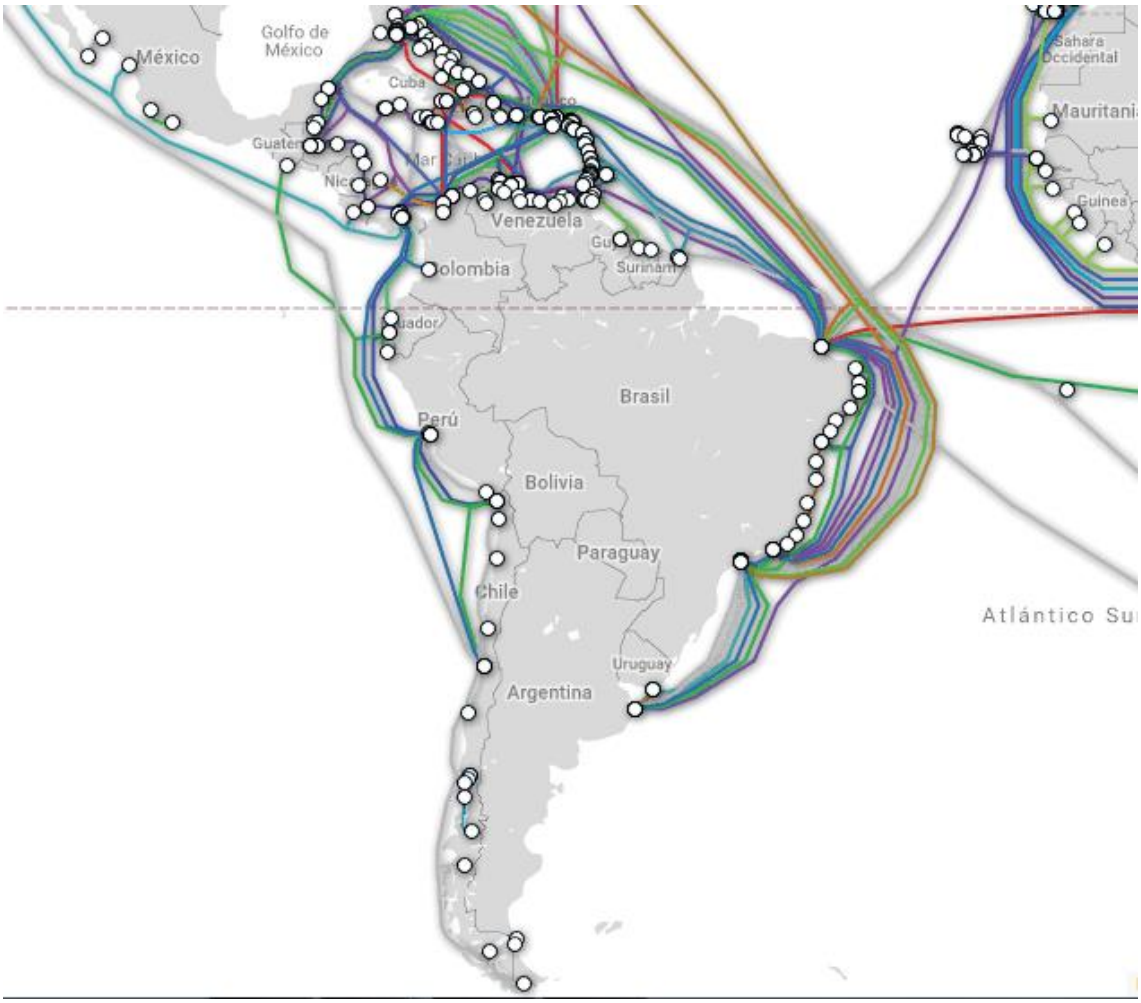
También hay una creciente interconexión de redes a través de puntos de intercambio de tráfico de Internet (IXP) que también desempeñan un papel relevante en la reducción de los precios de las tarifas de acceso a Internet para el usuario final, promoviendo las conexiones de entre pares y el intercambio de contenido a nivel local. Al mismo tiempo, los Content Delivery Networks (CDN) entregan contenido directamente a los IXP, evitando el tránsito a través de redes existentes.

Tanto los IXP como los CDN reducen los costos de acceso y la latencia porque promueven el intercambio de contenido y tráfico a nivel local. El informe de ISOC indica que hay más de 500 IXP en el mundo, y en América Latina también han experimentado un aumento relevante. La instalación de los IXP y los CDN está principalmente impulsada por el sector privado. Los IXPs suelen ser promovidos por las asociaciones nacionales de ISP, mientras que los CDN son creados por

compañías especializadas que ofrecen servicios a terceros o por compañías que entregan sus propios contenidos directamente a los IXP.

Los CDN y las grandes compañías de contenido están creando sus propias redes, que también tienen un impacto en los precios de tránsito, los que tienen una tendencia a la baja.

También hay una tendencia a la descentralización en el sistema de nombres de dominio DNS basada en los servicios de DNS recursivo, que realizan una búsqueda de dirección IP en el DNS en nombre del usuario. Este servicio generalmente proporcionado por los proveedores de servicios de Internet (ISP), ahora lo ofrecen otros actores en el ecosistema de Internet..[7].



Mapa de cables submarinos en LAC. Fuente: Submarine Cable Maps[8]

[7] El DNS público de Google es considerado el más grande entre estos servicios. Permite el uso de las siguientes direcciones IP de DNS: IPV4: 8.8.8.8 y 8.8.4.4 - IPV6: 2001: 4860: 4860 :: 8888 y 2001: 4860: 4860 :: 8844. Las estimaciones de APNIC indican que casi el 15% de todos los usuarios de Internet dependen de este servicio.

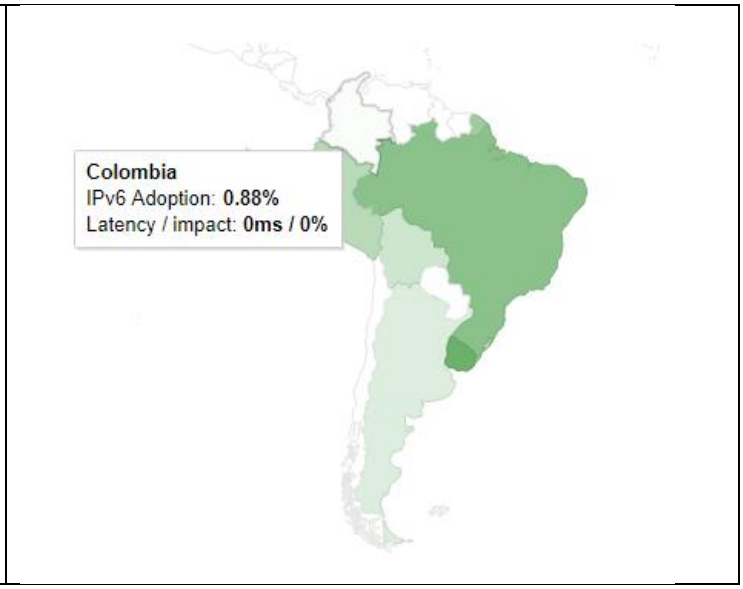
[8] Submarine Cable Map https://www.submarinecablemap.com/#/

Nombre	Ubicación	On line desde	Enlace
CABASE IXP GBA Zona Oeste	Buenos Aires, Argentina	2016	http://www.cabase.org.ar/ixp-gba-zona-oeste/
CABASE IXP Jujuy	Jujuy, Argentina	2016	http://www.cabase.org.ar/ixp-jujuy/
CABASE IXP Junin	Junin, Argentina	2016	http://www.cabase.org.ar/8430-2/
CABASE IXP Norte de Gran Buenos Aires	Pilar, Argentina	2016	http://www.cabase.org.ar/ixp-gba-zona-norte/
CABASE IXP Pergamino	Pergamino, Argentina	2015	http://www.cabase.org.ar/ixp-pergamino/
CABASE IXP Resistencia	Resistencia, Argentina	2017	http://www.cabase.org.ar/ixp-resistencia/
CABASE IXP Sáenz Peña, Chaco	La Plata, Argentina	2016	http://www.cabase.org.ar/ixp-saenz-pena/
CABASE IXP Salta	Salta, Argentina	2016	http://www.cabase.org.ar/ixp-salta/
CABASE IXP Tandil	Tandil, Argentina	2016	http://www.cabase.org.ar/ixp-tandil/
CABASE IXP Tucuman	San Miguel de Tucuman, Argentina	2015	http://www.cabase.org.ar/ixp-tucuman/
CABASE IXP Viedma	Rio Negro, Argentina	2016	http://www.cabase.org.ar/ixp-viedma/
PIT Chile	Santiago, Chile	2016	http://www.pitchile.cl/
Intercambio de tráfico de Internet de Honduras	Tegucigalpa, Honduras	2016	---
Jamaica IXP	Kingston, Jamaica	2015	---
Aracaju	Brasil	2017	http://ix.br/adesao/se
Foz do Iguaçu	Brasil	2016	http://ix.br/adesao/igu
João Pessoa	Brasil	2017	http://ix.br/adesao/jpa
Santa Maria	Brasil	2017	http://ix.br/adesao/ria/

Listado de IXP instalados en Latinoamérica desde 2015
Fuente: CEPAL - Telegeografía - CGI Br

La siguiente lista muestra la adopción de IPV6 en la región y otras referencias internacionales.

Adopción IPV	
Argentina:	7,94 %
Bolivia:	11,94 %
Brazil:	27,92 %
Ecuador:	17,7 %
Colombia:	0,88 %
Chile:	0,14%
México:	27 %
Peru:	16,55 %
Paraguay:	0,46 %
Uruguay:	35,54 %
USA:	33,5 %
Canada:	21 %
Germany	43 %



Adopción IPV6 por país
Fuente: Estadísticas de Google [9]

1.1.4. La seguridad y las regulaciones nacionales

Con el aumento de ataques cibernéticos, problemas de privacidad y noticias falsas, entre otros desafíos, varios gobiernos están reaccionando ya que estos eventos tienen un impacto en la economía, los impuestos, la seguridad nacional y otros problemas relacionados.

Hay varios ejemplos de leyes nacionales que tienen un impacto en una Internet global y abierta, algunas de estas leyes y regulaciones incluyen la necesidad de localización de datos a nivel nacional, leyes de protección de la privacidad, regulaciones relacionadas con la tributación de empresas basadas en la web ubicadas en el extranjero, entre otros.

Los principales impulsores de la participación gubernamental y las reacciones con regulaciones y leyes concretas son:

- Protección de Datos / Privacidad
- Regulaciones de la competencia
- Obligaciones tributarias a nivel nacional
- Influencia de noticias falsas y redes sociales en eventos políticos

[9] Source: https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

- Desinformación
- Fugas de datos
- Exigir el consentimiento del usuario para fines publicitariospurposes
- Temas tributarios

Las regulaciones y leyes a nivel nacional pueden tener un impacto a nivel global dada la conectividad de Internet que traspasa las fronteras de los países[10].

En algunos casos, estas regulaciones pueden tener un impacto no deseado en la libertad de expresión, las actividades políticas, los periodistas y algunas personas.

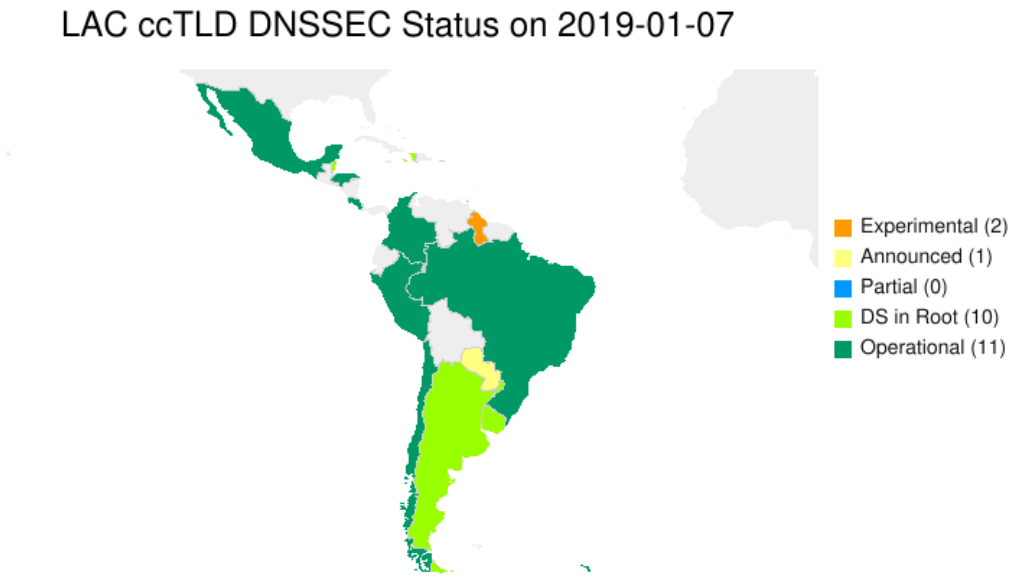
DNSSEC significa "Extensiones de seguridad de DNS" y es una tecnología importante para evitar ciertos ataques cibernéticos. Si se intercepta la consulta de DNS al realizar la solicitud correspondiente de la dirección IP, entonces el navegador puede conectarse a un sitio web diferente al que se esperaba. Esto puede causar varios problemas, incluido el robo de información personal, contraseñas y otras actividades delictivas.

DNSSEC proporciona una manera de evitar este problema agregando seguridad al permitir que el navegador web verifique la información del DNS y confirme que no se modificó.

El Informe de ICANN sobre DNS en América Latina destaca el hecho de que solo Brasil en su ccTLD .br tiene más del 25% de sus dominios bajo administración con DNSSEC habilitado y México con .mx tiene un 5%.

Al parecer existe una baja demanda de este servicio o falta de conocimiento de los beneficios positivos para la seguridad relacionados con su uso.

[10] Fuente: https://www.internetsociety.org/policybriefs/ixps/



Fuente: Internet Society[11]

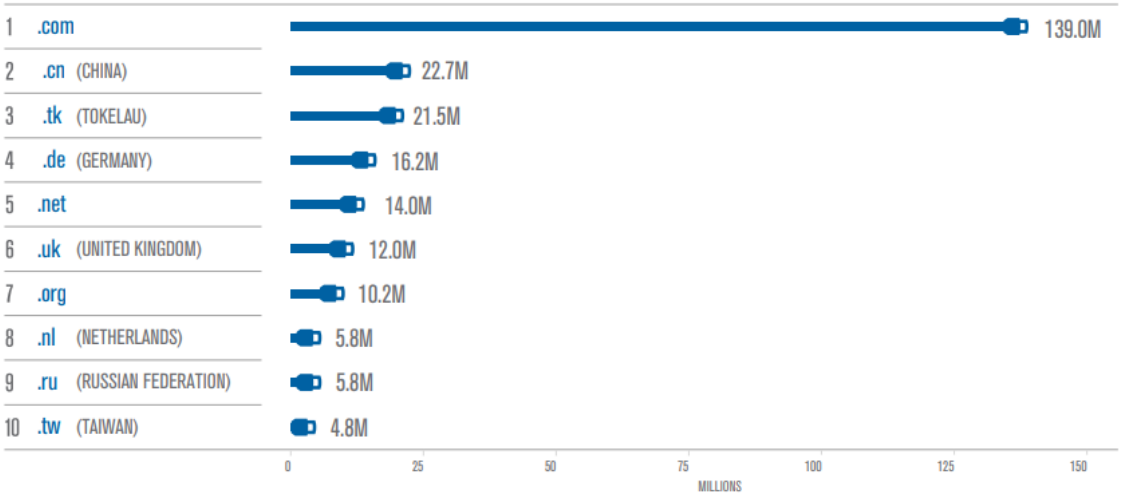
[11] Fuente: https://www.internetsociety.org/deploy360/dnssec/maps/

1.2. Tendencias internacionales en el Mercado de dominios global y en la región de América Latina

1.2.1. El mercado global de dominios de Internet

Informes recientes emitidos por la industria de dominios de Internet indican que el mercado global de dominios se estima en 348 millones en todos los TLD[12] registrados. El número de dominios registrados crece cada año a un ritmo más lento. El informe de estadísticas de CENTR indica que a partir de enero de 2019, ha registrado su tasa interanual más baja registrada de 3.7%[13].

Las tasas de registro más bajas de los nombres de dominio tienen varias explicaciones, ya que ahora hay presencia en línea en formas alternativas, como por ejemplo las redes sociales.



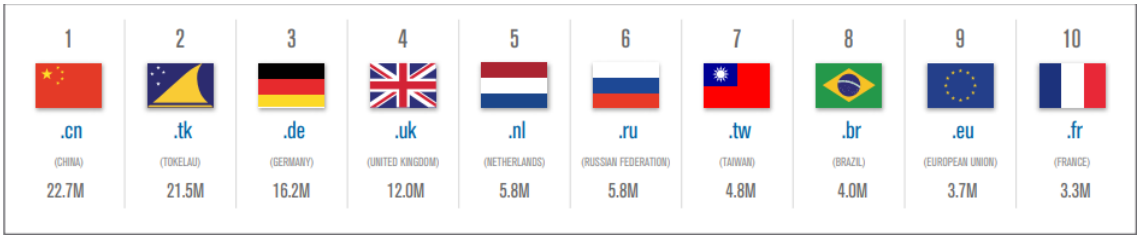
Top TLDs por número reportado de Dominios
Fuente: Verisign Domain Name Industry Brief [14]

En relación con los ccTLD, el repotre Verisign Domain Name Industry Brief indicó que había aproximadamente 154.3 millones de registros de nombres de dominio ccTLD al final del cuarto trimestre de 2018, con un aumento de aproximadamente 5.0 millones de registros de nombres de dominio (3.4 %), en comparación con el tercer trimestre de 2018.

[12] TLD: Dominio de nivel superior o dominio de nivel superior. Ej: .co, .com, etc.
[13] Se refiere al crecimiento medio de los 500 TLD principales (por dominios) con datos confiables. Fuente: CENTRstats Global TLD Report - https://www.strategyr.com/MarketResearch/market-report-infographic-domain-names-forecasts-global-industry-analysts-inc.asp
[14] Fuente: https://www.verisign.com/assets/domain-name-report-Q42018.pdf

El informe indica que los ccTLD más grandes representan el 64.7 por ciento de todos los registros de nombres de dominio de ccTLD. Fueron hasta diciembre de 2018: .cn (China), .tk (Tokelau), .de (Alemania), .uk (Reino Unido), .nl (Países Bajos), .ru (Federación de Rusia), .tw (Taiwán), .br (Brasil), .eu (Unión Europea) y .fr (Francia).

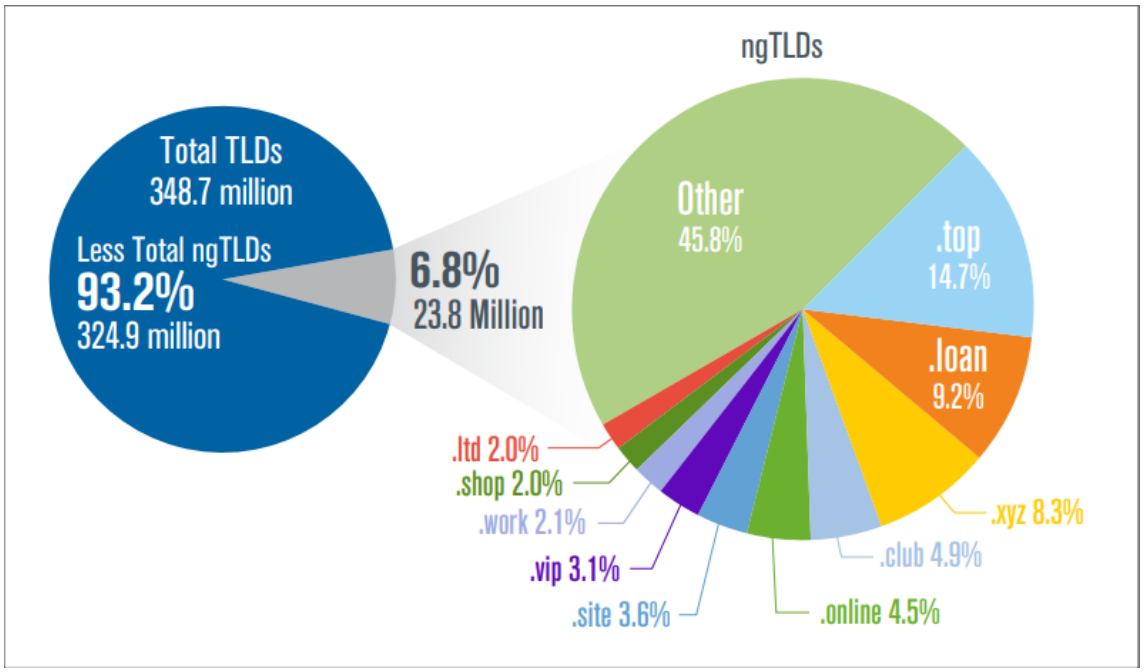
Al 31 de diciembre de 2018, había 302 extensiones de ccTLD globales delegadas en la zona raíz, incluidos los Nombres de dominio internacionalizados (IDN).



ccTLD con mayor cantidad de dominios reportados en el mundo
Fuente: Verisign Domain Name Industry Brief

Los nuevos gTLD no tuvieron el impacto que se esperaba originalmente, solo algunos de los nuevos gTLD han resultado exitosos y la industria está mostrando cierta concentración con las adquisiciones realizadas por los Registros más grandes de los nuevos gTLD más pequeños y menos sustentables.

Los 10 nuevos gTLD principales representan el 54.2 por ciento de todos los registros de nombres de dominio ngTLD. La siguiente figura muestra los registros de nombres de dominio ngTLD como un porcentaje del total de registros de nombres de dominio, de los cuales representan el 6.8 %, así como los 10 ngTLD principales como porcentaje de todos los registros de nombres de dominio ngTLD para el cuarto trimestre de 2018.



Nuevos gTLDs como porcentaje del total de TLDs
Fuente: Verisign Domain Name Industry Brief

Los informes indican que los registros de ngTLD fueron aproximadamente 23.8 millones al final del cuarto trimestre de 2018, con un aumento de aproximadamente 0.4 millones de registros de nombres de dominio, o 1.6 %, en comparación con el tercer trimestre de 2018.

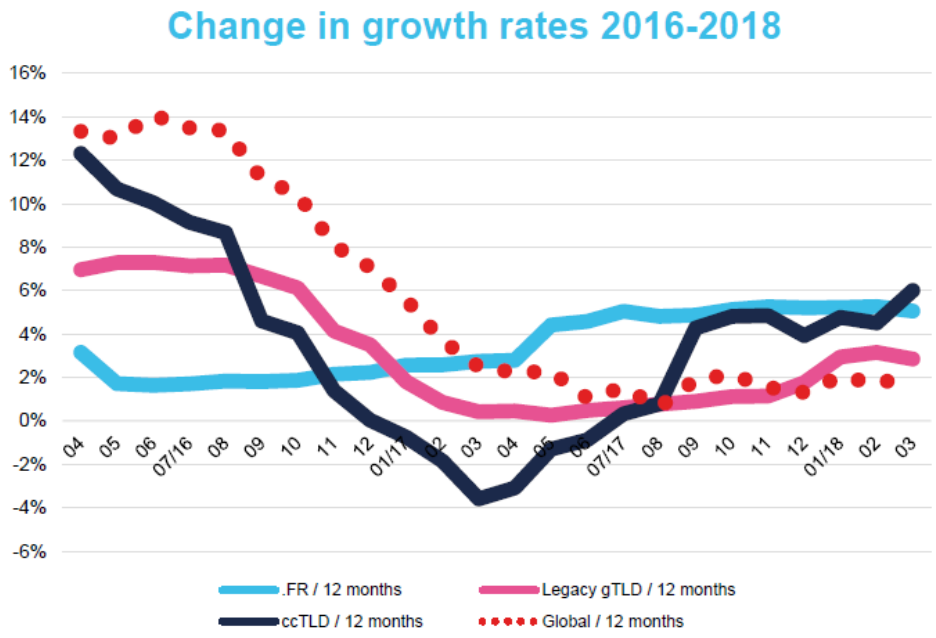
Los nuevos gTLD representan alrededor del 12% de todos los gTLD, los gTLD anteriores o “legacy” han visto una reducción del 2% respecto al mismo período del año anterior.[15]

Desde una perspectiva regional, los informes muestran una situación estable en América del Norte y América Latina con un mayor crecimiento en África y Asia Pacífico. La evolución del mercado se puede ver en los siguientes gráficos.

[15] Legacy gTLD. Lista de 18 gTLD: .aero, .asia, .biz, .cat, .com, .coop, .info, .jobs, .mobi, .museum, .name, .net, .org, .post, .pro , .tel, .travel, .xxx. Fuente: ICANN

	Stock (millions)			Variations (%)		Market share (%)			
	2015	2016	2017	2016	2017	2015	2016	2017	17/16
North America	4.2	4.8	4.8	15.7%	-0.4%	3.0%	3.4%	3.3%	-0.1
Latin America	7.0	7.7	7.7	9.1%	0.0%	5.0%	5.5%	5.2%	-0.3
Africa	2.3	3.3	5.8	45.0%	72.7%	1.6%	2.4%	3.9%	+1.5
Asia-Pacific	59.3	55.8	56.2	-5.9%	0.8%	42.0%	39.5%	38.3%	-1.2
Europe	68.3	69.5	72.2	1.8%	3.9%	48.4%	49.2%	49.2%	0
TOTAL	141.1	141.1	146.7	0.0%	3.9%	-	-	-	-

Evolución regional del mercado de nombres de dominio 2015 - 2017
Fuente: AFNIC con información de organizaciones regionales de ccTLD



Cambio en la tasa de crecimiento de los nombres de dominio
Fuente: Informe del mercado mundial de nombres de dominio de AFNIC [16]

El informe de CENTR indica que se prevé que el mercado global de nombres de dominio alcance los 536,2 millones de registros acumulativos para 2024 debido a la rápida expansión en las regiones en desarrollo, las altas tasas de adopción de teléfonos inteligentes y el crecimiento de la economía mundial.

Habrá una creciente demanda de dominios premium que sean cortos, relevantes y fáciles de recordar y también con el aumento de la demanda de IDN (nombres de dominio internacionales).

[16] Fuente: CENTRstats Global TLD Report | Jan 2019

Europa representa el mercado más grande del mundo y se espera que Asia-Pacífico tenga el mayor crecimiento liderado por la migración de empresas a Internet y el creciente volumen de transacciones de comercio electrónico.

Internet está evolucionando para convertirse en un servicio público y todas las empresas e individuos necesitarán presencia en línea, esto tendrá un impacto en la demanda global de nombres de dominio de Internet.

1.2.2. Mercado de Nombres de Dominio en América Latina y el Caribe

Basado en informes de LACTLD [17] y de ICANN, ha habido un crecimiento en todos los ccTLD en la región en el período 2010 - 2016, excepto en Argentina (.ar) que cambió la política de precios de los dominios .ar [18]. El impacto de este cambio en la política de .ar impactó en la caída general en los registros de ccTLD para la región en el período 2013-2014.

Las estadísticas de LACTLD y la ICANN muestran una tasa de crecimiento de un promedio del 6% desde 2010, que está más cerca del crecimiento global del dominio del 8%. Estos porcentajes excluyen a .co y .ar que tenían diferentes tasas de crecimiento. En el caso de .co de Colombia, ha mostrado un aumento muy alto de registros de dominio basados en una nueva estrategia de marketing y en el caso de .ar de Argentina, el número de dominios disminuyó debido a un cambio en el precio.

La lista de ccTLD en la región de América Latina y el Caribe está compuesta por:

- 1 en Norteamérica
- 7 en América Central
- 13 en Sudamérica
- 28 en el Caribe

[17]LACTLD es la organización de ccTLD de América Latina y el Caribe. https://www.lactld.org/

[18] Para los años anteriores, .ar no cobraba tarifas por los registros de nombres de dominio que llegaban a aproximadamente 2.5 millones de nombres de dominio bajo administración. En 2014, .ar cambió a un sistema de registro basado en tarifas, y los dominios .ar se redujeron de un total de 2.5 millones en 2013 a 850,000 en 2014 y 550,000. Ahora

Norteamérica:

- .mx: Mexico

Caribe:

- .ag: Antigua y Barbuda
- .ai: Anguilla
- .aw: Aruba
- .bb: Barbados
- .bl: Saint-Barthélemy
- .bq: Bonaire, Saba, San Eustaquio
- .bs: Bahamas
- .cu: Cuba
- .cw: Curacao
- .dm: Dominica
- .do: República Dominicana
- .gd: Granada
- .gp: Gruadalupe
- .ht: Haiti
- .jm: Jamaica
- .kn: St. Kitts y Nevis
- .ky: Cayman Islands
- .lc: Sain Lucia
- .mf: Saint-Martin
- .mq: Martinica
- .ms: Montserrat
- .pr: Puerto Rico
- .sx: Saint Maarten
- .tt: Trinidad Tobago
- .tc: Turc and Caicos
- .vc: St Vincent and Grenadines
- .vg: Virgin Islands (Uk)
- .vi: Virgin Islands (USA)

América del Sur:

- .ar: Argentina
- .bo: Bolivia
- .br: Brazil
- .cl: Chile
- .co: Colombia
- .ec: Ecuador
- .gf: French Guyana
- .gy: Guyana
- .py: Paraguay
- .pe: Perú
- .sr: Suriname
- .uy: Uruguay
- .ve: Venezuela

América Central

- .bz: Belize
- .cr: Costa Rica
- .gt: Guatemala
- .hn: Honduras
- .ni: Nicaragua
- .pa: Panamá
- .sv: El Salvador

Existen diferentes modalidades de administración de los ccTLD regionales, y hay muchas de ellas que no tienen carácter comercial. Un tercio de los registros de ccTLD son empresas privadas, otros son administrados por gobiernos o universidades. Algunos tienen una orientación comercial y son competitivos a nivel internacional, como .mx y .co. El hecho de que algunos sean administrados por gobiernos o por organizaciones como universidades, suele resultar en algunas limitaciones a las normas de registro. Este hecho también limita la capacidad de desarrollar una estrategia comercial abierta para las ventas de nombres de dominio.

El tamaño de los diferentes registros varía desde TLD grandes como Brasil con más de 4M de dominios registrados, hasta pequeños con menos de 1000 como algunos en el Caribe.

En relación con la tercerización del servicio de back-end, aproximadamente la mitad de los ccTLD utilizan servicios tercerizados para las operaciones de back-end. El resto tiene su propio sistema de registro e infraestructura.

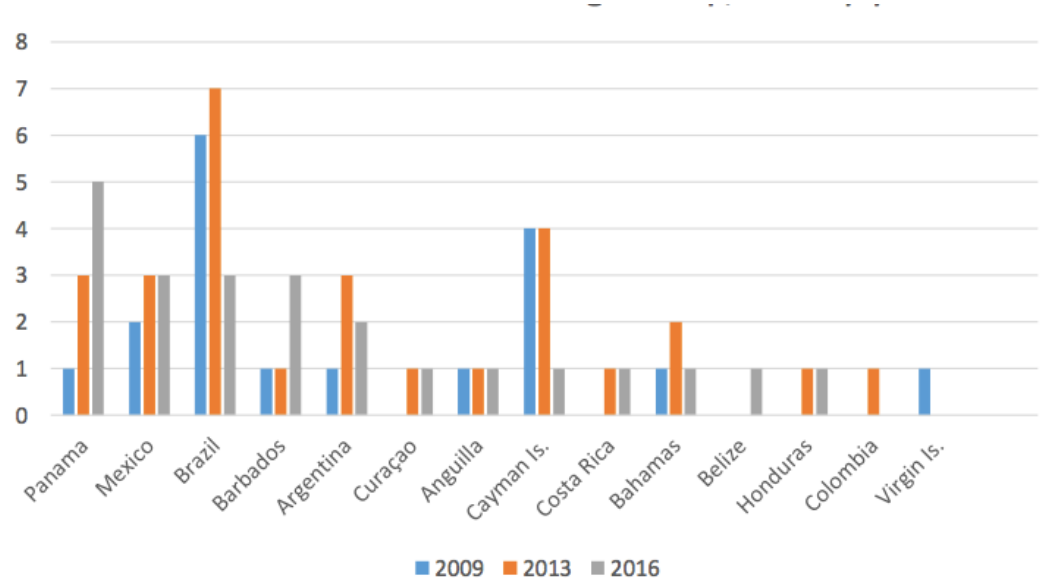
Al momento de este informe, no se han publicado estadísticas actualizada generales para todos los ccTLD de LAC publicados por LACTLD. Aproximadamente el 95% de los dominios en los ccTLD de LAC se registran principalmente en cinco ccTLDS que son: .ar, .br, .co, .mx y.cl. Según informaron los administradores de ccTLD, estos son los registros de nombres de dominio hasta mayo de 2019:

- .ar: 492.238
- .br: 4.039.913
- .cl: 584.909
- .co: 2.200.000
- .mx: 1.127.680
- .pe: 114.755
- .uy: 84.878

Algunos de los ccTLD más grandes no utilizan intermediarios para vender dominios, como es el caso de Argentina. En Brasil, que es el ccTLD más grande de la región, existe una combinación de ventas directas y registradores acreditados.

Convertirse en un registrador acreditado en América Latina y el Caribe es una tarea fácil, y algunos de ellos una vez en operaciones no resultan económicamente sustentables en el tiempo. Por esta razón el número de registradores acreditados por ICANN está disminuyendo cada año.

El estudio de ICANN Lac DNS Market Place indica que aproximadamente el 60% de los ccTLD no dependen de registrars para sus ventas. La falta de canales de venta como Registradores Acreditados de ICANN, es una de las razones del lento crecimiento de las ventas de nombres de dominio en América Latina y el Caribe. Hay un número importante de revendedores, principalmente asociados con empresas de hosting, estudios de diseño web y proveedores de servicios de Internet.



Número de Registrars acreditados por ICANN en países de América Latina y el Caribe
Fuente: ICANN[19]

El principal problema con los registrars y revendedores no acreditados es que no están tan actualizados y conscientes de las diferentes opciones que puede ofrecer un canal de ventas más formal. Un ejemplo son los nuevos gTLD que actualmente ofrecen una gran variedad de opciones para usuarios finales y empresas a la hora de comprar un dominio.

El impacto del proceso de nuevos gTLD fue muy bajo en América Latina y el Caribe. Solo hubo 24 solicitudes de nuevos gTLD entre más de 1900 solicitadas en todo el mundo. Dentro de las 24 solicitudes, ocho fueron TLD de marcas, dos de tiepo geográfico y el resto fueron generales. En relación con la distribución geográfica, 11 fueron de Brasil, 6 de Uruguay, 3 de México, 3 de Paraguay y 1 de Colombia. El registro de dominios en nuevos gTLD no ha sido alto en la región, las estimaciones indican que los nuevos gTLD registrados en la región son aproximadamente 300,000.

NIC.mx es el único ccTLD en la región que desarrolló su propio registrador acreditado por ICANN (Akky). Tanto .mx como .co promueven activamente sus

[19] Source: https://www.icann.org/registrar-reports/accredited-list.html

canales de venta, mientras que en el caso de .br son registrars reconocidos por el ccTLD, pero no los promocionan ni se publicitan oficialmente.

Los registrars de la región de LAC se focalizan principalmente en su mercado nacional o local, y solo unos pocos tienen actividades fuera de las fronteras nacionales.

Se estima que existen unos 28,000 IDN asociados con la región registrada en ccTLD en el segundo nivel. Los IDN en la región se ofrecen para permitir algunos caracteres especiales del español del portugués.

1.3. Análisis del impacto de las discusiones que se llevan a cabo actualmente en ICANN sobre el mercado de nombres de dominio, con énfasis en el mercado de ccTLD

ANALISIS

La Corporación de Internet para Nombres y Números Asignados (ICANN) es el foro global para desarrollar políticas para la coordinación de algunos de los elementos técnicos centrales de Internet, incluido el sistema de nombres de dominio (DNS).

Lo que recomendamos es que el equipo de liderazgo .CO se involucre de manera proactiva con ICANN y participe en varios grupos multistakeholder y en el proceso de políticas según sea necesario. Como mínimo, los representantes del gobierno colombiano y / o .CO deben ser miembros activos de los siguientes grupos:

- El Comité de Gobierno / Government Advisory Committee[20] (GAC)
- El ccNSO Country Code Names Supporting Organization[21] (ccNSO)

Además de participar en estos dos grupos dentro de ICANN, sería prudente monitorear los esfuerzos de los siguientes grupos:

- Generic Names Supporting Organization (GNSO)[22]
- Geo TLD Group[23]

La sección 2.2 incluye con más detalle estas organizaciones en las que .CO puede querer participar.

Debido a la naturaleza híbrida de .CO, se enfrenta a problemas diferentes a los de un ccTLD tradicional, por lo que debe informarse más allá del ccNSO en ICANN. Casi toda la formulación de políticas se define en el GNSO y sus estructuras relacionadas. Hay algunos temas, como la transición de la IANA, que se deliberaron en un Grupo de trabajo intercomunitario, sin embargo ocurren con poca frecuencia. Los temas clave dentro del espacio de ICANN que deben ser monitoreados incluyen:

[20] https://gac.icann.org/
[21] https://ccnso.icann.org/en
[22] https://gnso.icann.org/en
[23] http://geotld.group/

- Subsequent Procedures Working Group[24] (SubPro)- este es grupo de trabajo que definirá las reglas de las ofertas de nuevas rondas de gTLD. El grupo no solo está refinando las reglas de la ronda de 2012, también está desarrollando, cuando sea necesario, nuevas políticas que guiarían las futuras solicitudes y delegaciones. El grupo comenzó su trabajo en 2016 y el cronograma actual, que está sujeto a demoras, sugiere que el trabajo de políticas podría completarse tan pronto como finalice 2019 con la apertura de la próxima ronda de apertura en el primer trimestre de 2022. .CO vio un aumento en la competencia de la ronda de 2012 y es espreable suponer que cuando se lance la próxima ronda, habrá una mayor competencia. El grado de competencia depende de la cantidad de aplicaciones que ingresen y, eventualmente, de la delegación. La selección de TLD también será clave, ya que no todos los nuevos gTLD son lo suficientemente genéricos para algunos potenciales registrantes de dominios.
- WT5 discussions within Sub Pro – Como el tema de los nombres de países y territorios en el nivel superior tuvo una gran atención en la primera ronda con las aplicaciones de .AMAZON y .PATAGONIA, el liderazgo de SubPro tomó la decisión de crear una grupo de trabajo separado para centrarse en estos temas. Cuenta con una participación importante de los gobiernos y es donde se determinará lo que se puede y no se puede aplicar, incluidas las posibles palabras como .COL. Actualmente, hay opiniones divergentes entre los participantes sobre lo que deberían incluir las reglas futuras, por lo que no está claro qué cambios a partir de 2012 podrían acordarse. Los intentos de resolver estas diferencias tendrán lugar en los próximos meses.
- The EU General Data Protection Regulation (GDPR) - Este es el cambio más importante en la regulación de la privacidad de los datos en 20 años. Los impactos se perciben mucho más allá del espacio de la ICANN / DNS, pero lo que más preocupa a .CO debe ser los requisitos que se está desarrollando en ICANN para continuar brindando un servicio de Whois y al mismo tiempo cumplir con los requisitos de las regulaciones. No tenemos conocimiento de ninguna acción tomada por las Autoridades Europeas de Protección de Datos contra las operaciones de ccTLD fuera de la UE, pero como .CO se comercializa más como un TLD genérico, es posible que haya registrantes

[24] https://community.icann.org/display/NGSPP/New+gTLD+Subsequent+Procedures+PDP+Home

que estén alcanzados por la regulación. Los alcanzados se definen como todos los ciudadanos individuales de la Unión Europea y el Espacio Económico Europeo (EEE), independientemente de dónde vivan. El trabajo dentro de ICANN está siendo manejado por un Proceso de Desarrollo de Políticas Acelerado (EPDP)[25]. La EDPD finalizó recientemente la Fase 1 de su trabajo (a partir del 13/5/2019 está en espera de la aprobación de la Junta Directiva de ICANN). La fase 2, que desarrollará métodos para acceder a los datos restringidos de Whois, acaba de comenzar su trabajo y las estimaciones varían acerca de cuándo se completará. Una vez completado, .CO debe evaluar si se deben adoptar los productos como parte de sus procedimientos operativos para garantizar el cumplimiento de GDPR

- El plan estratégico de ICANN, incluida la evolución de la eficacia del modelo de múltiples partes interesadas: si bien esto puede no tener un impacto directo en la operación de .CO, los cambios en la forma en que opera ICANN podrían tener un impacto en la forma en que se desarrollan las políticas que podrían impactar en el futuro. El reciente lanzamiento de esta discusión es algo a tener en cuenta y monitorear.

Cómo facilitar esta participación es una pregunta difícil de responder. El enfoque más directo sería que MinTIC forme un equipo interno para supervisar los aspectos operativos de .CO, pero también agregar un componente de temas de política al equipo para garantizar una cobertura adecuada.

A falta de recursos internos, una opción a considerar la creación de una una Fundación .CO externa que pueda reunir los recursos para permitir una mayor participación de los miembros del equipo de MinTIC o consultores externos que brinden apoyo a MinTIC. La fundación podría estar estructurada de forma tal que se financie con los ingresos de la venta de dominios .CO o mediante una contribución del proveedor de servicios de registro.

[25] https://community.icann.org/display/EOTSFGRD

RECOMENDACIONES:

Explorar formas de estar al tanto de las activiades del GNSO de la ICANN, ya sea directamente por el personal de MinTIC o indirectamente a través de un requisito para que el nuevo proveedor de servicios de registro proporcione dicha supervisión.

Explorar la posibilidad de establecer una fundación como parte de la operación de .CO para facilitar la cobertura de Internet necesaria.

Personalizar el equipo en MinTIC de manera adecuada para garantizar la capacidad de cubrir más de una reunión a la vez.

1.4. Identificación de posibles escenarios para modelar escenarios prospectivos relacionados con el mercado de nombres de dominio con énfasis en el mercado de ccTLD

ANALISIS

Por favor ver el Reporte económico incluido en sección 4.3 de este informe.(Página 97)

2. Parte 2 (Ref: 2.2.2.)
Apoyar en el análisis e identificación de mejores prácticas a nivel global y en la región Latinoamérica y el Caribe (ventajas y desventajas), de acuerdo con los requerimientos establecidos por ICANN/IANA (cuando aplique) y mejores prácticas a nivel internacional

2.1. Analisis de las políticas sobre DNS establecidas por ICANN/IANA

ANALISIS

A pesar de su naturaleza soberana, los ccTLD sienten el impacto de las políticas desarrolladas en la ICANN. A continuación se muestra una descripción general de algunos de los más importantes que se encuentran actualmente en desarrollo o en su lugar.

Políticas del ccNSO

La ccNSO no solo desarrolla sus propias políticas a través de un Proceso de desarrollo de políticas (ccPDP), sino que también participa activamente en varios procesos de desarrollo de políticas en ICANN, lo que incluye un papel de liderazgo en el trabajo sobre los nombres de país y geográficos en el nivel superior, respondiendo a los comentarios del público y proporcionando comentarios sobre las operaciones de la ICANN a través de comentarios sobre el presupuesto y el plan estratégico. De hecho, los comentarios de la ccNSO sobre estos dos últimos temas son muchas veces los comentarios más completos y detallados presentados. A medida que surgen problemas, el Consejo de la ccNSO constituye varios grupos de trabajo para abordar el trabajo necesario para abordar estas cuestiones de política. Los grupos de trabajo actuales incluyen:

- CCWG Auction Proceeds
- Guidelines Review Committee (GRC)
- ccNSO Meetings Programme Standing Committee (formerly WG)
- ccPDP Retirement Working Group
- ccNSO Strategic and Operational Planning Standing Committee (formerly SOPWG)
- Technical Working Group
- TLD-OPS Standing Committee

- ccNSO Review Working Party
- ccNSO Study Group on Use Emoji as Second Level Domains
- ccNSO Internet Governance Liaison Committee (IGLC)

La ccNSO también organiza el "Día de la Tecnología" en las reuniones de ICANN. Se trata de una serie de presentaciones sobre temas técnicos que podrían afectar las operaciones de .CO. Investigadores líderes en la industria del DNS se presentan en un ambiente informal con mucho tiempo para preguntas y respuestas. Los temas cubiertos en el Día de la tecnología más reciente incluyen la Aceptación universal (UA), los asuntos relacionados con los Nombres de dominio internacionalizados (IDN), la implementación de IPv6, la recuperación de desastres, la seguridad del registro y el DNS a través de HTTPS. Las sesiones de los días se resumen en un Informe denominado Tech Day.

- De manera similar, la GNSO también se refiere a los procesos de desarrollo de políticas para trabajar en cuestiones de políticas que afectan a los gTLD. El Grupo de Trabajo de Procedimientos Subsiguientes (SubPro) está configurando las políticas que regirán la próxima ronda de nuevos gTLD. El grupo no solo está revisando las políticas que se usaron en la ronda de 2012, sino que también está desarrollando, cuando es necesario, nuevas políticas que guiarían las futuras rondas. El grupo comenzó su trabajo en 2016 y el cronograma actual, que está sujeto a demoras, espera que trabajo de políticas se podría completar a fines de 2019 con la apertura de la próxima ronda de nuevos gTLDs aproximadamente 2022. .CO ha experimentado un aumento en la competencia con el resultado de la ronda de nuevos gTLDs en 2012 y es muy probable suponer que cuando se lance la próxima ronda, habrá una competencia aún mayor. El grado de competencia depende de la cantidad de aplicaciones que ingresen y, eventualmente, de la delegación. La selección de TLD también será clave, ya que no todos los nuevos gTLD son lo suficientemente genéricos para algunos potenciales registrantes de dominios.
- Debates sobre comentarios de la WT5 dentro de Grupo de GNSO Sub Pro: como el tema de los nombres geográficos en el nivel superior resultó de gran relevancia en relación a las aplicaciones para .AMAZON y .PATAGONIA, el grupo SubPro tomó la decisión de crear un grupoo de trabajo separado enfocado en estos asuntos. Este grup de trabajo couenta con una gran

participacion de gobiernos, más que en otros procesos anteriores. De hecho, una de las cooordinadoras, Olga Cavalli, participa en el Comité de Gobierno de ICANNGAC y otra, Annebeth Lange, participa en el ccNSO. En este grupo es donde se determinarán algunas de las reglas de lo que se puede y no se puede aplicar, incluidas las posibles palabras como .COL. Actualmente, hay opiniones divergentes entre los participantes sobre qué deberían incluir las reglas futuras, por lo que no está claro qué cambios se realizarán en base a las reglas de 2012. Los intentos de resolver estas diferencias sucederán en los próximos meses.

- El Reglamento general de protección de datos de la Unión Europea (GDPR): este es el cambio más importante en la regulación de privacidad de datos en 20 años. Los impactos se perciben mucho más allá del espacio de ICANN / DNS, pero lo que más debe preocupar a .CO deben ser los requisitos que está desarrollando ICANN para continuar brindando el servicio de Whois y al mismo tiempo cumplir con los requisitos del amplio rango de las nuevas regulaciones. No tenemos conocimiento de ninguna acción tomada por las Autoridades Europeas de Protección de Datos contra las operaciones de ccTLD fuera de la UE, pero como .CO se comercializa como un TLD genérico, es probable que haya casos en los que haya registrantes que estén alcanzados por esta regulación. Aquellos alcanzados se definen como todos los ciudadanos individuales de la Unión Europea y el Espacio Económico Europeo (EEE), independientemente de donde vivan. Dentro de ICANN este trabajo está siendo realizado p or el Expedited Policy Development Process (EPDP)[26]. EDPD recientemente terminó la Fase 1 de su trabajo (a partir del 13/5/2019 se espera la aprobación de la Junta Directiva de ICANN). La fase 2, que desarrollará métodos para acceder a los datos restringidos de Whois, acaba de comenzar su trabajo y las estimaciones varían acerca de cuándo se completará. Una vez completado, .CO debe evaluar si deben adoptar los productos como parte de sus procedimientos operativos para garantizar el cumplimiento de GDPR

[26] https://community.icann.org/display/EOTSFGRD

Temas Cross Community de relevancia para .CO

- CCWG Auctions Proceeds[27] – El nuevo programa de gTLD estableció las subastas como un mecanismo de último recurso para resolver la disputa por cadenas. La mayoría de las solicitudes de nuevos gTLDs se resolvieron por otros medios antes de llegar a una subasta realizada por ICANN. Se acumularon importantes fondos como resultado de varias subastas. Los ingresos actuales superan los $ 250 millones de Dólares Estadounidenses. Los ingresos de la subasta se han reservado hasta que la Junta autorice un plan para el uso apropiado de los fondos. A través de las Ganancias de Subastas del CCWG, la Junta, el personal y la comunidad están trabajando juntos para diseñar y definir el uso de los ingresos de las subastas de nuevos gTLD.
- El plan estratégico de ICANN y la evolución de la eficacia del modelo de múltiples partes interesadas (multistakeholder): si bien esto puede no tener un impacto directo en la operación de .CO, los cambios en la forma en que opera la ICANN podrían tener un impacto en la forma en que se desarrollan las políticas que podrían impactar en el futuro. El reciente lanzamiento de esta discusión es algo a tener en cuenta y monitorear.

A medida que las cuestiones de políticas son más importantes en las reuniones de ICANN, el personal ICANN desarrolla informes de políticas previos a la reunión [28] y reportes posteriores[29]. Estos son recursos valiosos para ayudar al equipo de .CO a mantenerse al tanto de estos temas.

Otras políticas / Temas sobre los que .CO debe prestar atención:

- DNSSEC[30] – Desafortunadamente, el despliegue de DNSSEC está ocurriendo más lentamente que los expertos esperaban. Como operador de registro, .CO debería alentar a los registradores y solicitantes a habilitar esta importante tecnología.

[27] https://community.icann.org/display/CWGONGAP/Cross-Community+Working+Group+on+new+gTLD+Auction+Proceeds+Home
[28] https://go.icann.org/pre64
[29] https://go.icann.org/post64
[30] https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

- DNS Hijackings – Una reciente expansión de DNS Hijackings[31], ha obligado a los operadores de ccTLD a reexaminar cómo protegen sus servidores de nombres. Si bien la implementación de DNSSEC ayudó a mitigar los ataques en esos sitios, otros no fueron tan afortunados. Los expertos recomiendan [32] que los operadores emplean técnicas como los servicios de bloqueo ofrecidos por los registradores y los registros, la autenticación de dos factores, el fortalecimiento de la contraseña y otras prácticas comunes de higiene de seguridad son todas recomendaciones de seguridad de mejores prácticas.

[31] https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/
[32] https://blog.verisign.com/domain-names/revisiting-how-registrants-can-reduce-the-threat-of-domain-hijacking/

2.2. Analisis del funcionamiento de ICANN / IANA como organizaciones a través de sus políticas operativas

ANALISIS

Como se discutió en 1.3, es imperativo que .CO y MinTIC participen en varias organizaciones para no solo asegurarse de que se está al tanto de lo que está sucediendo en la industria, sino también para que pueda desempeñar un papel activo cuando sea necesario para promover sus intereses o prevenir eventos no deseados.

La Corporación de Internet para Nombres y Números Asignados (ICANN) es el foro global para desarrollar políticas para la coordinación de algunos de los elementos técnicos centrales de Internet, incluido el sistema de nombres de dominio (DNS). ICANN opera en base al consenso, con las partes interesadas (stakeholders) involucradas que se reunen para formular políticas coordinadas para los elementos técnicos centrales de Internet en base al interés público. Posteriormente las políticas se implementan mediante el acuerdo de quienes operan los elementos centrales, incluidos los registries (operadores y patrocinadores de registros de gTLD), los administradores de ccTLD, los registros regionales de Internet (RIR) y los operadores de servidores de nombres de raíz o root servers.

Tradicionalmente, la relación entre ICANN y los organismos que implementaron estas políticas fue informal, pero con el crecimiento mundial de Internet y crecimeinto de la importancia del rol del DNS, se han ido formalizando estos acuerdos. Estos incluyen acuerdos de registries, registrars y con organismos de estándares como el IETF.

Desde el año 2000, ICANN también trabaja para documentar las relaciones que tiene con los administradores de los ccTLD. Estas relaciones son más complejas debido a las diferentes circunstancias (en términos de tipo de organización, desarrollo de políticas, economía, idioma, cultura, entorno legal y relaciones con los gobiernos) de diferentes ccTLD y las organizaciones que los operan. Un factor adicional que debe abordarse es la función, reconocida en el Libro Blanco del Gobierno de EE. UU. Alli se establece que desde Junio de 1998, los gobiernos

nacionales tienen libertad para "gestionar o establecer políticas para sus propios ccTLD".

Varios ccTLD en la región de América Latina y el Caribe han formalizado su relación con ICANN a través de marcos de responsabilidad o mediante un intercambio de cartas.

Estos ccTLDs incluyen

- .cw – Curacao – ICANN Accountability Framework (12 March 2012)
- .an – Netherlands Antilles – ICANN Accountability Framework (23 June 2010)
- .ec – Ecuador – ICANN Accountability Framework (23 June 2010)
- .py – Paraguay – ICANN Accountability Framework (24 June 2009)
- .mx – Mexico – ICANN Accountability Framework (22 June 2009)
- .uy – Uruguay – ICANN Exchange of Letters (24 June 2009)
- .ht – Haiti – ICANN Accountability Framework (24 June 2009)
- .aw – Aruba – ICANN Accountability Framework (2 March 2009)
- .bo – Bolivia – ICANN Accountability Framework (2 March 2009)
- .cr – Costa Rica-ICANN Accountability Framework (25 June 2008)
- .pr – Puerto Rico-ICANN Accountability Framework (26 June 2007)
- .sv – El Salvador-ICANN Accountability Framework (4 June 2007)
- .br – Brazil-ICANN Exchange of Letters (10 May 2007)
- .pa – Panama-ICANN Accountability Framework (Spanish) (4 December 2006)
- .ni – Nicaragua-ICANN Accountability Framework (28 September 2006)
- .gt – Guatemala-ICANN Accountability Framework (5 September 2006)
- .pe – Peru-ICANN Accountability Framework (14 August 2006)
- .hn – Honduras-ICANN Accountability Framework (20 July 2006)
- .no – Norway-ICANN Exchange of Letters (17 July 2006)
- .cl – Chile-ICANN Accountability Framework (24 June 2006)

Colombia no tiene un acuerdo de este tipo con ICANN ni estamos sugiriendo que sea necesario.

Lo que recomendamos es que el equipo de liderazgo .CO se involucre de manera proactiva con ICANN y participe en varios grupos de partes interesadas y en el proceso de políticas según sea necesario. Como mínimo, los representantes del gobierno colombiano y / o .CO deben ser miembros activos de los siguientes:

- El Comité Asesor Gubernamental (GAC, por sus siglas en inglés): este es el foro para que los gobiernos y las Organizaciones Inter Gubernamentales brinden asesoramiento a ICANN sobre cuestiones de política pública, especialmente donde puede haber una interacción entre las actividades o políticas de ICANN y las leyes nacionales o los acuerdos internacionales.
- Organización de Apoyo para Nombres de Código de País (ccNSO): este es el organismo de desarrollo de políticas para una gama limitada de problemas globales relacionados con ccTLD dentro de la estructura de ICANN. Además, proporciona una plataforma para fomentar el consenso, la cooperación técnica y el desarrollo de habilidades entre los ccTLD y facilita el desarrollo de mejores prácticas voluntarias para los administradores de ccTLD.

Además de participar en estos dos grupos dentro de ICANN, sería prudente monitorear los esfuerzos de los siguientes grupos :

- Organización de apoyo para nombres genéricos (GNSO, por sus siglas en inglés): la GNSO es el principal organismo de formulación de políticas para los gTLD. Si bien las decisiones tomadas aquí pueden no tener un impacto directo en .CO, algunas políticas, como la delegación de 2 caracteres en el segundo nivel de nuevos gTLD, la sincronización de la próxima ronda de nuevos gTLD y la resolución de los problemas relacionados con los Nombres Geográficos en el Nivel Superior podrían tenerlo.
- Geo TLD Group: esta asociación voluntaria de TLD en su mayoría de ciudades, aboga por el respeto de los derechos soberanos de las ciudades en el espacio de dominio de nivel superior genérico. Son miembros activos del Grupo de Partes Interesadas del Registro (RySG) y participan en algunos desarrollos de políticas, incluido el Grupo de Trabajo de Procedimientos Subsiguientes y el WT5 sobre nombres geográficos en el Nivel Superior. De la región, .RIO y .LAT son miembros.

Otras organizaciones donde sería conveniente participar son:

- Organización de ccTLD de América Latina y el Caribe (LACTLD): .CO es actualmente miembro y debe continuar participando, ya que es la organización principal para la creación de redes y el intercambio de mejores prácticas entre los operadores de ccTLD en la región.
- Consejo de registros de dominios nacionales de nivel superior europeo (CENTR). .CO actualmente figura como miembro asociado a través de su relación con Neustar. CENTR es una organización ampliamente respetada que fomenta el intercambio de buenas prácticas y la investigación entre sus miembros. Independientemente del proveedor elegido como parte de la licitación, se recomienda encarecidamente la continuación y la posible expansión de la participación directa del MINTC.
- LACNIC - MinTIC es miembro. LACNIC es el registro regional de internet responsable de la distribución de direcciones IP en la región. Las políticas para regir estas distribuciones también se desarrollan como parte de las actividades de LACNIC.

Otros espacios para explorer:

- El Foro de Gobernanza de Internet (IGF): organizado bajo los auspicios de las Naciones Unidas y los países anfitriones, el IGF es una reunión anual de partes interesadas que participan en debates sobre cuestiones de políticas relacionadas con Internet. Si bien no hay resultados negociados ni acuerdos vinculantes, el IGF proporciona un terreno fértil para discutir ideas que pueden tomar forma en otros foros. El programa es bastante diverso y puede haber varios talleres que traten temas de interés vital para .CO, o puede que no haya ninguno. El compromiso debe ser determinado sobre una base anual.
- IGF Colombia - MinTIC y CO Internet SAS son participantes activos en la versión colombiana del IGF. La participación continua ayuda a demostrar a la gente colombiana su compromiso de apoyar este evento y ayuda a aumentar la exposición a posibles registrantes colombianos de nombres de dominio .CO.
- Reunión preparatoria regional para el Foro de Gobernanza de Internet (lacigf) MinTIC fue miembro del Comité del Programa 2018 y la participación debe

continuar, reconociendo que habrá representantes de gobierno en la junta del programa.

RECOMENDACIONES:

- Continuar con la participación en el GAC y la ccNSO. Esto se logra esto asistiendo a 3 reuniones de ICANN al año y a cualquier reunión intercesional relevante.
- Explorar formas de monitorear la política del GNSO de ICANN, ya sea directamente por el personal de MinTIC o indirectamente a través de un requisito para que el proveedor de servicios de registro proporcione dicha supervisión.
- Continuar con la participación en organizaciones regionales de ccTLD, incluyendo LACTLD y CENTR, participando en sus reuniones regulares.
- Continuar participando en las reuniones de LACNIC, Colombia IGF y lacigf.
- Considerar la participación en el IGF sobre una base anual.
- Personalizar el equipo en MinTIC de manera adecuada para garantizar la capacidad de cubrir más de una reunión a la vez o, alternativamente, explore la posibilidad del desarrollo de una Fundación .CO para facilitar la participación ampliada.

2.3. Análisis de coordinación para el desarrollo de políticas relacionadas con el sistema de identificadores únicos de Internet. (ccTLD)

ANALISIS

Si bien CANN está encargada, de conformidad con lo que indican sus estatutos, con el funcionamiento estable y seguro de los sistemas de identificadores únicos de Internet, el desarrollo de políticas que involucren los identificadores únicos (nombres de dominio y direcciones IP) no se realiza exclusivamente enICANN. De hecho, es mejor bifurcar cualquier análisis de desarrollo de políticas entre las direcciones IP y los nombres de dominio debido a las diferencias.

Direcciones IP y desarrollo de políticas

ICANN no tiene un papel directo en el desarrollo de políticas. En su lugar, el desarrollo de políticas se realiza a nivel regional dentro de cada uno de los cinco RIR (AFRINIC, APNIC, ARIN, LACNIC y RIPE NCC) que administran un proceso de desarrollo de políticas abierto. Mientras que los cinco RIR coordinan sus actividades a través de la Number Resource Organization (NRO) por sus siglas en inglés), la NRO en sí misma no tiene ninguna responsabilidad en el desarrollo de políticas. [1] La NRO es principalmente un organismo coordinador que ha ejecutado un Memorando de Entendimiento (MoU) con ICANN para el establecimiento de la Address Supporting Organization (ASO). La responsabilidad exclusiva de la ASO es "asesorar a la Junta Directiva de ICANN con respecto a cuestiones de políticas relacionadas con la operación, asignación y administración de direcciones de Internet". [2]

La mayoría de los operadores de registros de TLD tienen un compromiso directo limitado con los RIR, sin embargo, algunos ccTLD se han involucrado activamente con RIR y los Registros locales de Internet (LIR) en relación con la promoción del espacio de direcciones IPv6. Un ejemplo de ello es el operador de ccTLD de Brasil NIC.BR. [3] Si bien la participación activa en el desarrollo de políticas de RIR no es un requisito previo, es un requisito que cualquier administrador de ccTLD tenga un conocimiento práctico de la comunidad de RIR y tenga una política de IPv6 bien pensada y documentada para la administración del ccTLD.

Desarrollo de políticas de nombres de dominio para ccTLD

Al igual que el proceso de desarrollo de políticas de los RIR y las direcciones IP, ICANN tiene un rol limitado en relación con el desarrollo de políticas para un ccTLD. Si bien ICANN ha actuado en relación con las redelegaciones de ccTLD, no existe ninguna disposición en los estatutos de ICANN ni en las leyes nacionales que indique que ICANN debe imponer políticas a los ccTLD. Sin embargo, ha habido casos en los que los Administradores de ccTLD adoptaron voluntariamente las políticas de consenso elaboradas dentro de ICANN que se consideraron de mayor interés para las comunidades locales, como por ejemplo en relación con la Política Uniforme de Resolución de Disputas (UDRP). Si bien ICANN adoptó la UDPR como una política de consenso legalmente vinculada a todos los gTLD regulados por la ICANN [4], muchos ccTLD adoptaron voluntariamente un mecanismo de resolución alternativa de disputas (ADR) similar a la UDRP. [5]

Dado el rol limitado de ICANN en reglas para los ccTLD, se han establecido varias Organizaciones Regionales de Dominio de Nivel Superior (RTLDO: Regional Top Level Domain Organizations, por sus siglas en inglés) para proporcionar un liderazgo y coordinación más localizados en cada región. Estos RTLDO incluyen CENTR (Europa), LACTLD (América Latina y el Caribe) y APTLD (Asia Pacífico). Si bien muchos ccTLD participan en estos RTLDO y dentro de la ccNSO de la ICANN, en la mayoría de los casos, el desarrollo de políticas comienza y termina dentro de la jurisdicción nacional del ccTLD. Teniendo en cuenta esta realidad, la mayoría de los Administradores de ccTLD tienen recursos dedicados para promover el modelo de consenso bottom-up o de abajo hacia arriba de las múltiples partes interesadas (multistakeholder) dentro de cada jurisdicción nacional.

Políticas específicas de ccTLD

A pesar de la naturaleza local del desarrollo de políticas, han surgido áreas temáticas comunes dentro de los ccTLD. Estas incluyen políticas en las áreas de: Privacidad; Uso aceptable / anti-abuso; Mecanismos de protección de derechos (RPM), como la UDPR y la Suspensión rápida uniforme (URS); Declaración de práctica de DNSSEC; Registro de servicios de directorio (RDDS) / WHOIS; y ciclo de vida del nombre de dominio.

.CO Internet SAS ya ha implementado varias de estas políticas en relación con su operación existente del .CO ccTLD. Uno de los desafíos para el .CO como un TLD híbrido (enfocado a gTLD y ccTLD) es equilibrar las políticas de gTLD de ICANN y las desarrolladas dentro de la comunidad local.

RECOMENDACION:

El gobierno de Colombia debe exigir a todos los oferentes que detallen su experiencia relevante en el proceso de desarrollo de políticas en ICANN; RTLDO; y niveles locales de ccTLD. Cada oferente también debe indicar si adoptará o realizará cambios sustanciales a las políticas existentes de .CO publicadas en el sitio web del Administrador de ccTLD en https://www.cointernet.com.co.

Como mínimo, cada oferente debe abordar las siguientes políticas: Privacidad; Uso aceptable / anti-abuso; Mecanismos de protección de derechos (RPM), como por ejemplo UDPR y URS; Declaración de práctica de DNSSEC; Registro de servicios de directorio (RDDS) / WHOIS; y ciclo de vida del nombre de dominio.

2.4. Análisis de la institucionalidad del sistema de nombres de dominio, atribuciones y funciones. (ccTLD)

ANÁLISIS

Como se analiza con más detalle en 2.5, hay una gran variedad de modelos de cómo se controlan y operan los ccTLD. Tampoco existe un marco técnico uniforme, ya que algunos ccTLD operan su propia infraestructura técnica y otros lo subcontratan a un tercero.

A pesar de que no hay dos ccTLD gobernados de la misma manera, los modelos de gobierno generalmente se dividen en 3 categorías diferentes: pública, privada y académica.

Modelo público

En este modelo, el gobierno, a través de un organismo gubernamental o regulador, actúa como administrador del ccTLD y realiza todas las funciones de supervisión, así como las operaciones diarias. Algunos también pueden operar la infraestructura, mientras que otros subcontratan esta función a un tercero.

Modelo privado

Ya sea a través de la historia (ya que la administración de los ccTLD se atendió por primera vez) o a través de una decisión consciente, la mayoría de los ccTLD son operados por entidades privadas en beneficio del país. El administrador diario del ccTLD puede ser una empresa privada, una asociación o una fundación. En este modelo, todas las operaciones del ccTLD son manejadas por un proveedor de servicios externo supervisado por el gobierno.

Modelo académico

En este modelo, el ccTLD es parte de una institución académica que podría ser pública o privada.

Asociaciones regionales de ccTLD

Independientemente del tipo de modelo de gobierno empleado, muchos ccTLD eligen participar en una de las asociaciones regionales de operadores de ccTLD. Estos grupos brindan oportunidades de creación de redes, intercambio de mejores prácticas, creación de capacidades, investigación y promoción de la comunicación y cooperación entre los operadores de ccTLD. Cada una de estas organizaciones lleva a cabo al menos una reunión importante por año con algunas que realizan talleres intercesionales más pequeños y otras reuniones. Las principales organizaciones incluyen:

- Africa Top Level Domain Organization (AfTLD)[33]
- Asia Pacific Top Level Domain Association (APTLD)[34] – Neustar es miembro
- Council of European National Top-Level Domain Registries (CENTR)[35] – Neustar es miembro
- Latin American and Caribbean ccTLDs Organization – LACTLD) - .CO Internet SAS es miembro y Neustar es afiliado

La participación primaria de .CO debe continuar a través de LACTLD si proporcionan la información más relevante para la región. Como muchos proveedores de servicios de registro son miembros de las cuatro asociaciones regionales, .CO Internet y MinTIC también deberían beneficiarse de estas membresías.

Otros foros donde .CO puede involucrarse

ICANN DNS Forum[36] y LAC DNS Forum

En los últimos años, hemos visto una proliferación en los foros de DNS patrocinados por la ICANN. Inicialmente, se lanzó para ayudar a la ICANN a llegar a las partes interesadas que no asisten a una reunión de la ICANN, y se han convertido en una parte habitual del ritmo de las reuniones de la ICANN. A diferencia de las 3 reuniones

[33] http://www.aftld.org/
[34] https://www.aptld.org/
[35] https://centr.org/
[36] https://www.icann.org/ids

grandes de la ICANN por año, estas sesiones tienen una duración más corta y tienden a centrarse en aspectos más técnicos. Las reuniones regionales, incluido el Foro de DNS de LAC se llevan a cabo una vez al año y el Foro de DNS de LAC se lleva a cabo normalmente en el otoño (la fecha para 2019 no se ha establecido). En 2019, la ICANN probó un nuevo enfoque para el Foro de DNS de ICANN al colocarlo junto con otras 3 reuniones: la Cumbre de GDD de la ICANN, el Taller de Operadores de Registro y el DNS OARC. Este esfuerzo pareció funcionar con buena asistencia y 3 días de programación convincentes. Intel sugiere que la reunión del próximo año se lleve a cabo en París, Francia

LAC-i-Roadshow

Ahora en su quinto año, LAC-i-Roadshow, un proyecto creado como parte de la Estrategia de América Latina y el Caribe, viaja a través de la región para llegar a las partes interesadas regionales sobre temas clave relacionados con el sistema de nombres de dominio. Si bien no es tan técnico como los foros de DNS, podría tener sentido que .CO participe en una iteración convenientemente localizada de este esfuerzo o que pueda albergar una futura reunión en Colombia.

The Domain Name Association

La asociación de nombres de dominio (DNA) representa los intereses de la industria de nombres de dominio. Sus miembros son grupos, empresas e individuos involucrados en la provisión, el soporte y la venta de nombres de dominio. Esto incluye organizaciones tales como registros de nombres de dominio, registradores, revendedores y proveedores de servicios de registro, así como aquellos interesados en la denominación de Internet y la innovación con nombres de dominio. La misión de DNA es promover los mejores intereses de la industria de los nombres de dominio al promover el uso, la adopción y la expansión de los nombres de dominio como la herramienta principal para que los usuarios naveguen por Internet. Neustar es miembro, al igual que algunos operadores de ccTLD (.CA, .AT, FM, NZ y .UK). El enfoque real de la asociación parece estar en la promoción de nuevos gTLD. El futuro del ADN no está claro con preguntas en curso sobre su capacidad de supervivencia financiera. No recomendaríamos participar en este momento.

RECOMENDACIONES

- Continuar la participación activa en LACTLD
- Considerar la posibilidad de participar en el Foro de DNS de ICANN y en el Foro de DNS de LAC cuando y donde sea organziado. Gran parte de esto será impulsado por la ubicación y la agenda.

2.5. Identificación y análisis de la operación del modelo de gestión y mantenimiento de dominios ccTLD.

ANÁLISIS

Existe una amplia variedad de modelos sobre cómo se gobiernan y operan los ccTLD. No existe un marco técnico uniforme, ya que algunos ccTLD operan su propia infraestructura técnica y otros la subcontratan a un tercero.

A pesar de que no hay dos ccTLD gobernados de la misma manera, los modelos de gobierno generalmente se dividen en 3 categorías diferentes: público, privado y académico.

Modelo público

En este modelo, el gobierno, a través de un organismo gubernamental o regulador, actúa como administrador del ccTLD y realiza todas las funciones de supervisión, así como las operaciones diarias. Algunos también pueden operar la infraestructura, mientras que otros subcontratan esta función a un tercero. Este modelo viene acompañado de eficiencias, ya que las decisiones sobre operaciones y políticas están a la entera discreción del Gobierno. Si bien puede haber consultas públicas sobre políticas y operaciones, al final del día, la decisión está en manos del gobierno. Para operar un modelo como este, la agencia gubernamental que supervisa el ccTLD debe tener suficiente experiencia interna para operar los ccTLD.

Modelo privado

Ya sea a través de la historia (ya que la administración de los ccTLD fue realizada por primera vez) o a través de una decisión, la mayoría de los ccTLD son operados por entidades privadas en beneficio del país. El administrador del ccTLD puede ser una empresa privada, una asociación o una fundación. En este modelo, todas las operaciones del ccTLD son manejadas por un proveedor de servicios externo supervisado por el gobierno. La forma en que se desarrollan las políticas varía pero, en algunos casos, el gobierno aún tiene la última palabra. Dentro de este modelo,

también hay variaciones, ya que algunos adoptan un enfoque de múltiples partes interesadas como CGI.br y AuDA, mientras que otros se ejecutan estrictamente como empresas privadas con fines de lucro.

Modelo académico

En este modelo, el ccTLD es parte de una institución académica que podría ser pública o privada. Así es como se manejó .CO previamente.

.CO es operado actualmente por .CO Internet SAS en nombre del Gobierno de Colombia. Entendemos que, aparte de la supervisión del contrato, no hay representantes del gobierno colombiano involucrados en la operación diaria del ccTLD. Para ayudar a desarrollar la capacidad interna y una mejor supervisión, sugerimos con el tiempo que MinTIC explore la posibilidad de adoptar un modelo de gobierno que se parezca más a CGI.br o AuDA.

Estos dos modelos de gobernanza incluyen la participación de varias partes interesadas en las decisiones políticas y la gobernanza del ccTLD. AuDA tiene más de un modelo de membresía para las elecciones a la Junta, mientras que el Comité Directivo de CGI.br es designado por las partes interesadas. Ambos abarcan las responsabilidades operativas que tiene el día a día de .CO Internet SAS pero con una ampliación de la participación externa para ayudar en la formulación de políticas y la supervisión organizativa. El cambio del modelo .CO Internet SAS a uno como CGI.br o AuDA no sería complicado, pero requeriría un análisis adicional por parte de MinTIC. Un aspecto atractivo de cada uno de estos modelos es que ambas organizaciones participan activamente en la comunidad que apoya los esfuerzos locales para aumentar el uso de Internet y, como resultado, los registros de dominios aumentan. Esta capacidad de hacer buenas acciones en la comunidad tiene impactos positivos en la percepción del ccTLD.

Tendencias en la operación de ccTLD

Otro componente a considerar son las tendencias que estamos viendo en las operaciones de ccTLD. Además de algunos países que buscan fortalecer su control sobre Internet, observamos una liberalización continua de los requisitos de elegibilidad para el registro, el cambio de marca de los ccTLD para atraer a una

audiencia más amplia y, en algunos casos, los requisitos de verificación del solicitante para agregar un nivel de seguridad a el ccTLD.

Tendencia – Políticas de registro abiertas vs cerradas

El modelo de registro abierto permite que los dominios sean comprados y utilizados por cualquier persona u organización. El modelo cerrado es protector e impone reglas con respecto a la presencia física en el país relevante al que pertenece el ccTLD. El modelo de gobierno abierto se está volviendo más popular a medida que fomenta más compras de ccTLD y, por lo tanto, contribuye a la economía del país. Existen algunas desventajas relacionadas con el modelo de registro abierto, incluida la pérdida de identidad del país, ya que el ccTLD se convierte en una marca global y el potencial de que las empresas offshore aprovechen su "presencia" aparentemente física en un país, implícita en su uso del ccTLD de ese país, genrea confusiones a consumidores desprevenidos mientras se benefician económicamente de ese país, evitando al mismo tiempo el cumplimiento de sus leyes nacionales.

La razón principal para políticas de registro más estrictas es que, como si fuera una bandera o un pasaporte que representa la "marca" de un país, nos tranquiliza con respecto a la fuente de un producto o persona. También un ccTLD tiene un significado más profundo que otros nombres de dominio . En el modelo cerrado, un ccTLD solo está disponible para individuos y organizaciones con presencia física en el país.

Como .CO ya tomó la decisión de ser un ccTLD abierto, revertir esta decisión tendría un impacto devastador en los volúmenes de registro.

Tendencia – Verificación de registro

Como se describe en un documento de investigación del CENTR, existe una clara tendencia entre los operadores de ccTLD para verificar los registrantes de nombres de dominio en sus ccTLD. Son notables los esfuerzos de Estonia, Dinamarca, República Checa, Bulgaria, Países Bajos y Alemania. Aparte de los Países Bajos y Alemania, los otros operadores confían en un esquema de identidad digital nacional subyacente para implementar su servicio. Alemania está integrando un servicio de identidad federado llamado ID4me.

Sin una necesidad específica de implementar dicha verificación, creemos que es mejor observar esta tendencia y no implementarla en este momento

Tendencia - El cambio de marca de los ccTLD se vuelve más atractivo en el mercado global

La decisión de .CO de hacer que los dominios estén disponibles para el mercado global provocó una tendencia que continúa en la actualidad. Un enfoque para aumentar los registros de dominios es cambiar la marca o cambiar el significado de los ccTLD por parte del operador de registro. El ccTLD .PW (Palau) cambió su nombre a Professional Web, y el ccTLD .LA (Laos) se adoptó para referirse a "L.A.", el acrónimo común de la ciudad de Los Ángeles, California. El reciente auge en la industria de la Inteligencia Artificial aumentó los registros en el ccTLD .AI de Anguila. A medida que más ccTLD están adoptando este enfoque, se tiene el potencial de aumentar la competencia con el tiempo. Al igual que la ola de nuevos gTLD ha brindado más opciones a aquellos que buscan una alternativa a los TLD heredados, algunos de estos ccTLD recientemente reutilizados pueden llegar a un acuerdo con los posibles solicitantes de registro.

Tendencia - Colapsos de registros jerárquicos.

Los registros de ccTLD que buscan aumentar los ingresos y el uso local han ampliado las posibilidades de registro para permitir dominios más cortos y fáciles de recordar a través de registros de dominio de segundo nivel donde antes solo era posible realizar registros de tercer nivel; es decir, antes de que solo se pudiera registrar NAME.CO.UK o NAME.NET.UK, mientras que ahora se puede registrar NAME.UK (Reino Unido). Australia y Nueva Zelanda han adoptado estrategias similares.

RECOMENDACIONES

Se sugiere en etapas posteriores, explorar la incorporación de características de .CGI.br y AuDA en la operación y gobierno de .CO.

Se sugiere mantenerse al tanto de las tendencias actuales en el mercado de ccTLD para determinar y el impacto competitivo en .CO.

2.6. Análisis de la infraestructura mínima necesaria para la administración del ccTLD (hardware y software)

Consideraciones generales

El éxito de la transición al nuevo administrador dependerá en gran medida de su capacidad para gestionar un nuevo TLD dentro de su infraestructura técnica existente (tecnología y procesos). Para minimizar el riesgo en la transición, el proponente debe demostrar experiencia específica, reciente y continua con diversas operaciones de TLD. Esta diversidad debe ser evidente dada la experiencia del administrador que propone, con la misma infraestructura técnica, dominios con diferencias en las políticas de delegación, precios, sistemas contables, sistemas de seguridad y relación con los registradores.

La política para el ccTLD .CO, aprobada por la Resolución 001652 del 30 de julio de 2008, presenta complejidades en la administración del dominio que son, entre otras, las siguientes:

- Registro de dominio en dos niveles diferentes (segundo y tercer nivel)
- Registro de dominios para usuarios restringidos directamente por el administrado por el ccTLD .CO
- La creación de una red de registradores a través de un proceso de acreditación específico para el ccTLD .Co

Por esta razón, el proponente debe tener al menos una experiencia reciente, específica, individual y en la operación técnica de al menos tres (3) TLD, cada uno de al menos 500,000 nombres de dominio en tamaño, para asumir la responsabilidad de administrar el ccTLD. Co, asegurando un crecimiento adecuado en el número de registros de ccTLD .CO.

El concesionario (administrador) debe tener al menos dos experiencia específica, individual y particular en la operación técnica de al menos 1,000,000 nombres de dominio bajo un ccTLD que tenga varios niveles de registro.

Dicho TLD debe tener al menos 3 de los siguientes elementos específicos de políticas y operaciones:

- Localización de datos
- Conformidad con las Reglas de Privacidad
- Conformidad con los requisitos de Nexus y las operaciones locales en el país que utilizan equipos en el país.

Los proponentes deben tener esta experiencia mínima, como lo reconoce ICANN y las expectativas de crecimiento para el ccTLD .Co:

El concesionario debe tener al menos dos experiencias específicas, individual y más de cinco (5) años en la operación del protocolo EPP en registros THICK con logro consecutivo de Acuerdos de Nivel de Servicio SLA y sin tiempo de inactividad no planificado en los últimos 5 años.

El concesionario debe haber realizado una transición exitosa, de un operador de registro a otro, un operador de registro no relacionado o de propiedad no beneficiosa, al menos 5 TLD con más de 1,000,000 de nombres y zonas firmadas por DNSSEC. (Las migraciones de la plataforma interna no se consideran transiciones, para los propósitos de esta definición)

Es factible para el proponente implementar la solución de back-end técnica utilizando servicios basados en la nube.

ALCANCE DE LOS SERVICIOS TÉCNICOS Y SOLUCIONES

El proveedor debe administrar el dominio cctld .CO con un conjunto completo de servicios de registro. Como parte de su propuesta, el proveedor debe proporcionar una descripción de su enfoque para entregar todos los servicios incluidos en el alcance.

El proveedor debe cumplir con todas las pautas emitidas por MINTIC (existentes o futuras), que incluyen, entre otras, cuestiones tales como seguridad, acreditación de registradores, compartiendo información y permitiendo el acceso de MINTIC a los sistemas, etc.

SISTEMA DE REGISTRO COMPARTIDO

El proveedor debe proporcionar servicios relacionados con la provisión y el mantenimiento del Sistema de Registro Compartido ("SRS") y el acceso del registrar al sistema, que incluye, pero no se limtia a:

a. Infraestructura requerida para un sistema de registro estable y soporte de acceso equivalente al sistema de registro compartido para todos los registrars
b. Sistema de registro escalable y confiable que incluye hardware y equipos y soluciones de software;
c. Soporte de registro Thick registry usando el estándar Extensible Provisioning Protocol (‘EPP’);
d. Infraestructura segura con capacidades adecuadas de respaldo / falla / recuperación de desastres, sistemas de seguridad redundantes y capacidades de equilibrio de carga para evitar violaciones de seguridad, ataques al sistema y problemas de sobrecarga del sistema;
e. Arquitectura de sistemas, servicios prestados y metodologías de mantenimiento para cumplir con los estándares mínimos requeridos para soportar un dominio de la escala y el tamaño como el registro .co;
f. Software de registro personalizado para satisfacer las necesidades políticas, comerciales y lingüísticas únicas del registro .co;
g. Provisión de un kit de herramientas de registro donde el proveedor debe proporcionar a todos los registradores un kit de herramientas de registro con especificaciones técnicas y documentación suficientes para ayudar a los registradores a desarrollar software de acceso al registro; y
h. Preparar y administrar las pruebas operativas y la evaluación ("OT&E") a los registrars, a medida que preparan y validan sus sistemas.

SERVICIOS DNS

El proveedor debe proporcionar servicios del Sistema de nombres de dominio (‘DNS’), incluida la generación y propagación del archivo de zona. Los servicios que debe proporcionar el proveedor deben incluir, entre otros, los siguientes:

a. Resolución del dominio .co asegurando la disponibilidad de los servidores de nombres autorizados .co y la precisión de la resolución de datos de la zona .co;
b. La diversidad de resolución de DNS y la infraestructura que debe operar el proveedor debe ser compatible con la diversidad de software en el software de resolución y la diversidad en todo el hardware utilizado;

c. Servidores DNS distribuidos geográficamente para cumplir con los estándares de SLA con un mínimo de 2 servidores de resolución en Colombia con accesibilidad diversa para garantizar la continuidad / redundancia;

d. La infraestructura de DNS debe utilizar múltiples proveedores de DNS y debe ubicar físicamente los servidores de nombres de dominio .co TLD dentro de los límites geográficos de Colombia;

e. Sistema de resolución escalable para manejar el número existente de nombres y el crecimiento proyectado, las cargas de consultas de DNS existentes, incluidos los picos normales y el crecimiento proyectado, los ataques y el tráfico generado por virus, gusanos y correo no deseado, ataques simultáneos en la red (geográficamente dispersos), etc. y

f. El sistema de resolución segura con capacidad de mitigación de Denegación de servicio distribuido ("DDoS") y debe ser compatible con Domain Name System Security Extensions ("DNSSEC"), Protocolo de Internet versión 6 ("IPv6") y Nombres de dominio internacionalizados ("IDNs").

SERVICIOS WHOIS

El proveedor debe proporcionar servicios WHOIS incluyendo, pero no limitado a:

a. Puerto 43 y WHOIS basado en la web;

b. Hardware y software de WHOIS;

c. Capacidades de búsqueda de WHOIS;

d. Entrega de datos de WHOIS configurable;

e. Soporte para información de contacto multilingüe en idioma local;

f. Debería existir un mecanismo de seguridad adecuado para evitar el abuso de los mineros de datos (data miners)

SOLUCIONES DE SOFTWARE

El proveedore debe proveer las herramientas de software requeridas, soluciones, y servicios incluyendo pero no limitado a:

g. El protocolo de registro de EPP en modo RFC compliant y el proveedor debe seguir las novedades de cualquier actualización adicional a los estándares de EPP

h. Registrar Toolkit (‘RTK’) que permite a los registradores construir sus propias interfaces en el sistema de registro;

i. Registro continuo de actualizaciones near-real-time DNS a una red de servidoes DNS;

j. Software de registro configurable que puede satisfacer todas las necesidades técnicas y de políticas de dominio .co, así como proporcionar opciones de precios flexibles para programas de marketing;

k. Cumplimiento de las normas aplicables publicadas por ICANN'y otros organismos relacionados, como el Grupo de Trabajo de Ingeniería de Internet ('IETF'), la Junta de Arquitectura de Internet ('IAB') y el Comité de Seguridad y Estabilidad ('SSAC');

l. Herramienta de administración basadas en web y una cuenta de registro asociada para facilitar la supervisión de todos los dominios y objetos en el registro .co. La herramienta y la cuenta deben permitir funciones que incluyen, entre otras, la capacidad de buscar y alterar cualquier registro en el registry, lo que permite controlar todos los dominios .co y una cuenta para administrar los nombres reservados utilizados por el registro; y

m. Respalde tecnologías nuevas y emergentes, desarrolle características y capacidades clave del producto e incorpore nuevas reglas, estándares y prácticas comerciales cuando sea necesario.

INSTALACIONES Y SISTEMAS

Se debe solicitar al proveedor que configure 2 instalaciones de centros de datos distintas en Colombia para la administración de las operaciones de registro de .co. Se debe solicitar al proveedor que configure las instalaciones físicas, equipos y sistemas requeridos, el ancho de banda de la red y la mano de obra en estas dos instalaciones del centro de datos.

El proveedor debe implementar el hardware requerido y llevar a cabo la administración de las instalaciones y los sistemas, incluyendo pero no limtado a:

a. Facilidades fisicas;

b. Hardware y equipo;

c. Centro de operaciones de red ("NOC") con herramientas de monitoreo para generar alertas para cualquier problema con el sistema de registro y su red;

d. Capacidad del centro de datos y ubicaciones;

e. Redundancia y tolerancia a fallos en los sistemas; y

f. Conectividad y servicios de internet.

SEGURIDAD DEL SISTEMA, SEGURIDAD FISICA Y CONFIABILIDAD

El proveedor debe ser responsable de proporcionar y ejecutar los procesos y metodologías de estabilidad operativa, confiabilidad y seguridad, incluyendo pero no limitado a:

a. Monitoreo 24x7x365 del Sistema de registro y red por parte de un Network Operations Centre (‘NOC’)
b. Cumplimiento de las normas aplicables publicadas por organismos tales como IETF o ICANN, IAB y SSAC, que están diseñados para garantizar la interoperabilidad de Internet y mejorar la experiencia del usuario
c. Protección contra software malicioso, ataques DDoS, data tampering, intrusiones, manipulación de datos y otras interrupciones en las operaciones
d. Implementar Sistemas de Information Security Management
e. Seguridad de la red
f. Políticas de seguridad de la información
g. Seguridad física
h. h. Personal con capacidad técnica, experiencia y experiencia para operar el registro con el fin de mantener y mejorar los niveles actuales de rendimiento
i. i. Procesos de revisión detallados para la integración de nuevos requisitos, así como el seguimiento del cumplimiento posterior y la revisión periódica.

PROCEDIMIENTOS DE RECUPERACIÓN DE DESASTRES, RESPALDO DE DATOS Y RECUPERACIÓN DEL SISTEMA

El proveedor debe proporcionar servicios para la recuperación de desastres, la copia de seguridad de datos y los procedimientos de recuperación del sistema, incluidos, entre otros:

a. Procedimientos completes de disaster recovery;
b. Backups y réplicas del registro;
c. Sistemas redundantes;
d. Disponibilidad de backup Software/Operating System/Hardware;
e. Mitigaciones de riesgo commercial y técnico;
f. Procedimientos para sistemas de restauración a operación en el evento de uno Procedures for Restoring System to operation in Event of corte de servicio; and
g. Procedimientos para mantenimientos planificados y preventivos.

IMPLEMENTACIÓN DE DNSSEC Y CONECTIVIDAD DE IPv6

El proveedor debe implementar los siguientes servicios desde el inicio de las operaciones de registro de .co:

a. DNSSEC;
b. Conectividad IPv6 connectivity (ej: rutas y direccionamiento) entre registrars y el registro;
c. Proveeer servicios DNS y servicios WHOIS con redes de IPv6

SOLUCIONES DE SOFTWARE, HERRAMIENTAS DE MONITOREO

Características del Software

Las siguientes funciones y procedimientos de software deben implementarse en las operaciones del registro .co:

a. EPP registry protocol en modo RFC-compliant;
b. Registrar Toolkit (‘RTK’) que permite a los regisrtrars crear sus propias interfases dentro del sistema de registro
c. Open-source Relational Database Management System (‘RDBMS’) con Multi-Version Concurrency Control (‘MVCC’);
d. Sistema de registro que puede escalar hasta 10 millones de nombres de dominio sin intervención y sin cambio de arquitectura;
e. Actualizaciones del Near-real-time DNS de una red distribuida de DNS
f. Multiples proveedores de DNS;
g. Registro de software configurable que sea capaz de acomodar todas las reglas y necesidades técnicas, así como proveer un pricing flexible para programas;
h. Servicios WHOIS con opciones de resultados configurables;
i. Capacidad de prover servicios IPV6
j. Sistema de registro que puede escalar hasta 10 millones de nombres de dominio sin intervención sin cambio de arquitectura;
k. Alojamiento y mantenimiento del sitio web de registro .co; and
l. Un Centro de operaciones de red ("NOC") utiliza una serie de herramientas de monitoreo para generar alertas para cualquier problema con el sistema de registro y su red.

Modelo Registry-Registrar y Protocolo

1. Extensible Provisioning Protocol (‘EPP’):

El protocolo de software que se usa en el ccTLD .co Shared Registration System (‘SRS’) es el Extensible Provisioning Protocol (‘EPP’).

2. Modelo Registry-Registrar:

El ccTLD .co debe mantener un registro THICK que centralice al registrante autoritativo y otros contactos en el registro.

3. Acreditaciones de Registrar:

Para vender nombres de dominio .co, los registradores deben completar un proceso de autorización que establece acuerdos legales entre el proveedor y el registrador, y comprueba la capacidad técnica del registrador para interactuar con el registro del PPE y el departamento de soporte técnico.

Para obtener la certificación técnica, se requiere que cada registrador cree un cliente EPP para interactuar con el servidor .co SRS. Todos los registradores cuentan con un kit de herramientas de registrador ("RTK"), que incluye varias versiones de código (por ejemplo, Perl, Java, etc.) que se pueden usar en la creación del cliente.

A cada registrador se le proporciona acceso a un entorno de prueba y evaluación operativas ("OT&E") que se utiliza para probar la implementación de los registradores de sus clientes. Se requiere que cada registrador pase una prueba OT&E para evaluar su habilidad para interactuar con el registro, su capacidad para enviar y recibir comandos del registro, completar transferencias, etc.

3. Parte 3 (Ref: 2.2.2.1) Análisis de políticas de DNS establecidas por ICANN/IANA.

3.1. Análisis de los aspectos de seguridad y temas relacionados con los datos de registro de los nombres de dominio de ccTLD.

ANALISIS:

La seguridad es obviamente una preocupación primordial en relación con la operación del .CO ccTLD. Sin embargo, no hay una manera uniforme de que este criterio se haya incorporado a las RFP. Este análisis buscará revisar el enfoque adoptado en relación con varias ofertas de RFP recientes y documentos relacionados para proporcionar un marco para que el gobierno de Colombia tome una decisión final.

A. Public Interest Registry (PIR)

Si bien algunas ofertas de RFP, como el ccTLD .AU, proporcionaron una lista detallada de temas de seguridad para que sean respondidos (veinticuatro en total), otros proporcionan un enfoque temático de alto nivel para la seguridad que permite a los oferentes proporcionar el nivel de detalle necesario. El enfoque de PIR fue hacia esta última opcioón, haciendo solo dos preguntas de alto nivel. Sin embargo, es importante tener en cuenta que el PIR requería que los encuestados abordaran los problemas de seguridad tanto en relación con el Sistema de Registro Compartido (SRS) como las funciones auxiliares relacionadas con la lógica empresarial. A continuación se enumeran las dos preguntas específicas que PIR incluyó en su RFP:

> *Security Q5.21. Base de datos del registrante y operaciones de registro. Describa las capacidades y los procedimientos técnicos y físicos que propone para evitar los ataques e intrusiones en el sistema, la manipulación de datos y otras interrupciones de las operaciones. Incluya en su descripción detalles sobre la evaluación de riesgos; la implementación y evaluación de controles; la seguridad de la base de datos del registrante; y otros elementos críticos de la infraestructura de operaciones de registro para mitigar los riesgos de la exposición de información no autorizada, la interferencia con el intercambio oportuno y preciso de información entre el registro y los registradores, la interferencia con la respuesta oportuna y precisa de los servidores de*

nombres a las consultas de DNS y otras amenazas a la integridad y continuidad del funcionamiento del registro.

Q6.17. Respondiendo a los controles de seguridad de la organización. Describa las políticas, procedimientos y otras características de los controles de seguridad que su organización ha implementado para detectar y combatir el acceso no autorizado a instalaciones o recursos, incluidos los ataques de ingeniería social, como el phishing; proteger contra y mitigar los ataques DDoS; y garantizar la seguridad física de los centros de datos, equipos, comunicaciones, servicios públicos y otras infraestructuras críticas.

Si el gobierno de Colombia aceptara el enfoque de alto nivel para solicitar información de los oferentes con respecto a sus sistemas, dependiendo de la experiencia técnica de los evaluadores, puede ser necesario proporcionarles una lista de criterios enumerados en la misma línea que el. AU RFP para asegurar que todos los aspectos de seguridad hayan sido abordados.

B. .US RFP

El Gobierno de los Estados Unidos (USG) en la RFP de los Estados Unidos siguió el enfoque de PIR descrito anteriormente: Sistemas seguros; Notificaciones del sistema seguro; Datos seguros; Plan de Seguridad Informática; y Director de Seguridad, ver Anexo A para el texto completo. La diferencia clave entre PIR y las RFP de Estados Unidos, fue el requisito de USG de que un licitador designe a un Director de Seguridad como Personal Clave.

C. .IN RFP

NIXI en su RFP para .IN realizó un análisis más profundo que PIR o el USG, describiendo trece criterios como se detalla en el Anexo A. Algunos de los criterios adicionales que incluyó NIXI fueron el funcionamiento de un Centro de Operaciones de Red (NOC) para monitorear el sistema y la red de registro y un requisito para cumplir con las leyes de “localización de datos” de la India. También hubo algunos problemas específicos de seguridad relacionados con el nombre de dominio, por ejemplo, un mecanismo para mitigar la "captura" de nombres de dominio (9.6.11) y una disposición para "restringir a los registradores para el bloqueo ilegítimo de nombres de dominio" (9.6.12).

D. .AU RFP

AuDA realizó el análisis más profundo de los requisitos de seguridad en relación con la RFP .AU definió veinticuatro puntos de datos de seguridad que se detallan a continuación:

3.1 Política de seguridad
3.2 Gestión de riesgos de seguridad de la información
3.3 Servicios de tecnología de la información subcontratados
3.4 Funciones y responsabilidades del operador de registro
3.5 Documentación de seguridad de la información
3.6 Acreditación del sistema
3.7 Monitoreo de la seguridad de la información
3.8 Incidentes de seguridad cibernética
3.9 Seguridad física
3.10 Seguridad del personal
3.11 Infraestructura de comunicaciones
3.12 Sistemas y Dispositivos de Comunicaciones.
3.13 Estrategias para mitigar los incidentes de seguridad cibernética
3.14 Seguridad del producto
3.15 Seguridad de los medios
3.16 Seguridad del software
3.17 Seguridad del correo electrónico
3.18 Control de Acceso
3.19 Administración Segura
3.20 Seguridad de la red
3.21 Criptografía
3.22 Seguridad entre dominios
3.23 Transferencias de datos y filtrado de contenido
3.24 Trabajando fuera del sitio

Si bien puede existir el deseo de incluir todos los criterios enumerados en la RFP de .AU bajo los auspicios de maximizar la seguridad natural, el gobierno de Colombia debe tener en cuenta el hecho de que necesitará contar con el personal necesario para revisar todas las respuestas en una línea de tiempo muy apretado. Sin embargo, la inclusión de otros criterios de selección puede limitar el número de respuestas que deberán revisarse por completo. Además de esta lista de criterios

enumerados, AuDA incluía una disposición separada en el paquete de ofertas de RFP que requería que el oferente ganador *"tenga un acuerdo establecido (aceptable para auDA) con el Equipo de Respuesta de Emergencia Informática del Gobierno de Australia, el Fiscal General (CERT Australia) y el Acuerdo incluirá obligaciones continuas por parte del proveedor para comprometerse con el CERT Australia en relación con la seguridad cibernética y los problemas de protección de datos"*. Si el gobierno de Colombia opera un CERT nacional o participa en un CERT regional, es posible que desee incluir una disposición similar en el acuerdo de registro final. En el Anexo A se incluye una lista completa de estos requisitos adicionales.

E. ICANN

ICANN ha comenzado recientemente a incorporar la disposición de seguridad estándar en varios acuerdos y documentos que produce, incluido el Anexo de procesamiento de datos de RRA y las Preguntas técnicas de MSA. El documento de preguntas técnicas de MSA es probablemente el más constructivo. Este es un documento que ICANN ha preparado para los operadores de registro de gTLD existentes que buscan cambiar de proveedor de infraestructura de registro bac-kend que actualmente no operan "uno o más registros de nuevos gTLD"[1]

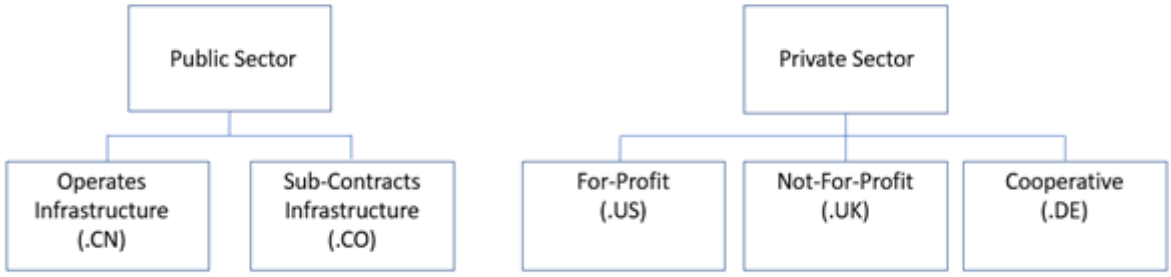
RECOMENDACIONES:

Se recomienda que el gobierno de Colombia modele cualquier pregunta relacionada con la seguridad después del enfoque actual utilizado por ICANN en relación con el MSA (Acuerdo de Subcontratación de Materiales, consultar el Anexo A). Este enfoque establece el equilibrio adecuado entre el detalle de la RFP de .AU y la de el PIR y el enfoque mas liviano de la RFP de .US. También se recomienda que las preguntas se incrementen con los requisitos / necesidades específicos de Colombia, por ejemplo las leyes de localización de datos de India, el requisito CERT de Australia o los requisitos de violación de datos.

3.2. Investigación y análisis de prácticas comerciales de nombres de dominio ccTLD.

ANÁLISIS:

Ha habido una evolución en las prácticas comerciales y la estructura de gobierno de la mayoría de los administradores de ccTLD desde la formación de la ICANN desde hace veinte años. Antes de la creación de la ICANN, la mayoría del ccTLD ya había sido delegado por el Dr. John Postel a los administradores dentro de las comunidades locales de Internet, con mayor frecuencia a individuos dentro de la comunidad académica. A lo largo de los años, ha habido una tendencia creciente en la que los ccTLD se redelegaron a una entidad patrocinada por el gobierno. Hoy en día, existe un panorama bastante diverso de los modelos de negocios de ccTLD como se describe a continuación con más detalle. Sin embargo, el modelo de negocio para la mayoría de los ccTLD se encuentra en una de las categorías enumeradas a continuación.



A. <u>China Internet Network Information Center (CNNIC)</u>

CNNIC es una agencia gubernamental que es responsable de la administración del ccTLD .CN. Actualmente, el archivo de zona .CN contiene más de 22.7 millones de nombres de dominio. CNNIC es una agencia dependiente del Ministerio de Industria y Tecnología de la Información (MIIT), que es el regulador gubernamental responsable de la regulación y el desarrollo del servicio postal, Internet, tecnología inalámbrica, transmisión y comunicaciones en China.

Además de operar el dominio de nivel superior .CN, CNNIC también es responsable de la verificación del Nombre Real, que garantiza que se verifique a todos los

registrantes chinos antes del registro de cualquier nombre de dominio. Esto es necesario para todos los registradores y registros con licencia de MIIT. Como se señala en el Entregable 5.3, las acciones de .CO Internet S.A.S. buscar la licencia MIIT, esto se debe tener en cuenta en relación con cualquier proceso de migración. Actualmente, CNNIC solo utiliza una búsqueda simple de nombre / identificación para la verificación del nombre real, pero CNNIC está buscando incorporar la biométrica en un futuro proceso de verificación del nombre real.

Otros servicios empresariales que proporciona CNNIC incluyen la asignación de IP, certificados SSL y DNSCERT. Finalmente, en conexión con la ronda de nuevos gTLD de ICANN en 2012, CNNIC ahora ofrece un conjunto completo de servicios profesionales llave en mano. Además de proporcionar servicios de registro backend a los operadores de registro de nuevos gTLD, ICANN también lo ha acreditado como Agente de depósito en garantía tanto para los registradores [1] como para los registros [2] y como Operador de registro de emergencia (EBRO). [3]

B. DeNIC

DeNIC es el operador de registro de Alemania, el .DE ccTLD, con más de 16.2 nombres de dominio bajo su administración. DeNIC tiene una estructura legal única como una cooperativa basada en miembros del sector privado. Esta estructura cooperativa proporciona beneficios y responsabilidades desde el punto de vista de la gobernabilidad. A diferencia de otros operadores de registro de ccTLD importantes que buscaron activamente oportunidades comerciales como proveedores backend de infraestructura de registro en la ronda de nuevos gTLD de la ICANN de 2012, los miembros de DeNIC no querían que realizaran estas actividades comerciales.

En lugar de buscar nuevas oportunidades comerciales de gTLD que tuvieran el potencial de diluir la marca .DE, DeNIC se centró en la gestión de identidad digital. [4] Este servicio se comercializa actualmente como DENIC ID, que se basa en el estándar ID4me, en el cual DeNIC ha sido su contribuyente / patrocinador principal. [5] ID4me está diseñado como una identidad federada de OpenID / OAuth (inicio de sesión único) que utiliza el DNS como un mecanismo de descubrimiento de ancla de confianza. Bajo este modelo, DeNIC, en su calidad de operador de registro, sirve como "autoridad de identificación" y los registradores sirven como "agente de

identificación". Este modelo busca utilizar a las partes contratantes del Registro y Registrador existentes como componentes fundamentales de un nuevo dispositivo digital del ecosistema de identidad.

C. Nominet

Nominet es el operador de registro del Reino Unido .UK ccTLD con aproximadamente 12 millones de registros de nombres de dominio bajo administración y tiene un personal de más de 190 personas. Además de los .UK ccTLD, también brindan servicios de soporte backend a más de 35 gTLD. En 2017 obtuvieron ingresos de más de 30 millones de libras y un beneficio de más de 8 millones de libras. Como una compañía sin fines de lucro, Nominet participa activamente en la filantropía y se expande a nuevos productos y servicios. Algunos de los nuevos servicios que están proporcionando incluyen la ciberseguridad y la gestión del espectro. Aunque no proporciona un servicio de identidad digital específico, Nominet se ha comprometido en la validación de datos para verificar el nombre y la dirección de los solicitantes de registro .UK. [6]

D. SIDN

SIDN es una empresa del sector privado que se desempeña como operador de registro de los países bajos, ccTLD .NL, que actualmente cuenta con más de 5.8 millones de nombres bajo su administración. Además de proporcionar servicios de registro para .NL, SIDN también se ha involucrado activamente en el mercado de infraestructura de registro al proporcionar servicios de registro de back-end a .AMSTERDAM y .AW. Además de los servicios de nombres de dominio, SIDN proporciona un servicio de vigilancia de nombres de dominio y opciones de seguridad mejoradas. La estructura de SIDN es única ya que tiene la unidad de SNDL Labs separada que participa activamente en la investigación y promoción de varias áreas de innovación tecnológica. Algunas de estas áreas incluyen, pero no se limitan a: Servicios de identidad y confianza; Mitigación de DDOS; DANE y seguridad del correo electrónico, y DNSSEC.

E. NIC.BR

El Centro de Información de la Red Brasileña es una entidad civil sin fines de lucro que es responsable de la administración y operación del ccTLD .BR, que

actualmente cuenta con aproximadamente 4 millones de nombres de dominio bajo su administración. NIC.BR es un jugador muy activo y destacado en ICANN y en la comunidad más amplia de Gobernanza de Internet. NIC.BR tiene una estructura organizativa muy diversa que involucra activamente a las múltiples partes interesadas, entre las que se incluyen: registro de nombres de dominio y asignación de IP (registro.br); seguridad y respuesta a incidentes (cert.br); estudios y encuestas sobre el uso de las TIC (cetic.br); Ingeniería de internet y nuevos productos (ceptro.br); tecnologías web (ceweb.br); intercambio de tráfico (ix.br); y estándares web (WC3-Brasil).

F. AFNIC

La Asociación Francesa para el Comercio de Internet en Cooperación "(AFNIC) es el administrador del ccTLD .FR de Francia, con más de 3 millones de nombres bajo administración. Al igual que otros administradores de ccTLD, AFNIC ha buscado activamente contratos de servicio de registro backend con más de 17 nuevos gTLD, como .PARIS y .BZH. AFNIC también brindan servicios de registro de nombres de dominio a otros ccTLD, como .NC, .PF y WF. [7] Además de estos servicios de registro de nombres de dominio, AFNIC también proporciona una gama de otros servicios de consultoría en El área de ciberseguridad, DNSSEC, e inteligencia empresarial.

G. CZ.NIC

CZ.NIC es el operador de registro del ccTLD .CZ , de República Checa, con aproximadamente 1.3 millones de nombres bajo administración. La estructura legal de CZ.NIC es una asociación de interés de personas jurídicas, compuesta por 115 miembros. A diferencia de otros administradores de ccTLD que buscaban aumentar los ingresos al proporcionar servicios de registro backend a otros operadores de registro, CZ.NIC ha desarrollado FRED, que es una plataforma de registro de código abierto que se usa tanto para los registros de nombres de dominio como para ENUM. Actualmente, el software FRED es utilizado por más de 10 ccTLD en todo el mundo. [8]

Además de los servicios de registro de nombres de dominio y software, CZ.NIC está involucrado en varias otras iniciativas. MojeID es uno de los proyectos más interesantes, ya que es una plataforma de identidad digital federada OpenID / OAuth

que se ha integrado en el software de registro FRED. Independientemente de la integración de FRED, MojeID está disponible como una solución de inicio de sesión único para otras plataformas de comercio electrónico. El compromiso de CZ.NIC con la identidad digital también es evidente al servir como el nodo E.ID para el gobierno de la República Checa en relación con la iniciativa eIDAS de la UE. eIDAS es un reglamento de la UE que estableció estándares para la identificación electrónica y servicios de confianza para transacciones electrónicas en el Mercado Único Europeo.

H. Tendencias

Hay algunas tendencias comerciales claras que han estado surgiendo entre los administradores de ccTLD en los últimos años, incluyendo:

- Un número creciente de administradores de ccTLD que operan su propia infraestructura que busca proporcionar servicios de back-end de registro para otros operadores de TLD.
- Un número creciente de administradores de ccTLD ha estado invirtiendo y / o integrando las plataformas de verificación digital e identidad digital en las operaciones de registro; y
- Administradores de ccTLD que invierten en ciberseguridad y otros servicios de inteligencia empresarial / consultoría.

RECOMENDACIONES:

Está en el mejor interés de MinTIC continuar externalizando la operación del ccTLD .CO a un proveedor calificado en términos comerciales más favorables que el último contrato. Después de la ronda de nuevos gTLD de ICANN 2012, el precio de los servicios de registro backend se ha reducido drásticamente en respuesta a un mercado mucho más competitivo. MinTIC debe buscar reinvertir parte de los ingresos excedentes de cualquier contrato de registro futuro en futuras innovaciones en las áreas de identidad digital y ciberseguridad. Esta inversión permitirá a MinTIC fomentar un gran conocimiento institucional del mercado de nombres de dominio dentro del gobierno de Colombia y el sector local de TIC.

[1] Ver https://www.icann.org/resources/pages/registrar-data-escrow-2015-12-01-en
[2] Ver https://newgtlds.icann.org/en/applicants/data-escrow
[3] Ver https://www.icann.org/resources/pages/ebero-2013-04-02-en

[4] Ver https://www.denic.de/en/service/denic-id/
[5] Ver https://id4me.org/
[6] Ver https://registrars.nominet.uk/namespace/uk/data-quality/data-validation-process
[7] Ver https://www.afnic.fr/en/products-and-services/other-french-tlds-top-level-domains/
[8] Ver https://fred.nic.cz/

3.3. Investigación y análisis de prácticas para la protección de datos personales bajo la administración de dominios de ccTLD.

ANÁLISIS:

La creciente proliferación de leyes de privacidad a nivel internacional está complicando las operaciones para la mayoría de los operadores de TLD. Si bien la mayoría de los administradores de ccTLD tienden a centrarse exclusivamente en la ley nacional de privacidad, la operación híbrida de .CO en la cual los dominios de segundo nivel se comercializan a nivel mundial como un gTLD requiere un análisis más profundo. Al parecer el operador de registro .CO ha realizado cambios sustanciales en la información entregada por el WHOIS de .CO con el fin de alinearse con las mejores prácticas de GDPR que están adoptando otros operadores de registro. Consultar el Anexo para la información actual del WHOIS de .CO.

A. <u>Leyes nacionales de Colombia</u>

Existen dos leyes nacionales que pueden tener un impacto potencial en el funcionamiento del .CO ccTLD: la Ley 1266 de 2008 y la Ley 1581 de 2012. La Ley 1266 regula el procesamiento de los datos financieros, los registros de crédito y la información comercial recopilada en Colombia o en el extranjero, por lo tanto, es posible que las actividades de procesamiento del Administrador de ccTLD .CO puedan interpretarse como que están dentro del ámbito de esta ley. La Ley 1581 regula tanto el procesamiento de datos personales como las bases de datos. A diferencia de la Ley 1266, que específicamente tiene una disposición extraterritorial clara, no se pudo determinar si la Ley 1581 tiene una disposición similar. Los asesores legales de MinTIC deben revisar la aplicabilidad potencial de estas leyes nacionales y decidir sobre la inclusión de una disposición específica en la RFP que requiera que todos los postores respondan cómo pretenden cumplir con las leyes de privacidad aplicables de Colombia.

B. <u>GDPR</u>

El Reglamento General Europeo de Protección de Datos (GDPR) 2016/679 es una ley de la UE que aborda la protección de datos para personas naturales de la Unión Europea y el Espacio Económico Europeo. El GDPR ha generado una gran cantidad de atención internacional debido a las posibles multas de hasta 20 millones de euros del 4% de la facturación global anual de una empresa, la que sea mayor. Este interés

internacional se debe en parte a la naturaleza extraterritorial de la ley que impone la responsabilidad de los controladores y procesadores de datos fuera de la UE. El Consejo Europeo de Protección de Datos (EDPB) es el organismo europeo independiente que promueve la aplicación coherente de las normas de protección de datos en toda la UE y facilita la cooperación entre las Autoridades de Protección de Datos de la UE. [1]

El EDPB ha declarado públicamente que el procesamiento histórico de los datos personales en relación con el acceso a WHOIS es inconsistente con los requisitos de GDPR. Estas declaraciones han sido principalmente un controlador en relación con las actividades de ICANN para diseñar e implementar una solución de WHOIS / RDDS compatible con GDPR. Debido a que Europa representa aproximadamente el 12% de todos los registros en .CO, esto debe ser una preocupación legal / comercial para cualquier operador de registro .CO. [2] Por lo tanto, se debe pedir a todos los oferentes que proporcionen un marco sobre cómo pretenden operar el .CO de forma compatible con GDPR. Si bien es probable que el gobierno de Colombia sea inmune a cualquier exposición de responsabilidad de GDPR, la responsabilidad potencial del operador de registro .CO es una preocupación que debe abordarse porque tiene un impacto en la seguridad y estabilidad de las operaciones de CO.

Si bien GDPR es una ley europea, un número creciente de otras leyes nacionales lo han usado para modelar sus propias leyes nacionales. De hecho, el estado de California ha utilizado el GDPR para modelar su propia ley estatal en ausencia de cualquier ley nacional de los Estados Unidos.

C. Leyes de Localización de Datos

Además de las consideraciones legales de GDPR, cualquier operador de registro .CO debe ser consciente de la creciente proliferación de leyes de localización de datos que prohíben la exportación de datos personales de ciertos países, por ejemplo Vietnam, Indonesia, Brunei, Irán, China, Brasil, India, Australia, Corea, Nigeria y Rusia. Como se indica en el Entregable 5.3, .CO Internet S.A.S. ya ha obtenido la licencia del gobierno chino (MIIT). MinTIC deberá consultar con .CO Internet S.A.S. para conocer los detalles de cómo se procesan los datos del registrante chino local en China para que se pueda divulgar a los posibles oferentes. Esta información es necesaria para que los encuestados / oferentes puedan abordar

este problema en sus respuestas de RFP para garantizar una transición sin problemas. Si no se tiene en cuenta y no se aborda esta situación, se podría crear una interrupción potencial del servicio para los solicitantes de registro .CO en China.

D. ICANN

ICANN es un recurso excelente para los aspectos legales de GDPR y su impacto en los servicios de registro de nombres de dominio genéricos. ICANN ha participado directamente con la Comisión de la UE y el EDPR en relación con estos problemas, y ha creado una página dedicada en su sitio web que contiene esta información. [3]

E. ccTLDs

La comunidad de ccTLD, especialmente los operadores europeos, ha sido muy proactiva al abordar las inquietudes sobre la privacidad de los datos de los solicitantes de registro. Esto ha dado como resultado varios cambios relacionados con los datos que recopilan, por ejemplo, minimización de datos, a datos que ya no se hacen públicos a través de WHOIS / RDDS. En el Anexo A se incluye una encuesta que incluye la lista de campos de datos que los operadores de registro de ccTLD europeos recopilan y publican a través de Whois / RDDS.

También se incluye en el Anexo A la investigación que involucra la distinción entre personas registradas y personas físicas y jurídicas. Si bien GDPR y otras leyes nacionales de privacidad tienen un impacto directo en la recopilación y el procesamiento de datos relacionados con personas físicas, estas leyes generalmente no imponen ninguna limitación en la recopilación y el procesamiento de entidades jurídicas distintas de las personas físicas que trabajan para esas personas jurídicas. Ha habido otros administradores de ccTLD que han analizado la implementación de la solución de identidad digital en su proceso de registro de nombres de dominio (ver Entregable 3.2) para proteger la privacidad de los solicitantes de registro. Si bien el gobierno de Colombia debe solicitar este tipo de mejoras de privacidad / innovación a los encuestados en relación con la solicitud de propuesta, el gobierno de Colombia debe reconocer que, dado el estricto plazo de migración (aproximadamente 4 meses), algunos de estos cambios deberán retrasarse hasta después de la migración.

RECOMENDACION:

El gobierno de Colombia debe incluir una o más preguntas específicas en la RFP para abordar posibles problemas de privacidad de los datos desde la perspectiva de Colombia (nacional), europea (GDPR) e internacional (localización de datos).

Los oferentes también deben estar obligados a resumir / proporcionar sus políticas sobre el borrado de datos, por ejemplo el erecho al olvido, y sus procedimientos internos sobre el manejo de solicitudes de interés legítimo para acceder a los datos personales del solicitante de los siguientes tres grupos: propiedad intelectual, aplicación de la ley (tanto en Colombia como en el extranjero) e investigadores de ciberseguridad.

Existe una clara tendencia creciente entre los operadores europeos de ccTLD de distinguir entre personas físicas y jurídicas en la recopilación y el procesamiento de datos. El gobierno de Colombia debe considerar imponer una obligación similar a todos los posibles encuestados, o al menos proporcionar una puntuación mejorada para aquellos encuestados que aborden de manera proactiva esa solución. Dado el apretado cronograma para la migración que se indica en el Entregable 5.3, el gobierno de Colombia debe retrasar cualquier mejora potencial en el proceso de registro hasta al menos 6 meses después de la transición inicial.

3.4. Identificación de las calificaciones mínimas y el personal necesario que el ccTLD debe tener

Calificaciones técnicas y experiencia

Estas son las calificaciones mínimas recomendadas que debe tener el administrador de ccTLD en relación con la relevancia del ccTLD .CO, su alcance internacional y la seguridad y estabilidad requeridas por el estado actual de Internet:

Gestión del DNS y zona

a. Red global de DNS con más de 200 nodos.
b. Experiencia exitosa de más de 10 años contra ataques DDOS
c. Nodos DNS existentes que admiten al menos 10 mil millones de consultas de nombres de dominio de gTLD por día
d. Existing DNS nodes tested to collectively handle over 1 trillion queries per day
e. Nodos DNS existentes ya probados para manejar colectivamente más de 1 billón de consultas por día
f. No usar software de servidor de nombres provisto por terceras partes
g. Las ubicaciones de DNS utilizan al menos 10 puntos de intercambio de Internet dispersos en todo el mundo que utilizan más de mil pares de IPv4 e IPv6 colectivamente.
h. Experiencia exitosa en la implementación de claves en TLD con más de 3 millonesde dominios
i. Cumplimiento de todos los estándares DNS actuales y un historial de funcionamiento dentro de los estándares establecidos
j. Dispositivo DNSSEC (todos los componentes) totalmente certificado para FIPS-140-2 nivel 2
k. Experiencia en el manejo de más de 50,000 zonas firmadas

Servicios de registración y de datos

a. Experiencia exitosa escalando a más de 10 millones de dominios en un solo TLD
b. La base de datos de dominio gTLD existente debe admitir al menos 25 millones de transacciones diarias al mismo tiempo que cumple con los SLA
c. El registro de gTLD existente admite hasta 100M DUM (Domains Under Management) y 64K transacciones / min mientras se cumplen los SLA.

d. Sin tiempo de inactividad no planificado en los últimos 5 años. Tecnología probada para la eliminación en forma estable de dominios y un rápidas registraciones nuevos dominios

e. Numerosas extensiones EPP personalizadas, por ejemplo, Poll Queue, verificación / reclamos, Información de registrador, Extensión de tarifa (nombres premium)

f. Acceso continuo y equitativo al sistema de registro.

g. Cumplimiento de todos los estándares de registro actuales y un historial limpio de funcionamiento dentro de los estándares

h. Amplio liderazgo de la industria y participación para estar preparados para futuros estándares

i. Sistemas robusto de relaciones con los registradores con inicio de sesión único y facilidad de administración para los registradores

j. Entorno de prueba aislado para realizar pruebas de aplicaciones antes de ser incluidas en la producción (OT&E)

k. Canal de registro existente de más de 1500 registradores

Seguridad y Mitigación de abusos

a. Compromiso con la mitigación del abuso representado por las clasificaciones de TLD en SURBL y SPAMhaus, incluyendo la revisión del 100% de todos las nuevas registraciones

b. Mínimo de 9 años completando con éxito las auditorías externas de seguridad

c. Procesos comprobados de seguridad de registro que admiten más de 60,000 conexiones para más de 1,000 registradores

d. Experiencia de escalamiento exitoso para admitir 500,000 nombres de dominio de gTLD revisados por mes por abuso

e. Experiencia en la validación de un promedio de 200,000 nombres de dominio de gTLD por mes por abuso

Soporte al cliente

a. Sistema de ingresos diferidos validado por la auditoría

b. Herramientas integrales de inteligencia de negocios

c. Equipo de atención al cliente con altas calificaciones anuales de desempeño

d. Resolución comprobada de más de 10,000 tickets anuales de soporte al cliente

e. Soporte para múltiples programas de precios concurrentes, programas de precios complejos, monedero común, soporte prepago y pospago

f. Equipo de administración de cuentas dedicado con procedimientos de escalamiento comprobados 24x7
g. Sistemas listos para UA (Universal Acceptance) para admitir todos los TLD e IDN utilizados por los registradores

Marketing y ventas

a. Equipo de ventas enfocado en nombres de dominio con buenas relaciones con los registradores más grandes y globales.
b. Experiencia en marketing de productos de dominio que demuestre un crecimiento constante y estable de nuevos gTLDs
c. Sistema de administración de registradores en línea que facilite a los registradores gestionar TLDs
d. Sistema de registro conectado a más de 1400 registradores, incluido el 100% de los 25 líderes mundiales principales

Transición

a. Cero Interrupción de servicio DNS
b. Sin riesgo financier para el Gobierno de Colombia, ni para registradores ni para registrantes
c. Transiciones exitosas de TLD s de al menos 3 millones

Equipo de management

Para cumplir con la ejecución del objeto contractual, el proponente debe crear un equipo que se considere necesario para garantizar la obtención de los productos requeridos.

Las habilidades en este equipo de administración son fundamentales para el éxito de la operación del ccTLD .CO.

El equipo de administración de trabajo básico estará integrado por las funciones que se detallan a continuación.

Rol	Descripción
Gerente del ccTLD .co	Profesional con posgrado en cualquiera de las áreas de ingeniería, economía, administración, derecho u otras ciencias sociales que certifican una experiencia profesional mínima de cinco (5) años en la definición e implementación de políticas para dominios de ccTLD y en el sistema de gobierno de nombres de dominio (Contacto administrativo de la .co de acuerdo con RFC 1591)
Director de seguridad	Profesional de ingeniería de sistemas que certifica una experiencia profesional mínima de tres (3) años relacionada con la dirección, supervisión o implementación de sistemas de seguridad informática, planes de contingencia y planes de continuidad de negocios. Debe tener certificación internacional en seguridad informática y / o continuidad de negocio.
Director de proyectos	Profesional en cualquiera de las áreas de ingeniería o administración que certifican una experiencia profesional mínima de al menos tres (3) años relacionada con consultoría, supervisión y / o implementación de sistemas de información o desarrollos para aplicaciones en Internet que incluyen bases de datos, interfaces para usuarios, pagos online y atención al cliente. La experiencia debe incluir la gestión de grupos de desarrollo y el mantenimiento de sistemas, la gestión de grupos de operaciones para el soporte de servicios (help-desk), la planificación y gestión de presupuestos de proyectos y la gestión de proveedores. El profesional debe tener una maestría en ingeniería industrial, gestión de proyectos o administración de empresas.
Director técnico	Profesional de ingeniería de sistemas o telecomunicaciones, con una experiencia mínima de tres (3) años relacionada con la implementación y administración del DNS, sistemas de registro de dominios, operaciones entre registro y registradores y administración del protocolo de comunicación de computadora EPP. (Contacto técnico de .co según RFC 1591)
Gerente de soporte al cliente	Profesional en el área comercial y de marketing con experiencia en herramientas de inteligencia de negocios, gestión de equipos de servicio al cliente con altas calificaciones de desempeño anual, múltiples programas de precios concurrentes, programas de precios complejos, billetera común, soporte prepago y pospago.
Gerente de ventas y marketing	Profesional con experiencia comprobada en ventas y marketing con relaciones buenas y probadas con los registradores globales más grandes, experiencia en marketing de productos de dominio que muestre un crecimiento constante y estable de nuevos gTLD.

3.5. Identificación de los minimos niveles aceptables de servcio para la disponibilidad del ccTLD y para los pedidos de información

ANALISIS:

Es fundamental que cualquier operador de registro de nombres de dominio de nivel superior de clase mundial garantice las eficiencias de operación y el tiempo de funcionamiento para cumplir con las expectativas de los registrantes y registradores. Los Acuerdos de nivel de servicio (SLA) se utilizan comúnmente para garantizar estos requisitos. Estos umbrales de SLA se incluyen con mayor frecuencia en la RFP; Sin embargo, no es un requisito previo. A modo de ejemplo, la RFP de .US más reciente no incluyó ningún SLA esperado. En cambio, las disposiciones de los SLA para la licitación .US se incorporaron previamente en el contrato ejecutado entre el gobierno de los Estados Unidos y el licitante seleccionado.

Lo que se incluye en los SLA también varía entre varias RFP. Mientras que la mayoría siempre incluye criterios técnicos operacionales, otros incluyen requisitos operacionales y comerciales. Por ejemplo, en relación con la licitación más reciente de PIR para su cartera de TLD, independientemente de los SLA de ICANN, PIR estableció una lista de requisitos de SLA centrados en el soporte al cliente (Registrador), así como algunos requisitos operativos / comerciales, por ejemplo: tramitación de órdenes judiciales, business intelligence.

Si bien es posible exigir estándares de SLA más altos o más estrictos que los que figuran en el Acuerdo de Registro de referencia de ICANN, es importante tener en cuenta que esta decisión podría tener un impacto negativo significativo en otras áreas. Primero, aumentar el SLA por encima de los mandatos de la ICANN podría dar lugar a un grupo más pequeño de posibles oferentes, lo que limitaría las opciones de elección del gobierno de Colombia. Sobre la base de la última oferta de .CO, es altamente deseable contar con al menos dos oferentes calificados para lograr los mejores resultados. En segundo lugar, aumentar el SLA por encima de los requisitos de la Especificación 10 de ICANN, probablemente requiera que el gobierno de Colombia despliegue recursos adicionales para garantizar que se cumplan los umbrales de cumplimiento.

RECOMENDACION:

Aunque no es obligatorio, se recomienda encarecidamente que se incluyan los umbrales de SLA esperados en la RFP .CO. Sin embargo, en función del análisis, se recomienda que el gobierno de Colombia emplee un enfoque híbrido hacia el cumplimiento de SLA para maximizar los resultados y minimizar los costos de cumplimiento. Específicamente, se recomienda que el gobierno de Colombia exija a cualquier proveedor que brinde una certificación periódica de que los requisitos de SLA de gTLD de ICANN según lo establecido en la Especificación 10 del Acuerdo de Registro de referencia se están cumpliendo en relación con la operación de .CO. De esta manera, el gobierno de Colombia puede garantizar un alto umbral de SLA sin asumir la carga y el costo de configurar nodos de prueba externos. Además de la certificación de SLANN de SLA, el gobierno de Colombia debe aumentar sus requisitos de SLA con requisitos no técnicos según lo establecido en la RFP PIR, ver el Anexo B Sección Anexos 3.5.-.

4. Parte 4 (Ref: 2.2.3)

Presentar estudios que contengan las principales recomendaciones al MinTIC de Colombia, teniendo en cuenta (i) las tendencias internacionales, (ii) los resultados y productos derivados de la gestión del actual Concesionario, (iii) los potenciales futuros cambios del mercado de ccTLD, y (iv) la normatividad colombiana vigente en torno al tema

4.1. Planteamiento de lineamientos para la formulación de una política respecto de la organización, administración, mantenimiento y operación del ccTLD de Colombia, .co.

Para elaborar las reglas o políticas para organizar, administrar y mantener el funcionamiento del ccTLD nacional .Co en Colombia, se deben considerar las siguientes pautas de actividades:

Promoción del ccTLD .co:

a. Definir e implementar la estrategia para promover el registro y uso de ccTLD .co.
b. Coordinar la relación con los registradores, que deben firmar y garantizar el cumplimiento de los acuerdos entre el Administrador y el Registrador, para maximizar el alcance de ccTLD.co.
c. Ser responsable de definir el modelo para la delegación de nombre de dominio en ccTLD .co, así como de los servicios de registro ofrecidos por registradores acreditados.
d. Responsabilidades del Administrador del ccTLD.co:
e. Responsable de la administración y organización del ccTLD .co
f. Gestionar la relación con ICANN, ccNSO y con LACTLD
g. Participar en la construcción de políticas relacionadas con la gestión de los ccTLD, a nivel regional e internacional.
h. Promover la confianza en su uso
i. Implementar y salvaguardar las políticas y / o actividades para asegurar el apoyo de la comunidad local de Internet con las pautas del Comité Asesor de Políticas de ccTLD.co
j. Interactuar con las entidades encargadas de la resolución de conflictos
k. Abordar parte del Comité Asesor como invitado permanente
l. Crear un entorno de diálogo entre las diferentes partes interesadas del ecosistema de Internet, alineado con el modelo de múltiples partes interesadas promovido por la ICANN

Actividades relacionadas con la opreración técnica del ccTLD .co

a. El contratista debe tener al menos cinco (5) puntos de servidores DNS, incluido uno (1) en Colombia, y los otros cuatro (4) deben estar conectados a Internet en diferentes lugares y redes para garantizar su funcionamiento en caso de daños temporales de cualquier de los servidores.

b. Los servidores DNS deben estar conectados a Internet a través de los anillos de alta velocidad del mundo, utilizando la tecnología anycast. Se espera que lo anterior garantice la seguridad, estabilidad y confiabilidad del sistema de nombres de dominio para el ccTLD .co.

c. Debe mantener las bases de datos, que consisten en almacenar la información de los dominios registrados (archivo de zona) y conectarlos con los servidores raíz principales, como misión principal, entre otras relacionadas

d. Operar y mantener el servidor primario de ccTLD .co

e. Operar y mantener los servicios secundarios de ccTLD.co

f. Compilar, generar y propagar los archivos de zona del ccTLD .co

g. Operar el ccTLD .co bajo un registro THICK

h. Garantizar el acceso público, creíble y actualizado a la base de datos de nombres de dominio (WHOIS) del ccTLD .co.

i. Establecer una copia de seguridad para los archivos de zona .c ccTLD y la información registrada para el nombre de dominio.

j. Cumplir con los estándares definidos por el IETF: RFC 1035, RFC 2181, RFC1034, RFC 1101, RFC 2182 y RFC 2234, y otros RFC aplicables, así como las políticas definidas por la ICANN o aquellas definidas en el futuro durante la ejecución del contrato.

k. En cualquier momento, cada servidor debe ser capaz de manejar una carga de solicitudes de datos equivalente a tres veces el valor máximo de dichas solicitudes desde el servidor más cargado en condiciones normales. Esto con el fin de garantizar la continuidad del servicio.

l. Cada servidor debe tener conectividad permanente y amplio ancho de banda para satisfacer las necesidades del requisito anterior. La conectividad a internet debe ser lo más diversa posible. Además, los servidores deben tener mecanismos para aceptar la conectividad IP de cualquier proveedor de Internet.

m. Desarrollar y distribuir entre los registradores acreditados para el ccTLD .co, el protocolo EPP (Extensible provisioning protocol software: Protocolo de aprovisionamiento extensible) para facilitar una interfaz segura y eficiente entre el administrador de .co ccTLD y los registradores, así como proporcionarles soporte técnico.

n. Instalar y operar sistemas de comunicaciones de acuerdo con las mejores prácticas en el campo. El Contratista debe implementar comunicaciones autenticadas y debe documentar todas las prácticas y la configuración de todos los sistemas.

o. Definir e implementar planes de contingencia y continuidad de operación de DNS.

p. Definir e implemente un plan de seguridad informática: el contratista debe desarrollar e implementar un plan de seguridad informática. El contratista debe actualizar el plan anualmente y entregarlo al Ministerio de TIC cuando sea necesario.

q. Asegurarse de que los datos de registro de nombres de dominio bajo el ccTLD .co se gestionen bajo los más altos estándares de seguridad; asimismo, debe garantizar la protección de los mismos para evitar prácticas como el spam.

r. Proporcionar el servicio de registro para dominios de solicitantes restringidos (.org.co, edu.co, gov.co, mil.co) y brindar el soporte adecuado a dichos solicitantes.

s. Garantizar la transición de la operación del dominio en colaboración con el operador actual a la estructura propuesta, asegurando en todo momento la estabilidad del DNS. Asegurar también la transición técnica con el futuro contratista.

4.2. Propuesta de lineamientos técnicos para la formulación de la estrategia para el diseño de un proceso de selección objetiva que permita la administración eficiente del ccTLD de Colombia, .co, bajo la modalidad de contrato de concesión

RECOMENDACIONES SOBRE LOS REQUISITOS TÉCNICOS (SEGURIDAD):

Infraestructura para la seguridad de la información:

Seguridad de Activos: Clasificación y Control

Todos los activos de información importantes (como bases de datos o archivos de datos, documentación del sistema y manuales de usuario, material de capacitación, procedimientos operativos y de soporte, planes de continuidad, acuerdos de reserva e información archivada) deben ser rastreados y tener un responsable asignado del equipo de administración de seguridad del oferente.

Los activos de software, como el software de aplicaciones y sistemas, las herramientas de desarrollo, los servicios públicos, así como los activos físicos, incluidos los equipos y las piezas, y los activos de servicios como los servicios públicos generales y los proveedores de servicios públicos, deben ser rastreados para garantizar el control.

Personal de seguridad

Las responsabilidades de seguridad se establecen en la política de seguridad del oferente, que debe estar disponible en la respuesta de la RFP.

Comunicaciones y gestión de operaciones

Las principales áreas de enfoque en Gestión de Operaciones deben incluir:

a. Control de Cambios Operacionales
b. Procedimientos de manejo de incidentes
c. Segregación de roles y responsabilidades
d. Separación de instalaciones operativas y de desarrollo
e. Gestión de acceso de terceros a instalaciones operativas

RECOMENDACIONES SOBRE MIGRACION Y PLAN DE TRANSICIÓN

El oferente deberá proporcionar un plan de migración / transición completa que incluya, por lo menos lo siguiente:

1. Fase de Pre-transición:
    a. Definición detallada del plan de migración con el alcance completo de las actividades que se requerirían para la transición de los activos de TI existentes. Esto incluiría el estudio de los sistemas existentes para identificar activos de TI tangibles e intangibles (incluidos los datos) que estarían dentro del alcance de la transición. Todos los elementos necesarios para las operaciones de los sistemas .CO deben incluirse dentro del alcance.
    b. Finalizar el programa y los requisitos de calidad para la migración de datos de los proveedores actuales (operadores de mostrador y proveedores de TI existentes)
    c. Preparar el enfoque de transición para el proyecto que debe incluir la estrategia de transición, el estado actual y futuro, las partes interesadas involucradas en la transición, la evaluación de la preparación para la transición y el cronograma para el lanzamiento del proyecto.
    d. Preparar e implementar planes de back-up adecuados para garantizar que ninguno de los activos de TI tangibles o intangibles se pierda
    e. Migración de DNS y plan de continuidad (plan detallado para la preparación del sistema, implementaciones de software y ejecución paralela de los sistemas hasta la fecha de puesta en marcha)
    f. Migración de los registradores al nuevo sistema
    g. Continuidad de las operaciones diarias de registro
    h. Planes de respaldo y contingencia

2. Fase de Transición / Migración Transition:
    a. Migrar el 100% de los datos de la aplicación actual al módulo / aplicación desplegado por el licitante
    b. Migrar la conectividad correspondiente cuando el dispositivo o su software asociado se migran de una versión / modelo a otro adhiriendo al SLA de tiempo de actividad

c. Migrar la configuración de un dispositivo a su modelo más reciente / actualizado durante la migración
d. Migrar la conectividad / LUN (Logical Unit Number) del host correspondiente cuando el dispositivo o su software asociado se migre de la versión / modelo existente a otro mientras se adhiere al SLA de tiempo de actividad
e. Migrar y verificar un subsistema de copia de seguridad y replicación cuando alguno de sus componentes o su software asociado se migre de la versión / modelo existente a otro mientras cumple con el SLA de tiempo de actividad para garantizar que se mantengan los niveles de servicio
f. Migrar la configuración de cualquier componente a su modelo más reciente / actualizado durante la actualización
g. Migrar los sistemas y servicios de copia de seguridad y replicación de un Centro de Datos a otro, si es necesario durante una migración del Centro de datos, preparando un plan detallado de migración aprobado por el MINTIC
h. Migrar los dispositivos virtuales cuando el dispositivo o su software asociado se migran de una versión / modelo a otro mientras se adhieren al tiempo de servicio del SLA
i. Migrar la configuración de un dispositivo a su modelo más reciente / actualizado durante la actualización

3. Fase de Post-transición:

j. Preparar informe de evaluación de migración y enviarlo al MINTIC. La evaluación de la migración comienza cuando el licitante puede proporcionar un soporte para un estado estable para las operaciones. La evaluación de la migración se puede realizar según las variaciones programadas, la cantidad de incidentes notificados y los criterios establecidos inicialmente. El ofertante deberá crear un informe detallado del análisis de la causa raíz y las medidas correctivas.
k. Preparar documentos de transición y recursos de conocimiento. Esto implica la finalización de la documentación general sobre los activos de TI que se han incluido bajo la responsabilidad del licitante. Además, los problemas enfrentados durante la transición, sus causas, los pasos tomados para resolver y las medidas de precaución sugeridas deben documentarse.

RECOMENDACIONES SOBRE LA EVALUACION DE PLANES DE MARKETING Y PROMOCION PARA .CO

Las siguientes actividades de marketing y promoción deben incluirse en los planes del nuevo administrador de ccTLD:

a. Objetivos de nombres de dominio propuestos para crecimiento año por año;
b. Estrategias propuestas a seguir para marketing directo e indirecto;
c. Canales y métodos propuestos;
d. Propuesta de mecanismos de evaluación para medir la efectividad de los planes.
e. Demostrada experiencia previa y resultados de logrado crecimiento

RECOMENDACIONA SOBRE EL NUMERO REDUNDANTE DE NODOS DISTRIBUIDOS GLOBALMENTE EN EL DNS

El proponente debe presentar en su propuesta detallada el número de nodos redundantes, incluida la distribución global que actualmente tiene para operar el sistema de nombres de dominio DNS. Para los fines de evaluar este factor de selección, el proponente deberá demostrar para cada nodo redundante su ubicación, sus características, incluida la fecha en que entró en operación, y el ccTLD o gTLD para el que presta servicios. El número de nodos redundantes con distribución global presentado en la propuesta será el mínimo con el que el proponente, en caso de que se le otorgue la conexión, administrará el ccTLD.co durante el plazo de la concesión.

Para los fines de la evaluación de este factor de selección, el proponente debe demostrar que cada nodo está ubicado en un punto geográfico diferente, sus características técnicas, la fecha en que entró en funcionamiento y el ccTLD o gTLD para el que sirve. Si el nodo no se especifica con la información descrita anteriormente, se considerará como no existente. Finalmente, se destaca que no será posible certificar los nodos DNS que forman parte de un esquema de subcontratación.

Si el proponente tiene a nivel de infraestructura DNS entre seis (6) y ocho (8) nodos redundantes en diferentes puntos geográficos, obtendrá diez (10) puntos; si hay entre nueve (9) y once (11) nodos, obtendrá treinta (30) puntos y, finalmente, si hay doce (12) o más nodos redundantes distribuidos globalmente, obtendrá sesenta (60)

puntos. Si el proponente tiene al menos un (1) nodo DNS ya instalado y en ejecución en Colombia, se otorgarán diez (10) puntos adicionales por la presencia local; si el proponente tiene 2 o más nodos DNS ya instalados y funcionando en Colombia, se otorgarán quince (15) puntos adicionales. Los nodos locales en Colombia aumentarán la velocidad de resolución de Internet en el país.

Se propone el siguiente sistema de puntuación para evaluar la infraestructura DNS:

a. Si el proponente tiene nodos DNS a nivel de infraestructura DNS ubicados en IXP puntos de intercambio de tráfico de Internet en diferentes puntos geográficos, obtendrá 45 puntos
b. si hay más de 10 nodos DNS ubicados en IXP globalmente dispersos que admiten tanto IPv4 como IPv6
c. si hay entre 6 y 9 nodos DNS en IXP dispersos globalmente que soportan tanto IPv4 como IPv6, obtendrá 20 puntos
d. si hay 3-5 nodos DNS en IXP dispersos globalmente que soportan tanto IPv4 como IPv6, obtendrá 10 puntos
e. y finalmente, si hay menos de 3 nodos DNS en IXP dispersos globalmente que soporten tanto IPv4 como IPv6, obtendrá cero (0) puntos.

RECOMENDACIONES EN RELACIÓN CON EL APOYO DE LA INDUSTRIA NACIONAL

Se sugiere el siguiente puntaje para evaluar el impacto de la promoción de la industria nacional en la propuesta. En este sentido, se sugiere la sugerencia de asignar 100 puntos, de acuerdo con la Ley 816 de 2003, como se define a continuación:

Factor de calificación	**Calificación**
El director general del ccTLD .co debe tener residencia en Colombia	20 puntos
El director del proyecto debe tener residencia en Colombia	20 puntos
Como parte del equipo de registrars (10, diez) que se presenten , uno (1) debe tener 100% capital nacional	10 puntos
Experiencia (respaldada por cartas de referencia o certificados) para el desarrollo de capacidades relacionadas con Internet en América del Sur. (La promesa de creación de capacidades no constituye motivo suficiente para otorgar puntos)	30 puntos

El oferente con Capital Nacional recibirá un puntaje con las siguientes condiciones: Capital nacional entre 0% y 30% Capital nacional entre 30 % y 40% Captial nacional entre 40 % y 80% Menos que 80% de capital nacional	Cero puntos 10 puntos 15 puntos 20 puntos

RECOMENDACIONES SOBRE EL METODO DE EVALUACION

Para determinar el método de evaluación de los méritos técnicos de los oferentes para un TLD del tamaño y alcance de .CO, es importante agregar otros factores como la mitigación del abuso, la ciberseguridad y la transición, como factores críticos.

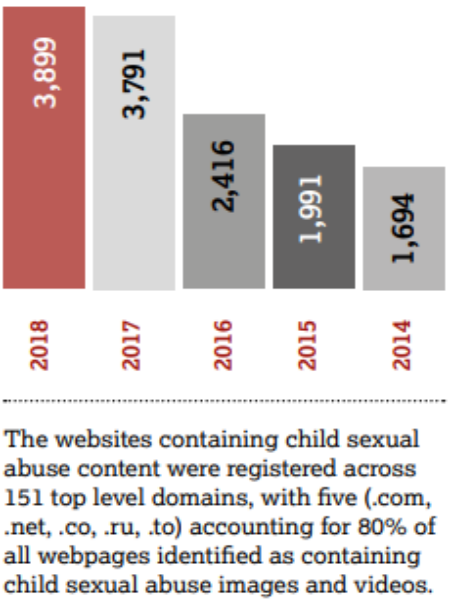
Todos los oferentes técnicos calificados para el back-end ofrecerán experiencia equivalente en los sistemas de registro principales (EPP, Whois, Escrow, etc.). Sin embargo, es muy importante examinar también la capacidad del oferente para los servicios de próxima generación como RDAP, DNSSEC, IPv6, anti-phishing, etc. Dado el gran interés del MINTIC por expandir Internet en Colombia, se debe dar importancia a los oferentes que han establecido infraestructura para la resolución de DNS dentro de Colombia, así como a oferentes que se comprometan firmemente a expandir el DNS en toda Colombia.

Por ser un TLD con más de 2.2 M de nombres de dominio en el segundo y tercer nivel, el .CO TLD es uno de los ccTLD más grandes del mundo; los nombres de domino representan una infraestructura crítica tanto para el país de Colombia como para la base global de usuarios de .CO que dependen del correcto funcionamiento del espacio de nombres de dominio.

Como resultado, cualquier transición del TLD .CO se debe realizar con mucho cuidado y debe confiarse solo a las partes que tengan experiencia previa significativa en la realización de transiciones de TLD, medida tanto por el número de transiciones realizadas como por el tamaño de las transiciones realizadas. El puntaje relacionado con la experiencia de transición y el plan de transición deben tener un alto puntaje

en la evaluación, mayor que el realcioando con la funcionalidad de los sistemas de registro.

Específicamente, el puntaje máximo debe reservarse para un operador que haya demostrado una transición de "operador a operador" para un número crítico de TLD en escala. Los proveedores que hayan realizado más transiciones, y en una escala más grande, deben ser preferidos a los proveedores sin tal experiencia, debido al alto riesgo de la transición.



The websites containing child sexual abuse content were registered across 151 top level domains, with five (.com, .net, .co, .ru, .to) accounting for 80% of all webpages identified as containing child sexual abuse images and videos.

También se debe considerar el plan técnico para la transición y las medidas específicas identificadas para mitigar el riesgo de una transición del TLD.

La seguridad y el uso indebido de abusos son las principales áreas de preocupación para Internet en su conjunto y deben serlo para el .CO ccTLD en particular. Un informe de 2018 realizado por Internet Watch Foundation muestra que los TLD .CO están dentro de los 5 TLD más abusados para URL de abuso sexual infantil. Que el .CO TLD sea conocido por la pornografía infantil presenta una mala imagen tanto para el país como para los niños que afecta en todo el mundo.

Como resultado, se considera relevante una clasificación significativa para los proveedores que tienen un historial de logros y éxitos en las prácticas contra el abuso y la seguridad cibernética. Estas deben ser métricas mensurables, y no deben basarse únicamente en las promesas hechas por cada oferente. Las referencias a los servicios de mejores prácticas globales como Spamhaus, SURBL, APWG, IWF, etc. deben usarse como referencias para garantizar una revisión imparcial.

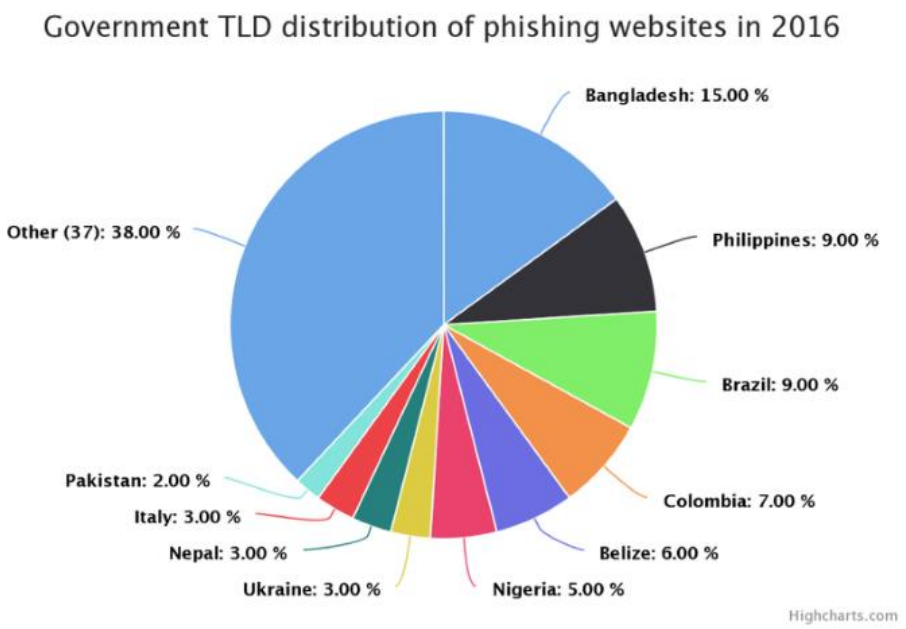


Fig-3 These countries have some work to do improving their security posture

Distribución de sitios de phishing en ccTLDs de gobiernos en 2016

Fuente: RISKIQ[37]

El análisis de RiskIQ de 2016 demuestra que los dominios de nivel superior de gov.co son el cuarto objetivo más grande en todos los intentos de phishing en todo el mundo. Los oferentes deben poder demostrar que los TLD que actualmente administran en nombre de los países no tienen una alta calificación en cuanto a phishing u otras métricas de abuso.

El alcance y la disponibilidad del DNS dentro de Colombia y en todo el mundo deben tener un peso muy alto en la puntuación. A diferencia de los servicios de registro, el alcance y la disponibilidad del DNS no son un producto básico, y si bien muchos proveedores hacen afirmaciones sobre la disponibilidad global, es importante valorar la disponibilidad de los servicios del DNS dentro de Colombia, de tal manera de asegurar que los colombianos obtengan la mayor velocidad y valor de los servicios provistos por el proveedor, y que los usuarios colombianos se beneficien de accesos rápidos a sitios web y transmiones veloces de emails dentro de Colombia usando el ccTLD .co. Se deben asignar puntos para una infraestructura de directorio distribuida

[37] https://www.riskiq.com/blog/labs/2016-phishing-attacks

y multi-capa para asegurar que no haya un punto único de falla en la red, lo que mejora la confiabilidad y que no haya interrupciones en el servicio de .co.

El proponente debe presentar una propuesta técnica detallada para ser habilitado. Los puntos principales de la propuesta técnica detallada están relacionados con los siguientes temas:

a- Consistencia y apoyo a la política de ccTLD .co: El proponente debe demostrar en la propuesta detallada el conocimiento en la planificación, ejecución, control y mejora de los procesos clave o de la misión en la administración de un ccTLD.

b- Plan para el registro y la promoción de ccTLD .co en un segundo nivel: el proponente debe proporcionar información sobre los siguientes aspectos de la promoción y comercialización de ccTLD .co

- Objetivos de nombres de dominio propuestos para crecimiento año a año
- Estrategias propuestas a seguir para marketing directo e indirecto.
- Canales y métodos propuestos.
- Propuesta de mecanismos de evaluación para medir la efectividad de los planes.
- Demostrada experiencia previa y resultados logrando crecimiento.

c- Plan de contingencia y seguridad: El proponente debe demostrar en la propuesta detallada el conocimiento en la planificación, ejecución, control y mejora de los planes de contingencia y seguridad, lo que está alinado con la seguridad y estabilidad del DNS, que es una prioridad principal para el Estado Colombiano en relación con la administración del ccTLD .co.

d- Definición y aplicación de políticas: el proponente debe demostrar en la propuesta detallada el conocimiento de los principales problemas que enfrenta Internet, como el phising, y el conocimiento y la experiencia en los temas que forman parte de la agenda de ICANN.

e- Plan de transición: el proponente debe demostrar en el conocimiento detallado de la propuesta sobre la planificación, ejecución, control y mejora de los planes de transición con otros administradores, ya que el futuro administrador debe ejecutar una transición con el administrador actual de ccTLD. co.

f- Plan de negocios: el proponente debe demostrar que ha evaluado financieramente la concesión y que si presenta una propuesta debe ser consciente de los riesgos que asume porque existe la prosibilidad que no se alcance la cantidad de registros en los que se basa el plan de negocios, hecho sbre el cual el Estado colombiano no tendrá responsabilidad.

Por otro lado, los factores habilitadores asociados con los aspectos financieros son exigentes dado que la administración del ccTLD .co es delicada, ya que pone en peligro el correcto funcionamiento del ccTLD .co y la seguridad y estabilidad del DNS.

Además, el concesionario requerirá una gran inversión para mejorar la posición del ccTLD .co en todo el mundo.

Seis (6) indicadores son sugeridos. Todos los indicadores aplican a las empresas relacionadas del proponente de la RFP, a saber:

a. Rendimiento sobre el patrimonio (ingreso neto / patrimonio neto): medida de la capacidad del proveedor para generar ganancias de las inversiones de sus accionistas en la empresa. Esta relación determina tanto la eficiencia de la empresa como la efectividad de la administración. Para el administrador de ccTLD, esta es una relación importante porque les permite ver la eficiencia con la que el proveedor utiliza su capital.

b. Titularidad: Consistencia en la titularidad (propiedad) general e inversores mayoritarios y minoritarios por los últimos 5 años.

c. Para entidades de propiedad de riesgo (venture), informar en forma complete sobre todas las participaciones de los accionistas de 5% o más porcentajes.

d. Confianza en un solo contrato (viabilidad comercial): no más del 30% de los ingresos totales del proveedor deben provenir o ser resultado de un contrato para realizar servicios de registro back-end o para ejecutar un ccTLD para un gobierno. [Esto es importante porque una mayor concentración conlleva el riesgo de que el negocio de la concesionaria se vea gravemente afectado por la pérdida de un único back-end grande o contrato de ccTLD del gobierno].

e. Garantía bancaria (liquidez): el concesionario debe estar obligado a obtener una garantía bancaria adecuada en efectivo a partir de 1 año de la operación del ccTLD.

f. Capital de trabajo: un capital correspondiente a los ingresos estimados que recibirá el concesionario durante el primer año de operación, de acuerdo con el escenario normal definido en el estudio económico realizado por el Ministerio de TIC.

g. Rendimiento de los Activos (Ganancias netas después de impuestos / Activos totales) ROA: la estabilidad de toda la operación depende de la fortaleza financiera del concesionario; por lo tanto, es necesario tener un ROA positivo durante los últimos dos años consecutivos. Este indicador se ha tomado de las especificaciones del Banco Agrario, teniendo en cuenta que es una de las entidades del sector público que tiene la mejor competencia para analizar la solidez financiera de los proponentes..

Indicador Financiero	Requerimiento / Puntaje
Rentabilidad sobre recursos propios	Valor positivo REQUERIDO
Titularidad (últimos 5 años)	<5% cambio en los últimos 5 años: POSITIVO 5%-25% cambio en los últimos 5 años: NEUTRAL 25%+ cambio en los últimos 5 años: NEGATIVO
Viabilidad comercial	REQUERIDO
Garantía bancaria	REQUERIDO
Capital de trabajo	REQUERIDO
Retorno sobre activos	Valor positivo REQUERIDO

La evaluación de las propuestas se resume en la siguiente tabla general:

	Factores de evaluación	**Calificación**
Primera fase	Requisitos habilitantes	Habilitado / not habilitado
	Criterios de evaluación técnica (a)	Máximo 400 puntos
Segunda fase	Criterios para selección de la propuesta economica (b)	Máximo 500 puntos
Soporte a la industria nacional (Ley 816 de 2003) (c)		100 puntos
Puntaje máximo:		1000 puntos

a. CRITERIOS DE EVALUACION TECNICA: Max 400 puntos

The following scoring system takes into account important factors such as security and registry transition:

Sistemas de registro	75 (a.1)
DNS	100 (a.2)
Transición Seguridad de anti-abuso	105 (a.3)
Estabilidad, seguridad y abuso	120 (a.4)
TOTAL	400 (Mínimo de 360 puntos para calificar a la próxima ronda)

Debido a que los factores técnicos, la estabilidad y la seguridad son tan importantes, se propone que el puntaje PASSING en los criterios técnicos sea 360/400 (90%). Si el proponente obtiene una puntuación inferior a 360 puntos en la evaluación de los factores técnicos de elección, la propuesta presentada no continuará.

a.1- EVALUACION DE LOS SISTEMAS DE REGISTRO

Registry Systems	75 puntos TOTAL
EPP System and experience	30
Whois System and experience	10
RDAP System[38] and experience	30
Data escrow system and experience	5

a.2- EVALUACION DEL SISTEMA DNS

Sistema DNS	100 puntos TOTAL
Sistema y experiencia en DNS	60 points
DNSSEC, Sistema y experiencia	40 points

a.3- EVALUACION DE LA EXPERIENCIA Y PLAN DE TRANSICION

Plan de transición y experiencia	105 puntos TOTAL
Transición operador a operador (transiciones entre susbsidierios no se considera como transición)	45 puntos máximo 5 TLDs with 1m+ names: 45 points 3-5 TLDs with 1m+ names: 30 points 2-3 TLDs with 1m+ names: 20 points 1 TLD with 1m+ names: 10 points
Technical plan and roadmap	20 points
Measures to reduce/mitigate risk	20 points

[38] https://www.icann.org/rdap

a.4- EVALUATION OF STABILITY, SECURITY AND ABUSE

Stability, Security, Abuse	120 points TOTAL
Abuse in TLDs currently managed by vendor: Number of TLDs operated/provisioned by vendor in SURBL Top 20 abusive TLDs list	0-3: 60 points 4-6: 20 points 6+: 0 points
Rate of abuse in TLDs currently managed by vendor in SURBL Top 20 abusive TLDs list: Ratio of abused domains to total domains per TLD	<1%: 30 points 1%-2%: 15 points 2%-4%: 5 points 4+%: 0 points
Number of TLDs currently managed by vendor in Spamhaus “most abused” TLD list	0: 30 points 1: 20 points 2: 10 points 3+: 0 points

b. CRITERIOS DE SELECCIÓN: Propuesta económica

Criterio económico	**500 puntos**
Costo del Back-end	70%+ bajo: 500 60%-70% bajo: 350 50%-60% bajo: 250 40%-50% bajo: 175 <40% bajo: 150
Ingresos anuales garantizados al MINTIC	$35m+: 250 puntos $25m-$35m: 150 puntos $15m-$25m: 100 puntos $5m-$15m: 50 puntos

4.3. Recomendaciones específicas para estimar la valoración inicial de la concesión y para definir un modelo eficiente de contraprestación económica al Estado colombiano por la administración, mantenimiento y operación del ccTLD de Colombia.co

RESUMEN EJECUTIVO

El presente documento analiza los aspectos económicos y financieros relacionados con el mercado de dominios. En particular, el documento destaca la sensibilidad de la economía a los precios mayoristas del servicio back-end y las estrategias de marketing y promoción. En el caso de Colombia, Neustar tuvo la concesión de administrar el dominio .CO durante los últimos 10 años. Aunque el .CO tuvo un buen desempeño durante este período, el precio pagado a MINTIC (solo el 7% del precio total pagado por los usuarios) ha sido claramente bajo en comparación con el índice de referencia internacional. De manera similar, la desaceleración en el diseño e implementación de una campaña agresiva de mercadeo y promoción, no solo para mantener la base de clientes sino también para aumentarla activamente, ha provocado una estabilización en la tasa anual de mercadeo de crecimiento.

Del análisis de sensibilidad realizado queda claro que el plan de negocios relacionado con el .CO es altamente rentable; sin embargo, el modelo ha demostrado ser muy sensible a la variación de servicios back-end en el ccTLD y la estrategia de comercialización, promoción y comisión de ventas. El análisis de Montecarlo implementado con 10,000 iteraciones muestra que el VAN promedio para un período de diez años alcanza los US $ 200 millones, lo que podría ser el catalizador perfecto para proyectos alternativos relacionados con la mejora de la digitalización en Colombia. En particular, gracias al nivel estable de ingresos, el Ministerio podría asegurar el dominio .CO para aprovechar importantes recursos que podrían ser fundamentales para mejorar la estrategia de conectividad de la última milla.

En este sentido, dos aspectos específicos son muy importantes en el diseño de la licitación que MINTIC pretende lanzar: (i) La especificación de criterios financieros con tal peso que haga que los oferentes comprendan la importancia de mejorar las condiciones económicas existentes que recibe MINTIC (solo el 7% del precio final),

(ii) Relacionar la revisión del precio mayorista con incrementos en el número de dominios administrados. Es importante proporcionar los incentivos correctos al administrador potencial, no solo para aumentar la cantidad de usuarios que utilizan el dominio .CO, sino también para alentar la implementación de una estrategia activa de marketing y promoción.

Del mismo modo, será muy importante fomentar la adopción del dominio .CO por parte de las empresas colombianas. Para hacer eso, el MINTIC debe continuar haciendo esfuerzos para mejorar el nivel de conectividad dentro del país y mejorar la interconexión e interoperabilidad de las redes a nivel regional. Al mejorar la capilaridad de la red y la integración regional, la adopción y el uso de los servicios de Internet mejorarán y, con ello, el número potencial de usuarios del dominio .CO, tanto a nivel local como internacional.

Esta sección proporciona una descripción del mayor riesgo que se ha identificado en la transición y la implementación del dominio .CO y presenta un análisis de sensibilidad de la economía relacionada con el mercado en Colombia, destacando las variables que son más sensibles al modelo financiero. Además, esta sección presenta aspectos específicos a considerar en la revisión de precios de los servicios de back-end proporcionados por el administrador y recomendaciones específicas relacionadas con los criterios de evaluación.

4.3.1. Identificación del mayor riesgo

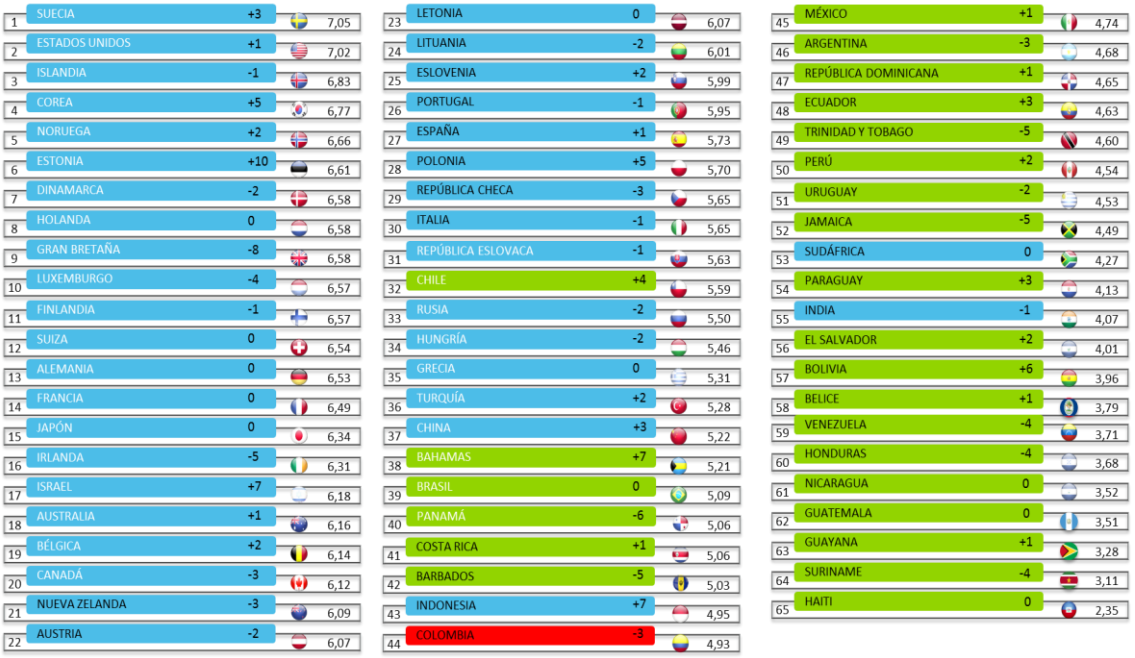
Teniendo en cuenta el análisis de mercado, podríamos identificar el siguiente conjunto de riesgos y estrategias de mitigación relacionados con la ejecución del proyecto.

Tipo de Riesgo	Evaluación de riesgo	Descripción del riesgo	Comentarios - Mitigaciones
Mercado	Bajo	El desarrollo del mercado parece bastante predecible a medio / largo plazo, con un riesgo asociado de considerar un nivel de crecimiento más bajo para el ccTLD y el dominio de segundo / tercer nivel que se consideró en el escenario base.	El mercado de dominios se comporta bastante predecible con una demanda que se ha mantenido bastante estable durante los últimos 10 años. Sin embargo, es importante que el ganador de la licitación dedique suficientes recursos a la comercialización y promoción del dominio .co. El análisis de sensibilidad que se presenta a continuación muestra la importancia de los esfuerzos en esta dirección..
Competencia	Medio	Se espera que este riesgo aumente en el tiempo, cuando los competidores introducen nuevas estrategias de marketing y promoción para promover nuevos servicios e innovaciones que surjan de la introducción de nuevas tecnologías asociadas a 5G, IoT, etc.	Los aspectos que podrían mantener a los competidores en una posición débil son: • Precios competitivos. Los competidores en el dominio .CO no tienen una base de clientes como la que se ha logrado a través del tiempo, por lo que es importante continuar trabajando para mantener la base de clientes existente a medida que se realizan nuevos esfuerzos para captar nuevos clientes. • Implementar una campaña agresiva de marketing / promoción y estrategia de ventas. El ganador de la licitación debe implementar un plan detallado para promover el dominio .CO para que los nuevos usuarios potenciales sean capturados. Se debe incluir

Tipo de Riesgo	Evaluación de riesgo	Descripción del riesgo	Comentarios - Mitigaciones
			esto como parte de los criterios de evaluación.
Implementa-ción	Medio	La gestión de la transición entre el administrador existente y el nuevo podría ser una complicación que podría comprometer la marca y la reputación del dominio .CO	El ganador de la licitación debe definir una estrategia clara sobre cómo se puede llevar a cabo la transición. Se deben incluir medidas de seguridad específicas como parte de la licitación y en los criterios de evaluación para asegurarse de que la transición sea fluida (en caso de que el ganador sea diferente al administrador existente).
Tecnología, Riesgo técnico de largo plazo	Medio	Puede haber problemas de calidad relacionados con la migración.	Incluir un Acuerdo de nivel de servicio específico en el proceso de licitación y una referencia específica en los criterios de evaluación relacionados con este problema será clave.
Pérdida del control de costos	Medio	El éxito y la alta rentabilidad pueden atenuar la gestión de la atención a los costos de cualquier categoría	El ganador de la licitación puede tomar las decisiones correctas a largo plazo en términos de Capex, favoreciendo las tendencias a largo plazo para mantener o aumentar el Opex relacionado con la promoción y la comercialización en lugar de las decisiones a corto plazo relacionadas con los gastos en efectivo.

La siguiente figura resume en un punto de referencia el nivel de desarrollo de banda ancha en Colombia frente a otros países de la Región y la OCDE.

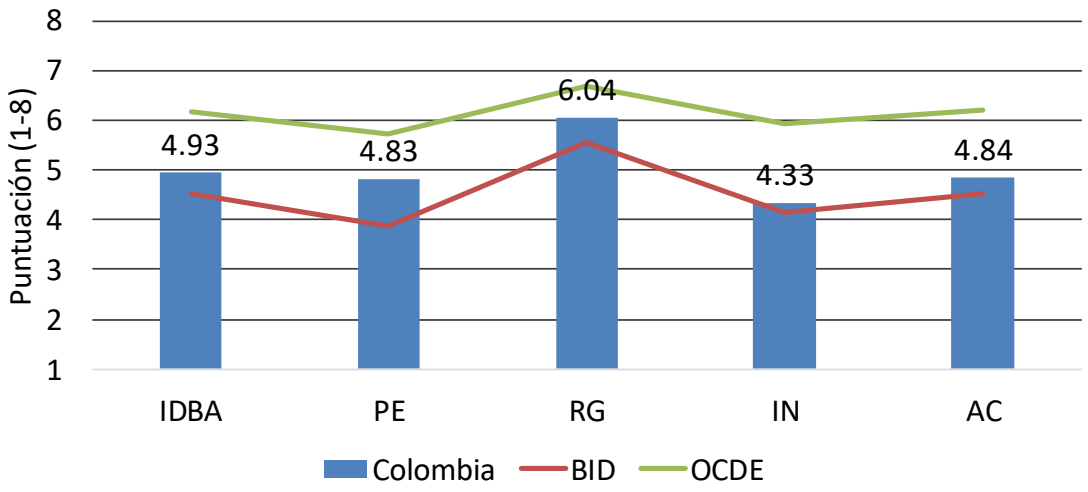
Figura 1 Comparación en el desarrollo de la banda ancha



Como se puede ver en la Figura anterior, para promover localmente el uso del dominio .CO, el gobierno debe continuar realizando esfuerzos para mejorar el nivel de infraestructura disponible, así como la asequibilidad de los servicios de Internet.

El índice de banda ancha que el Banco Interamericano de Desarrollo produce cada año destaca áreas específicas en las que el gobierno de Colombia podría prestar especial atención, como se muestra en la siguiente figura:

Figura 2 Areas de intervención colombianas para mejorar el acceso, adopción y uso de servicios de Internet



Hay cuatro pilares claros donde Colombia debe intervenir para mejorar el nivel de acceso, adopción y uso de los servicios de Internet:

- Política pública y visión estratégica (PE).
- Marco normativo. El trabajo existente para actualizar la ley de telecomunicaciones tendrá un gran impacto en la dinamización del mercado (RG)
- Infraestructura (IN)
- Desarrollo de ecosistema digital y alfabetización digital (AC)

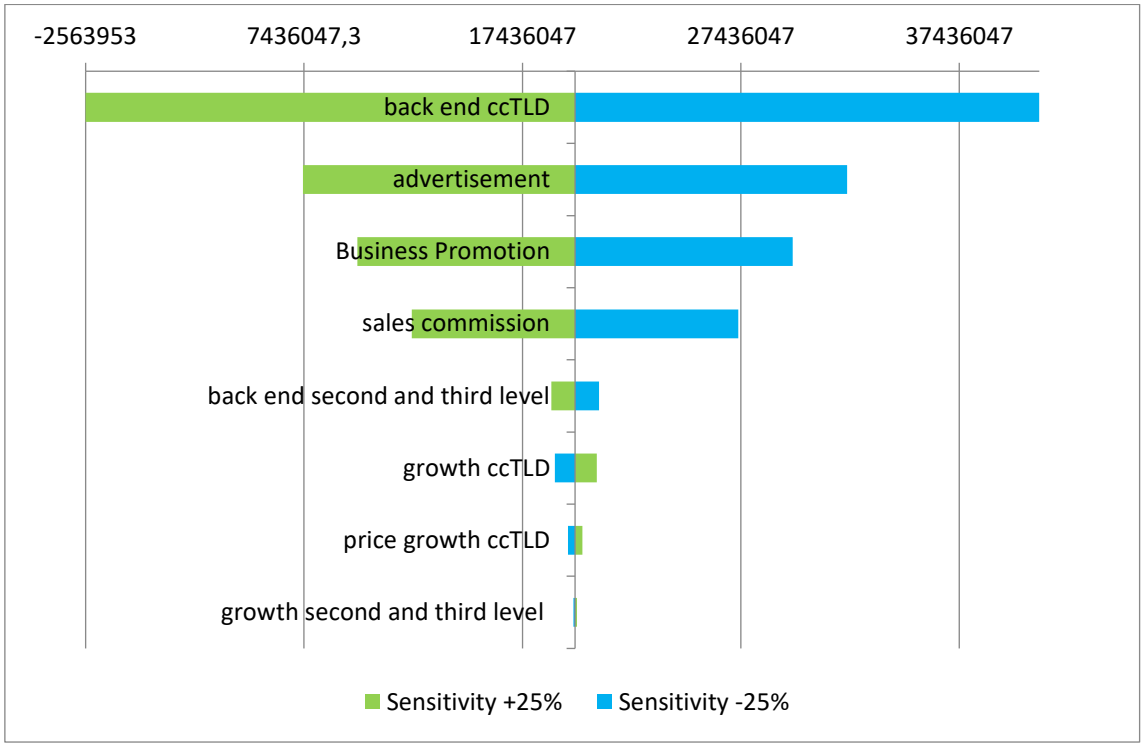
4.3.2. Escenarios considerados en la evaluación del modelo financiero relacionado con el dominio .CO

Para implementar el análisis de sensibilidad, se han considerado tres escenarios diferentes:

- **Escenario base:** este escenario presenta la situación actual a la que se enfrenta MINTIC, donde solo mantiene el 7% del precio recibido por el administrador, se espera que la demanda de ccTLD crezca a un ritmo del 6% anual, mientras que la demanda del segundo y tercer nivel crece a un porcentaje del 10%. De manera similar, se espera que los precios relacionados con el ccTLD y el dominio de segundo / tercer nivel crezcan anualmente al 2% y se supone que el WACC es 15%.
- **Escenario optimista:** En este escenario, debido a la nueva licitación que se espera lanzar en 2019, MINTEL puede reducir los costos de back-end hasta $ 2 por dominio (tanto para ccTLD como para dominios de segundo / tercer nivel) y la demanda de ccTLD de segundo/tercer nivel se espera que crezca a un ritmo del 16% y 20%, respectivamente, gracias a la agresiva campaña de marketing y promoción que el nuevo administrador está lanzando. El WACC permanece en 15%.
- **Escenario pesimista:** Este escenario se caracteriza por una situación en la que los precios de ccTLD y el dominio de segundo / tercer nivel permanecen invariables para mantener el dominio .CO competitivo y se espera que la demanda de cada tipo de nivel crezca a un 3% y un 5% anual. También hay una campaña intensiva de promoción y marketing para mantener el posicionamiento en el mercado del dominio .CO.

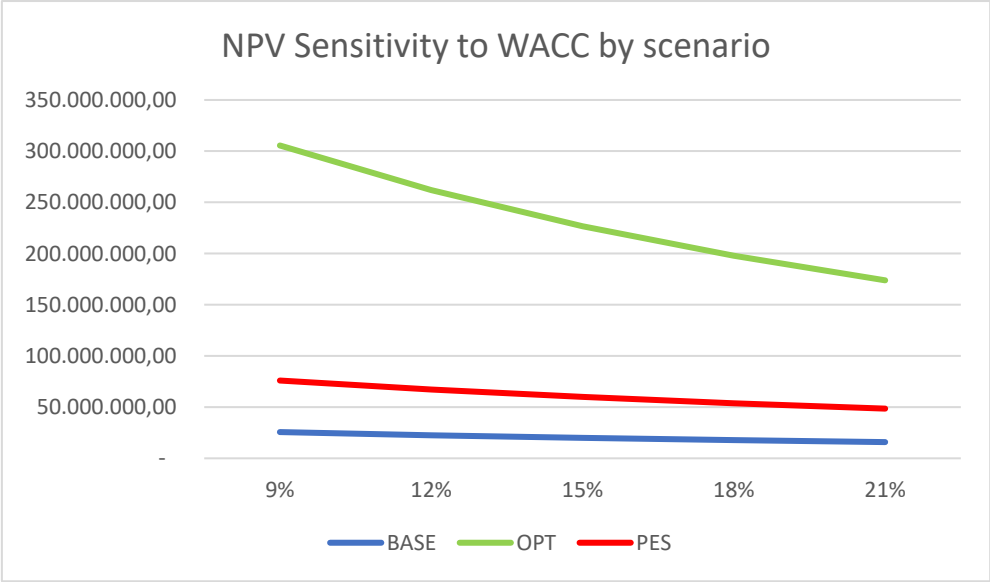
Al realizar un análisis Tornado, podemos ver que las variables que tienen un mayor impacto en el VAN son el costo relacionado con el back-end para ccTLD y los costos asociados de marketing, promoción y comisión de ventas..

Figura 3 Análisis Tornado



A continuación se pueden encontrar algunas de las sensibilidades del VAN a las modifcaciones de estas variables y el WACC.

Figura 4 Sensibilidad del VAN al WACC



Como puede verse en la figura anterior, incluso en una situación como el escenario pesimista, si MITIC es capaz de negociar los términos y condiciones relacionados

con el servicio de back-end y la comercialización y promoción, el Ministerio obtendría ingresos adicionales a los que está recibiendo actualmente. Esto demuestra cuánto se necesita una revisión del contrato existente y cómo el continuar con el administrador existente en las mismas condiciones afecta negativamente al modelo financiero. Como se puede ver, cuanto mayores sean los costos de oportunidad (medidos por el WACC), más bajo será el VAN.

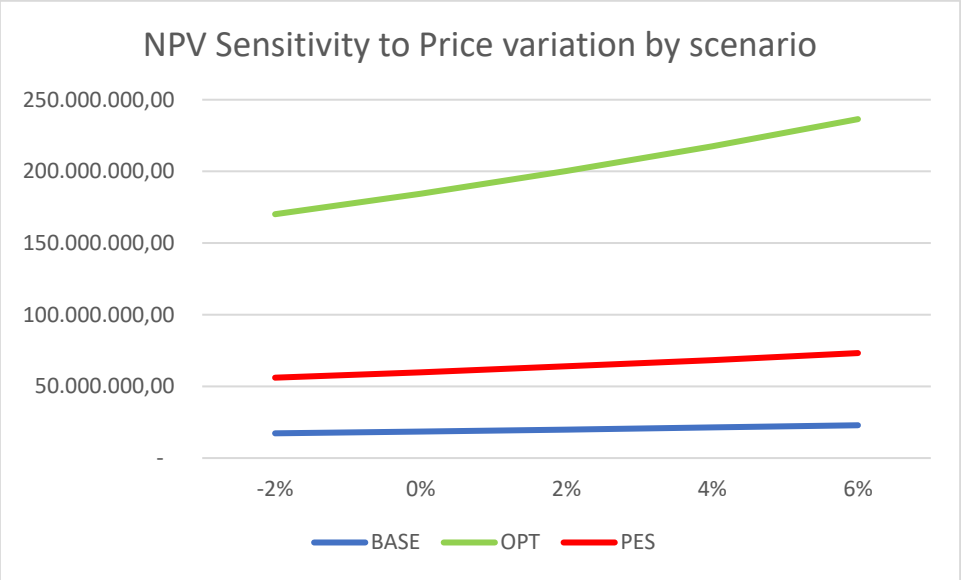
Tabla 1 Sensibiliad del VAN a variaciones en el WACC

WACC	**NPV**		
	BASE	**OPT**	**PES**
9%	25,638,979.37	305,531,437.29	75,986,303.65
12%	22,464,803.44	262,073,428.73	67,177,367.12
15%	19,845,516.38	226,746,783.28	59,857,432.54
18%	17,665,491.12	197,786,216.99	53,722,511.75
21%	15,836,232.38	173,852,257.76	48,538,970.04

De manera similar, si hacemos el mismo ejercicio para analizar la variación del VAN a los cambios en el precio para el ccTLD y el dominio de segundo / tercer nivel, podemos observar que incluso si el precio sigue siendo el mismo, el impacto positivo de reducir el monto de US $ pagado a la administrador del servicio de back-end y marketing y promoción hace que el VAN en el escenario pesimista sea mejor que el escenario base, donde se espera un incremento en el precio para ccTLD y un dominio de segundo / tercer nivel de 2%.

Figura 5

Sensibilidad VANa variaciones en precio del ccTLD y segundo/tercer nivel



Como puede verse en la Tabla siguiente, incluso si no hay crecimiento en el precio para ccTLD y en dominios de segundo / tercer nivel, el VAN es positivo, lo que nos dice que el escenario base es en realidad el caso más pesimista / peor para MINTIC.

Tabla 2

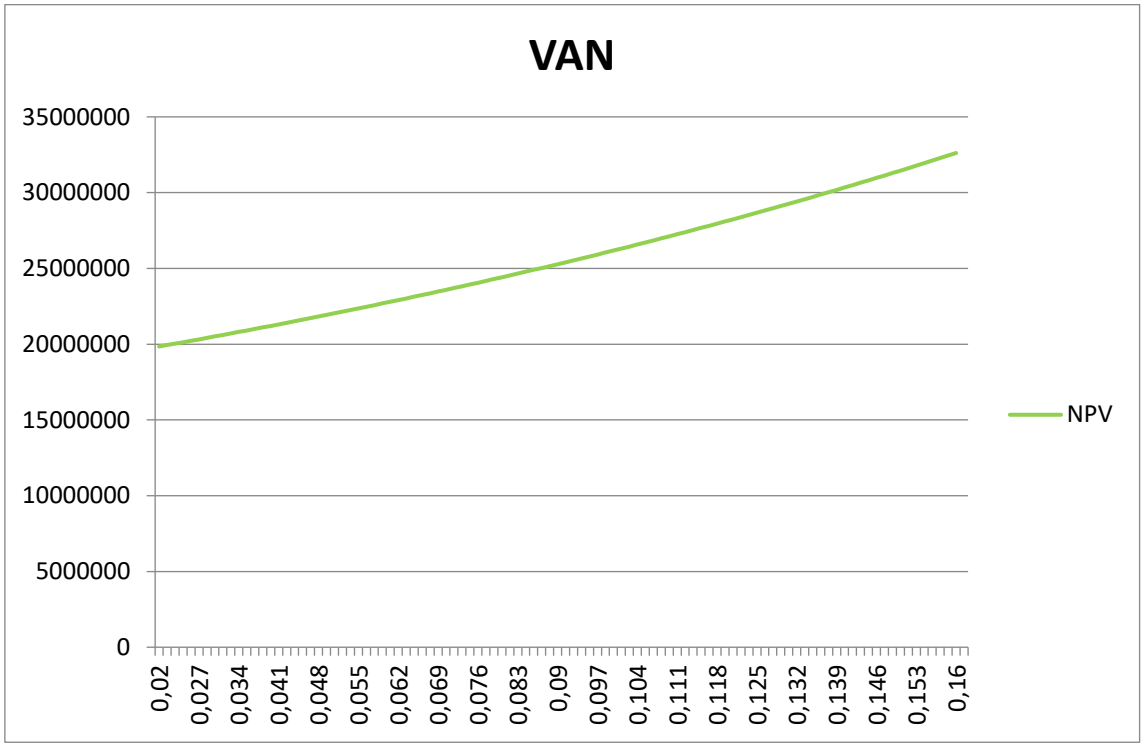
NPV sensitivity to variations in the price for ccTLD and second/third level domain

PRICE	NPV		
	BASE	OPT	PES
-2%	17,271,626.88	170,144,086.76	56,091,665.48
0%	18,502,704.05	184,465,593.67	59,857,432.54
2%	19,845,516.38	200,200,437.32	63,954,478.42
4%	21,310,080.39	217,481,690.01	68,411,961.41
6%	22,907,212.11	236,453,389.72	73,261,339.86

De manera similar, si observamos la sensibilidad del VAN a la variación en el precio, podemos concluir (como se esperaba) que, en general, el VAN siempre es positivo.

Figure 6

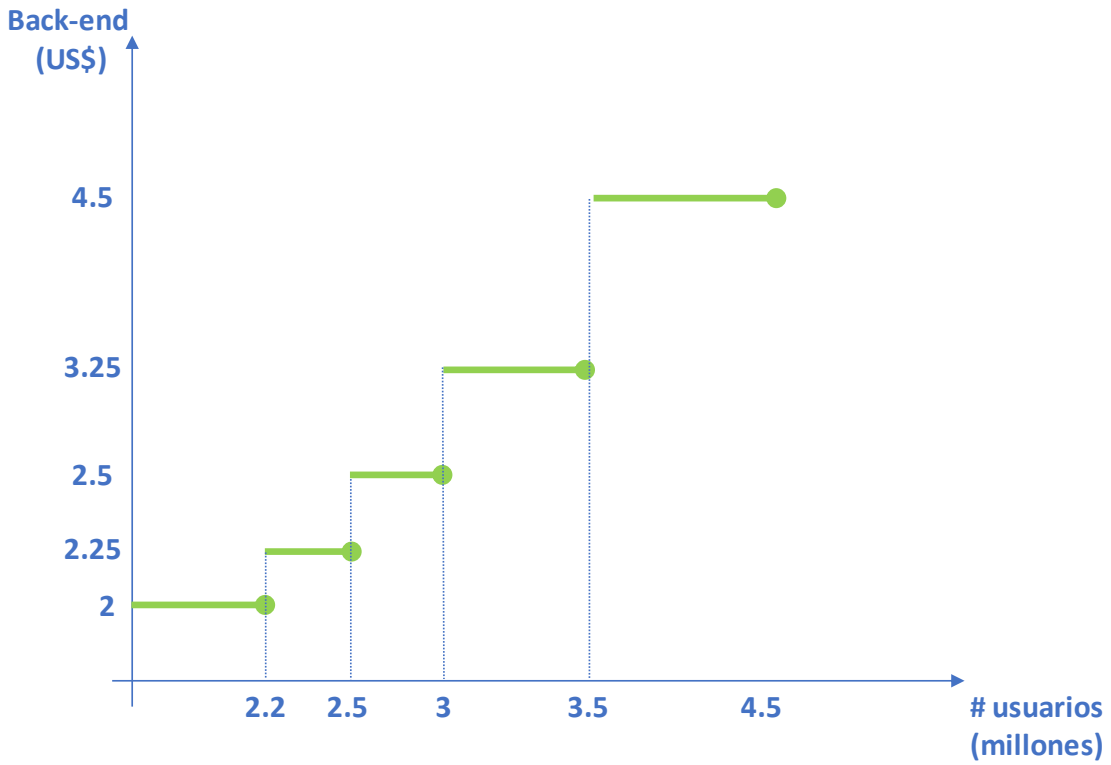
Analisis de Sensibilidad a variaciones en el precio del ccTLD



Teniendo en cuenta la sensibilidad del modelo financiero a la variación del precio del servicio de back-end, es importante proporcionar al administrador potencial los incentivos económicos para aumentar el número de usuarios del dominio .CO. Para alentar el diseño de una estrategia de marketing y promoción, MINTIC podría definir una estrategia de precios servicio de back-end como la que se muestra a continuación y podría incorporarse como parte de los criterios de retribución en el documento de licitación que se publica.

Figure 7

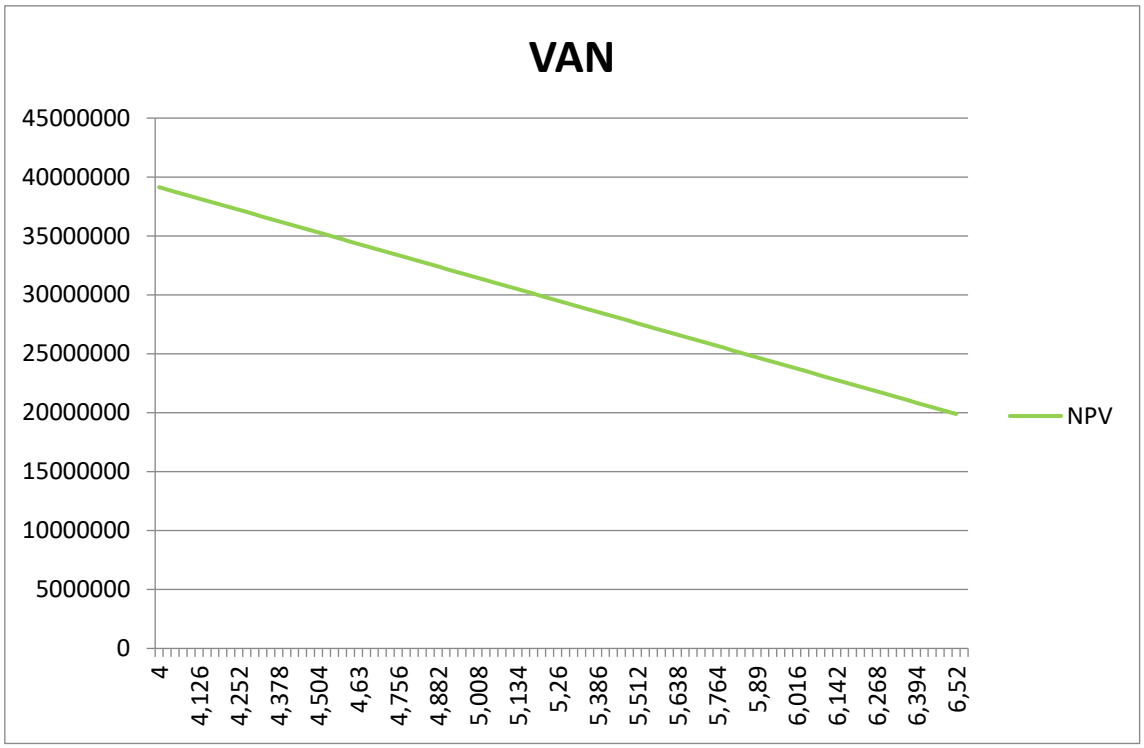
Precio del back-end dependiendo de nuevos usuarios captados por el administrador potencial



Sin embargo, en el caso de los gastos relacionados con la comercialización, el impacto resulta contrario. Cuanto más gastos (ceteris paribus), más bajo es el VAN:

Figura 8

Análisis de sensibilidad a varaiaciones en los gastsos de marketing



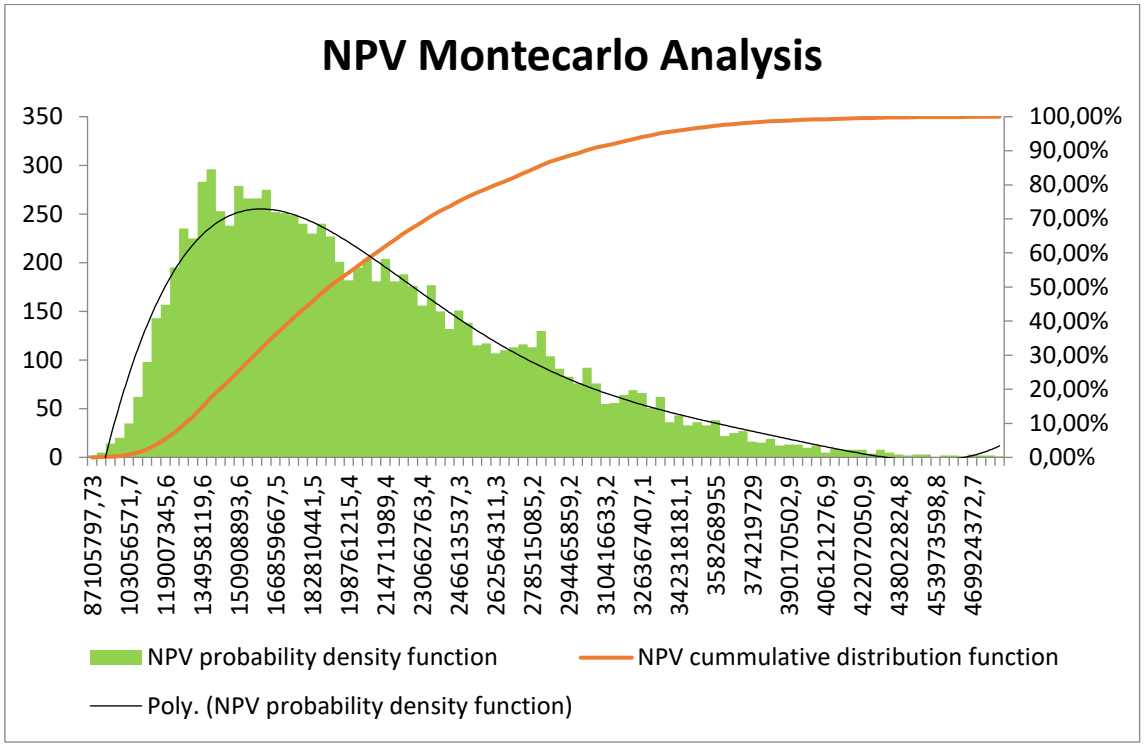
Ejecutando un análisis de Montecarlo con 10,000 simulaciones, se observa que en más del 99% de los casos, el VAN del proyecto es positivo.

Tabla 3 Resultados del Análisis de Montecarlo

Confidence Intervals		
	min NPV	max NPV
99%	104,600,194.98	394,556,965.78
95%	118,092,970.07	333,185,076.62
90%	127,585,317.42	301,617,700.78
80%	142,570,989.00	262,890,577.11
70%	157,804,904.86	232,825,580.17

El promedio esperado de VAN asociado al proyecto es positivo y ronda los US $ 204 millones.

Figura 9: Resultados del Análisis de Montecarlo con 10,000 iteraciones



Ver excel para mayor detalle.

Como se puede concluir del análisis, el dominio .CO es claramente una fuente de ingresos y los ingresos mensuales podrían ser una manera perfecta de financiar los proyectos existentes en la infraestructura de la última milla en la que está involucrado MITIC. El vehículo para hacer eso son los llamados bonos digitales que podrían ser respaldados por la titularización de los ingresos anuales que se espera que MITIC obtenga del dominio .CO. La titulización de estos recursos podría ayudar al gobierno de Colombia a tener acceso en el presente a los ingresos futuros que se esperan de la renovación y provisión del dominio .CO. El acceso a esta gran cantidad de dinero (aproximadamente US $ 204 millones) se podría dedicar a la implementación de proyectos de infraestructura de última milla que eventualmente acelerarán la digitalización de la sociedad en Colombia.

ASPECTOS ECONOMICOS Y FINANCIEROS

4.3.3. Aspectos cualitativos a incluir en la licitación

La siguiente lista pretende identificar los criterios básicos que todos los oferentes deben tener para calificar como administradores del dominio .CO:

- El administrador potencial, en el momento de la presentación de la propuesta, deberá proporcionar servicios de dominio similares a la licitación a al menos 4.500.000 usuarios. Este criterio se confirmará proporcionando información sobre el informe trimestral más reciente;
- El administrador potencial, en el momento de la presentación de la propuesta, no tendrá deudas con el Estado de Colombia. Este criterio deberá ser confirmado por la certificación emitida por la Administración Tributaria de Colombia (no más de 3 meses contados a partir de la fecha de presentación de la propuesta);
- El administrador potencial deberá proporcionar una Prueba del Tribunal de Comercio de que no se encuentra en un proceso judicial o previamente condenado por un delito penal, y que no está en el caso de quiebra o liquidación, no más de tres meses antes de la presentación del laudo.
- El administrador potencial deberá estar registrado como operador económico en el Registro de Negocios de Colombia. Este criterio se confirmará con la copia del Certificado de Registro de Empresas, el Certificado de Número Fiscal y una copia del Certificado de IVA

4.3.4. Aspectos cuantitativos a incluir en la licitación

Además de los aspectos cualitativos que debe incluir la licitación, habrá indicadores adicionales provenientes de la implementación del decreto 1082/2015 y que se establecen en la siguiente tabla:

Tabla 4: Financial indicators requested by Decree 1082/2015

INDICADOR	FORMULA	MARGEN SOLICITADO
Liquidez	Activo corriente sobre pasivo corriente	Mayor o Igual a 1.0
Nivel de endeudamiento	Pasivo total sobre activo total	Menor o Igual a 70%
Razón de Cobertura de Intereses	Utilidad operacional sobre gastos de intereses	Mayor o Igual a 1.0
Capital de Trabajo	Activo Corriente menos Pasivo Corriente	Mayor o igual a 10% del presupuesto oficial
Patrimonio	Activo Total menos Pasivo Total	Igual o mayor al 15% del presupuesto oficial
Apalancamiento a Corto Plazo (Solo para ESAL con Utilidad Operacional Negativa).	Pasivo Corriente sobre Total Patrimonio	Mayor o Igual a 0

INDICADOR	FORMULA	MARGEN SOLICITADO
Rentabilidad del Patrimonio	Utilidad Operacional sobre Patrimonio	Igual o Mayor a 0
Rentabilidad del Activo	Utilidad Operacional sobre Activo Total	Igual o Mayor a 0
Capital de Trabajo (Solo ESAL con Utilidad operacional negativa)	Activo Corriente menos Pasivo Corriente	Positivo
Patrimonio (Solo ESAL con Utilidad Operacional negativa)	Activo Total menos Pasivo Total	Positivo

Otros indicadores adicionales que podrían ser considerados son:

- Declaración financiera preparada y firmada por un auditor con licencia para los últimos 3 (tres) años (2018, 2017 y 2016) a partir de la fecha del anuncio de la Solicitud de solicitudes (se adjuntará una copia certificada ante notario de la licencia del auditor) o la Declaración anual emitida por la Administración Tributaria;
- Los ingresos totales de las actividades relacionadas del administrador potencial durante los últimos 3 años (2018, 2017, 2016) serán iguales o más al máximo del valor total estimado del contrato. Los ingresos de otras actividades deben excluirse de la comparación.
- En caso de ser seleccionado y antes de firmar el contrato, una garantía del banco estándar o compañía de seguros autorizada por el Banco Central a favor de MITIC por el 10% del valor del contrato por el período de implementación.

4.3.5. Aspectos económicos relacionados con los criterios de evaluación

Todos los oferentes que hayan pasado el control de elegibilidad y la evaluación serán considerados para una evaluación adicional como se describe a continuación.

El objetivo de esta evaluación es seleccionar el más económico y técnicamente, incluso en términos de presupuesto, un administrador potencial ventajoso para administrar y explotar comercialmente el dominio .CO en las condiciones más rentables para MITIC. Como hemos visto, la reducción en el nivel existente de back-end y la consideración de los gastos específicos de marketing y promoción deben ser altamente valorados.

La evaluación de la propuesta debe llevarse a cabo en función de los métodos de evaluación y las ponderaciones que utilizará el comité de evaluación. Los criterios para evaluar los administradores potenciales podrían ser:

1. *Criterio económico:* La propuesta económica será valorada en 50 (cincuenta) por ciento del total de puntos. Los puntos se calcularán aplicando el método de evaluación definido por la fórmula que se describe en la tabla a continuación. La razón para poner un porcentaje tan grande para la

propuesta económica se debe a los enormes costos que MINTIC debe pagar hoy al administrador existente. En futuras licitaciones, este porcentaje podría reducirse una vez que las cifras se ajusten al mercado.

1.1 Costo del Back-End. Por cada 20% de reducción en la tasa actual, el administrador potencial recibirá 10 puntos.

2. *Criterio técnico:* Los criterios técnicos se valorarán en un 50 (cincuenta) por ciento del número total de puntos, teniendo en cuenta la documentación técnica relevante. Los criterios técnicos podrían ser evaluados considerando, entre otras, las siguientes variables:

2.1 Plan de transición - 15 puntos;

2.1.1 Plan de trabajo dinámico, que indica la hora de inicio y finalización del proyecto de transición, así como el tiempo total de la implementación, incluidas las diferentes fases requeridas para el éxito.

2.2 Plan de implementación - 25 puntos;

2.2.1 Cumplimiento de SLA, por cada punto porcentual adicional después de un mínimo de 99,5%, el potencial administrativo recibirá 5 puntos.

Como ilustración, la tabla a continuación presenta los acuerdos de nivel de servicio definidos por Vanuatu en la última licitación.

Tabla 5: *SLAs defined by Vanuatu (.vu) in the last tender*

Service Level Standard	Target
DNS Practice Statement Acceptance	DNS Practice Statement to be accepted by the community that .vu serves.
DNS Performance	For UDP – handle 100 qps with ≤ 5 ms average latency For TCP – handle 100 qps with ≤ 50 ms average latency
DNS Server Planned Outages	Single outages ≤ 4 hours Total outages ≤ 8 hours / month No more than two .vu Name Servers should be scheduled for a planned outage at the same time
DNS Integrity	100 % correct and consistent outside Zone Push window
DNS Server Availability	≥ 99 % availability over the month. ≥ 95 % availability over any 24 hour period. respond to ≥ 99 % of queries. No more than two .vu Name Servers may be unavailable at any one time, whether for planned or unplanned outages.
DNS Zone Push (from primary to secondary DNS Servers)	≥ 6 Zone Pushes per day ≤ 60 minutes DNS Zone Push Window

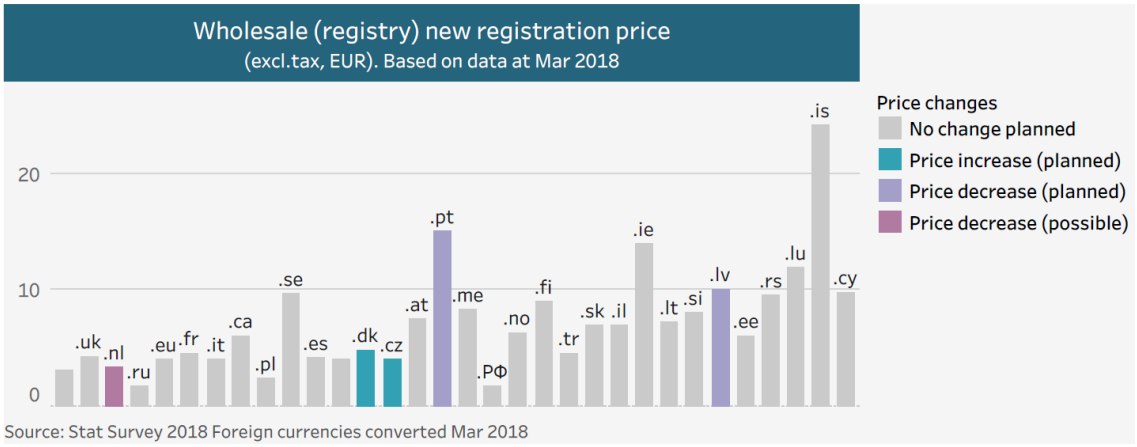
2.3 Plan de marketing y promoción – 10 puntos;

2.3.1 Plan de trabajo estratégico dinámico durante todo el período de la concesión, incluida la estrategia de publicidad, desarrollo de negocios y comisiones de ventas, entre otros.

4.3.6. Comparación de precios mayoristas

A continuación se presenta un punto de referencia con los precios al por mayor para ccTLD.

Figura 10: Comparación de precios mayoristas de ccTLD



Wholesale Prices | Ex-tax, 1Y new registration. Foreign currencies converted to EUR at Mar 2018

	New	Renew	VAT/tax
.at	7.5	7.5	0.2
.be	4.0	4.0	0.2
.ca	6.1	6.1	0.1
.cy	9.8	13.0	0.2
.cz	4.1	4.1	0.2
.de	3.1	NA	0.2
.dk	4.8	4.8	0.3
.ee	6.0	6.0	0.2
.es	4.1	4.1	0.2
.eu	4.0	3.8	NA
.fi	9.0	9.0	0.2
.fr	4.6	4.6	0.2
.ie	14.0	14.0	0.2
.il	7.0	7.0	NA
.is	24.1	24.1	0.2
.it	4.0	3.3	0.2
.lt	7.3	7.3	0.2
.lu	12.0	12.0	0.2
.lv	10.0	10.0	0.2
.me	8.3	8.3	0.2
.nl	3.4	3.4	0.2
.no	6.2	6.2	0.3
.pl	2.4	9.5	0.2
.pt	15.0	15.0	0.2
.РФ	1.7	1.7	0.2
.rs	9.5	9.5	0.2
.ru	1.7	1.7	0.2
.se	9.6	9.6	0.3
.si	8.0	8.0	0.2
.sk	7.0	10.0	0.2
.tr	4.5	4.5	0.2
.uk	4.3	4.3	0.2

Foreign currencies converted Mar 2018
Special cases: .ro - ROTLD has not yet implemented yearly fees for domain names. Domains are registered with one initial fee and are not deleted, except if requested by registrant or if in violation of ROTLD agreements.

4.3.7. Principios a considerar

- Principio de **no discriminación**. Todas las solicitudes están sujetas a las mismas reglas, independientemente del número de dominio del solicitante, la nacionalidad, la forma legal, el lugar de residencia o el registro y otras características individuales.
- Principio de **equidad**. El Registro no tiene ningún interés personal con respecto a la atribución del nombre de dominio a una u otra persona; por lo tanto, no es una parte a la que le corresponda abordar las cuestiones relacionadas con los derechos o intereses legales en las etiquetas utilizadas por los solicitantes de registro en los nombres de dominio.
- Principio de **exactitud de los datos**. Los solicitantes de registro deben garantizar que sus datos e información sobre el dominio especificado en el sistema de administración de dominios (DAS) sean constantemente correctos.
- Principio de **recompensa**. Por cada procedimiento permitido realizado, a excepción de aquellos sin costo, se debe garantizar el pago de tarifas al Registro. La tarifa es pagada al Registro por los Registradores, incluida en el costo de los servicios prestados a los Registrantes.

CONCLUSIONES

- Para mejorar el número de usuarios locales de .CO, Colombia debe continuar trabajando en la promoción de la universalidad de los servicios de banda ancha a nivel local y regional. La siguiente tabla presenta los desafíos para el Desarrollo del Acceso Universal de Banda Ancha y las estrategias para superarlos..

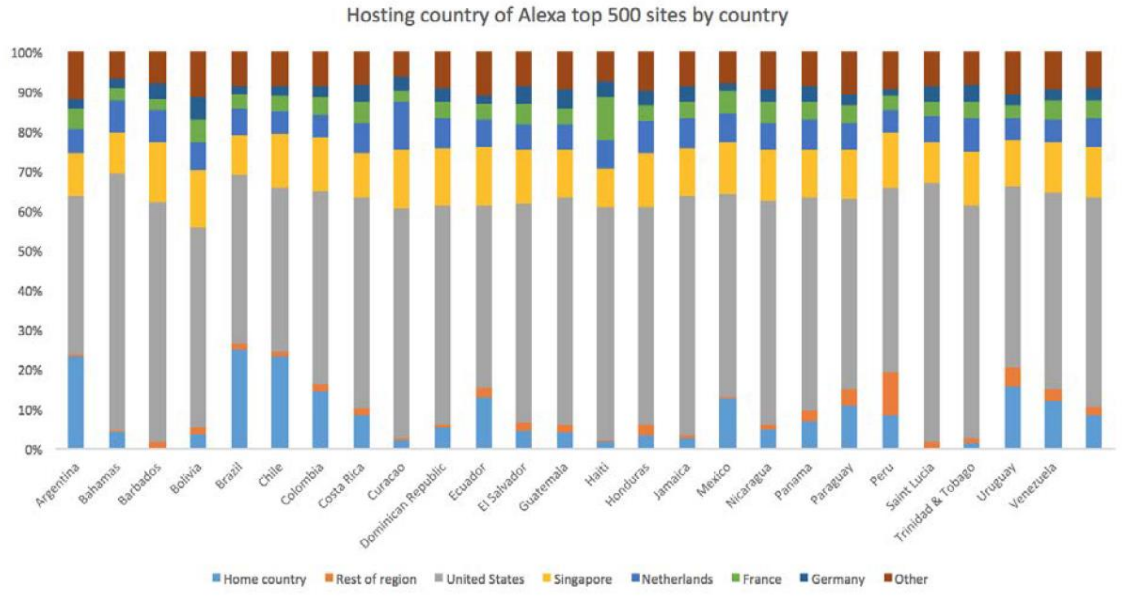
Tabla 6: Desafíos y estrategias en el desarrollo del Servicio Universal

	Desafíos	Estrategias
Demanda	Bajo nivel de poder adquisitivo y precios de servicio relativamente altos. Bajo nivel de educación, especialmente en habilidades TIC. Disponibilidad limitada de (y altos impuestos sobre) equipos electrónicos de consumo Disponibilidad limitada de contenido local relevante	Subvenciones por tarifas de servicios o compras de equipos. Descuentos obligatorios para ciertas clases de usuarios finales Impuestos reducidos para servicios y equipos relacionados con la banda ancha. Capacitación en TIC (en escuelas, institutos, etc.) Telecentros públicos
Oferta	Recursos financieros limitados, en general Infraestructura limitada en el país, especialmente redes nacionales de fibra óptica, e infraestructura limitada o muy costosa para conectividad internacional Cantidad limitada de espectro disponible para banda ancha inalámbrica Cobertura inadecuada de redes inalámbricas de banda ancha. Perspectivas limitadas para el crecimiento económico	Impuestos a los operadores para financiar a las FFU Fuentes adicionales de financiamiento (por ejemplo, de instituciones internacionales) Subvenciones para construir infraestructura, compartir infraestructura obligatoria Priorización de programas de desarrollo basados en criterios estrictos. Despliegue de WiFi público en espacios públicos. Reordenamiento del espectro

- La economía del mercado .CO es muy sensible a la variación en el precio de back-end al por mayor y la implementación de una estrategia de comercialización, promoción y comisión de ventas;
- El contrato con el administrador potencial debe definir una estrategia de precios al por mayor que aliente al nuevo administrador a tomar un rol activo para aumentar el número de usuarios de .CO;
- Las especificaciones de los indicadores económicos y financieros, aunque en línea con la legislación colombiana, también deben proporcionar señales claras a los oferentes en cuanto a lo que realmente importa para el MINTIC. Por lo tanto, dado que la retribución que está obteniendo el Ministerio está claramente

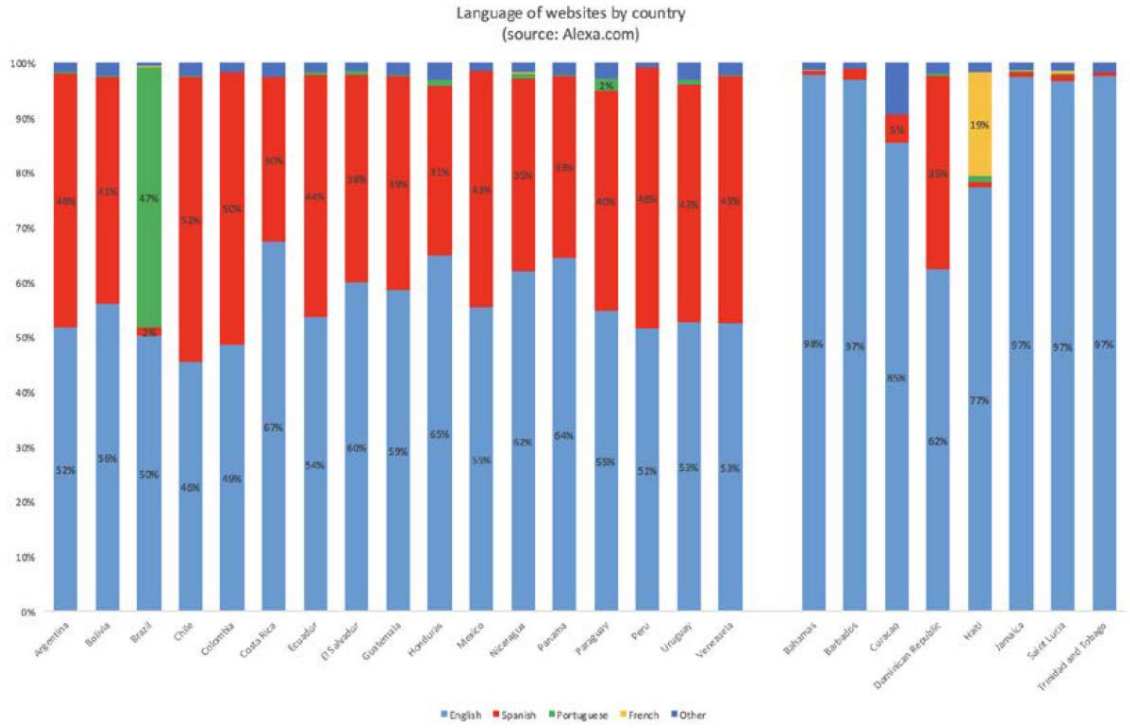
por debajo del índice de referencia internacional, una forma de indicar a los posibles oferentes la importancia de mejorar esto es aumentar el peso de la propuesta financiera;

- La licitación debe tener en cuenta los principios de no discriminación, imparcialidad, exactitud de los datos y recompensa;
- El modelo financiero relacionado con el dominio .CO es claramente rentable, en un modelo de Montecarlo de 10.000 iteraciones, el VAN promedio esperado para un período de 10 años será de $ 204 millones. Sin embargo, el modelo es muy sensible a las variaciones en el precio de back-end al por mayor y a los gastos relacionados con la comisión de comercialización, promoción y ventas;
- De un estudio reciente publicado por ICANN, más de la mitad del total de ccTLD de LAC ha decidido externalizar total o parcialmente las operaciones de back-end;
- El ccTLD en América Latina tiene diferentes esquemas de precios dependiendo de variables tales como: (i) Nuevos registros o renovación de un registro existente, (ii) Precio al por mayor para administradores, (iii) Nacionalidad o país de residencia del registro, (iv) Tipo de nombre (name.xx o second level name.com.xx), (v) Diferentes tipos de extensiones para el dominio de segundo nivel (.org.xx; .edu.xx; etc.);
- Para aumentar el número de .CO localmente, es necesario reducir la dependencia de los sitios extranjeros. Como puede verse en la figura a continuación, la mayoría de los sitios preferidos visitados por colombianos no se encuentran localmente sino en el extranjero:



- Para reducir esta dependencia de los sitios internacionales, el gobierno debe continuar realizando esfuerzos en el despliegue de infraestructura digital a nivel local y regional, mediante la mejora de la interconexión de Colombia con otros países de la Región y la creación de IXP regionales específicos que agreguen tráfico y faciliten la ubicación de hosts para contenido digital;

- Al mismo tiempo, la creación de contenido local debe venir con sitios escritos en español, lo que, como puede verse, también es un desafío. En resumen, podemos decir que aumentar el porcentaje de usuarios locales de .CO va más allá de las capacidades del administrador, pero se basa más en políticas específicas relacionadas con la mejora de la conectividad y la creación de contenido local en el idioma local (consulte la figura a continuación).



5. Parte 5 (Ref: 2.2.4)

Presentar estudios con las recomendaciones respecto a los siguientes aspectos y condiciones para diseñar un proceso de selección objetiva que permita la administración eficiente del ccTLD de Colombia, .co

5.1. Establecer los requisitos mínimos (funcionales, de infraestructura de software y hardware, personal, entre otros) que deben cumplir los interesados para ser un potencial concesionario para la administración eficiente del ccTLD de Colombia, .co

ANALISIS:

Como se indica en el Entregable 5.2, la mayoría de las RFP no enumeran / establecen requisitos mínimos (infraestructura de software y hardware, personal) que deben cumplir las partes interesadas para administrar de manera eficiente el ccTLD .CO. En su lugar, tienden a centrarse en los productos entregables según lo establecido en los Acuerdos de Nivel de Servicio. De esta manera, los operadores de registro pueden innovar y proponer diferentes configuraciones de hardware y software para cumplir o superar los estándares existentes.

Con el fin de proporcionar los puntos de datos constructivos del gobierno de Colombia para formular una RFP, este análisis implica la revisión de cinco ofertas recientes de RFP de TLD (4 ccTLD y 1 gTLD) para identificar los criterios comunes que se propusieron en estas RFP..

A. <u>Shared Registry System (Servicio de Registro Compartido: SRS)</u>

SRS es el conjunto de registro central al que los registradores acceden a través de una conexión segura mediante del protocolo EPP para realizar transacciones con el Registro. Para cumplir con los requisitos de SLA, este conjunto se suele alojar en centros de datos geográficamente redundantes, uno designado como principal y el otro como recurso activo. Algunas RFP han solicitado que los licitadores proporcionen pruebas de su capacidad de recuperación ante fallos, comp por ejemplo poder cambiar sin problemas entre sistemas primarios y secundarios..

Hay varios requisitos que algunos contratistas han incluido en su RFP en función de necesidades específicas, estos requisitos de adición incluyen, entre otros:

Volumen máximo de transacciones: algunas RFP requerirán que un encuestado de RFP demuestre las transacciones máximas en un volumen de registro múltiple (por ejemplo, 3X o 5X) por encima del volumen esperado. Esto se hace para asegurar el crecimiento futuro y la escalabilidad. En el caso de que el proveedor de infraestructura de registro aloje el TLD en un complejo compartido (por ejemplo, otros TLD que se ejecutan en las mismas máquinas), este número máximo puede usar un multiplicador más alto (por ejemplo, 10X);

- Bloqueo de registro: esta es una característica de seguridad que le permite a un registrante bloquear el nombre de dominio por motivos de seguridad en el nivel de registro;
- Función de sincronización de dominio: esto permite a los solicitantes sincronizar su cartera de nombres de dominio con una fecha de renovación común;
- Validación del registrante: un número creciente de solicitudes de propuestas (RFP) requieren la validación de los datos del registrante, ver el Anexo A.
- Soporte para revendedores: el sistema SRS puede requerir la necesidad de registrar revendedores además de registradores.
- Declaración de normas comerciales, por ejemplo, Renovar Período de Gracia, Pendiente de Eliminar, Transferir. Si el registro de ccTLD tiene una gran parte de los registradores acreditados por ICANN, la RFP generalmente tratará de mantener las mismas políticas de consenso que el gTLD de la ICANN para conservar la uniformidad.
- Kit de herramientas de desarrollo de software (SDT) del Protocolo de aprovisionamiento extensible (EPP): este kit de herramientas se proporciona a los registradores para permitirles establecer una conexión segura con la plataforma de registro, por ejemplo SRS, facturación, administración.

B. Servicios DNS

Los servicios de DNS generalmente requieren una constelación global de servidores (primario y secundario) para garantizar los tiempos de respuesta de SLA correctos. Los servicios de DNS casi siempre requieren un tiempo de actividad del 100%. Por lo general, también es un requisito que el operador de registro cumpla con las RFC

relevantes y existentes y las publicadas en el futuro por el Internet Engineering Task Force (IETF), incluidas todas las normas sucesivas, modificaciones o adiciones relacionadas con el DNS y las operaciones del servidor de nombres, incluidas pero no limitado a:

- RFC 1034 – Domain names – concepts and facilities (part of STD 13);
- RFC 1035 – Domain names – implementation and specification (part STD 13);
- RFC 1123 – Requirements for Internet Hosts – Application and Support (part ofSTD 3);
- RFC 1982 – Serial Number Arithmetic;
- RFC 2181 – Clarifications to the DNS Specification;
- RFC 2182 – Selection and Operation of Secondary DNS Servers (BCP 16);
- RFC 3226 – DNSSEC and IPv6 A6-aware server / resolver message requirements;
- RFC 3596 – DNS Extensions to Support IP Version 6 (STD 88);
- RFC 3597 – Handling of Unknown DNS Resource Record (RR) Types;
- RFC 4343 – Domain Name System (DNS) Case Insensitivity Clarification;
- RFC 5966 – DNS Transport over TCP – Implementation Requirements; an
- RFC 6891 – Extension Mechanisms for DNS (EDNS(0)) (STD 75).

C. Software

La mayoría de los siguientes software están relacionados con SRS y los sistemas DNS:

- An RFC compliant EPP registry protocol
- Registrar Toolkit (RTK)
- Database (Oracle, PostgreSQL, or equivalent)
- A Relational Database Management System (RDBMS) with Multi-Version Concurrency Control (MVCC) or equivalent;
- Integrated billing solution
- Multi DNS providers

D. Instalaciones y Sistemas

La mayoría de las RFP incluirán una disposición como la que se proporciona a continuación que requiere que el proponente describa las instalaciones y sistemas que albergarán la plataforma de registro propuesta.

Se debe especificar los tipos de sistemas que propone utilizar, y sus ubicaciones geográficas (ciudad y país), capacidad, interoperabilidad, disponibilidad y nivel de seguridad. Proporcionar diagramas de todos los sistemas que operan en cada ubicación. Incluir en su descripción información sobre los edificios, el hardware, el

software, la energía, los equipos ambientales, la conectividad a Internet y otras instalaciones que admitirán su SRS. Si alguna de las instalaciones está ubicada en lugares expuestos a riesgos ambientales más intensos (por ejemplo, terremotos, inundaciones, incendios), describirá cómo se mitigan esos riesgos.

E. Seguridad

Revisar entregable 3.1 para un análisis detallado de los requisitos de seguridad comúnmente incluidos en las RFP de TLD similares.

F. Escrow (fideicomiso)

Escrow es una característica de seguridad clave en caso de una interrupción de los servicios de registro. La mayoría de las RFP requieren que el encuestado:

- Describa su propuesta para realizar los depósitos de datos y otras actividades técnicas;
- Identifique el agente de custodia de datos que propone contratar y describa la forma en que propone administrar la relación de agente.

En relación con la ejecución real del Acuerdo de Registro, el gobierno de Colombia puede desear ser designado como beneficiario del acuerdo de Escrow que le permite acceder a los archivos de custodia en caso de incumplimiento / falla. ICANN tiene acuerdos de escrow modelo (fideicomiso) que el gobierno de Colombia podría querer usar como guía.

G. IPv6/DNSSEC

La mayoría de los RPF incluyen una disposición que requiere que el Operador de registro admita IPv6 y DNSSEC en la operación del registro.

H. Personal relevante

Este requisito varía de RFP a RFP, y no parece haber ningún estándar sobre qué personal clave debe designar un encuestado. Durante la misión de Bogotá en el sitio, se discutió la posibilidad de proporcionar una puntuación mejorada para cierto personal designado con títulos avanzados.

I. Service Level Agreements (SLAs)

Por favor revisar el entregable 3.5 para aplicaciones de niveles de SLA.

J. Inteligencia de Negocios

Basado en una consulta con el gobierno de Colombia, el actual .CO Internet S.A.S. , no se les proporciona acceso al sistema para descargar datos clave de inteligencia empresarial. La RFP PIR para .ORG es un recurso excelente para una RFP que incluya estos tipos de provisión. Esta característica debe incluirse en cualquier futura licitación para garantizar un mejor acceso a los datos clave del Registro para una auditoría independiente.

RECOMENDACIONES:

El gobierno de Colombia debe elegir incluir los criterios enumerados anteriormente según sea necesario para satisfacer las necesidades de MinTIC..

5.2. Determinar las condiciones técnicas mínimas de la infraestructura (hardware y software) necesarias para la administración del dominio .CO ccTLD

ANALISIS:

Es importante tener en cuenta que la mayoría de la RFP y la documentación relacionada no abordan la seguridad y la estabilidad de los TLD en el contexto de la prescripción de hardware y software específicos. En su lugar, tienden a centrarse en los productos entregables según lo establecido en los Acuerdos de Nivel de Servicio. De esta manera, los operadores de registro pueden innovar y proponer diferentes configuraciones de hardware y software para cumplir o superar los estándares existentes.

A modo de ejemplo, antes de la creación de ICANN, Network Solutions operaba los registros .COM, .NET y .ORG con un marco basado en tickets de correo electrónico basado en los identificadores de NIC. Uno de los primeros actos que ICANN realizó para promover la competencia dentro del espacio de nombres fue introducir un mercado competitivo de registradores (minoristas) para los registrantes de nombres de dominio. Para facilitar este nuevo mercado, NSI desarrolló el protocolo de registro de registro (RRP). Sin embargo, después de la ronda de pruebas de concepto de nuevos gTLD de ICANN en el año 2000, Afilias y NeuLevel fueron los primeros operadores de registro en implementar a gran escala el nuevo Protocolo de Provisión Extensible (EPP) en lugar del RRP. Hoy en día, el EPP se ha convertido en el estándar predeterminado dentro de la industria de los nombres de dominio para las comunicaciones seguras entre registros y registradores.

Otro ejemplo de cómo evitar los requisitos de hardware y software que puede llevar a la innovación se ilustra con más detalle en la ronda de prueba de concepto del 2000. Antes de la introducción de las operaciones de registro por parte de Afilias y NeuLevel en 2001, Networks Solutions y su sucesor VeriSign, solo estaban actualizando el archivo de la zona maestra para cada TLD dos veces al día. Sin embargo, después de que Afilias y NeuLevel avanzaron hacia una actualización casi

instantánea (en minutos) de sus zonas, esto estableció un nuevo estándar que la industria que todavía se utliliza.

Si bien EPP es el protocolo de comunicación estándar entre registros y registradores para la mayoría de los gTLD y los ccTLD, es importante tener en cuenta que, dado que el EPP es intrínsecamente extensible, cada código de registro del EPP no es intercambiable. De hecho, existen ligeras diferencias entre el código de la mayoría de los proveedores principales de infraestructura de registro back-end que deben tenerse en cuenta en cualquier posible migración entre proveedores de infraestructura de registro back-end. También es importante identificar cualquier extensión de EPP propietaria que un proveedor de infraestructura de registro pueda proponer usar en la operación del ccTLD .CO. ICANN planteó específicamente este problema de extensiones EPP propietarias en una nueva recomendación de gTLD como parte de la ronda de nuevos gTLD de 2012. [1]

Configuraciones comunes de hardware, software e instalaciones

A pesar del enfoque prudente de no prescribir configuraciones específicas de hardware y software, existen componentes comunes de hardware que el equipo de evaluación técnica probablemente encontrará al revisar cualquier respuesta de RFP a la oferta de .CO. Sin embargo, es importante subrayar que las desviaciones de estas configuraciones no son malas si existe una razón técnica válida proporcionada por el licitante para su uso.

Equipamiento

- Multi-Core processor servers con acceso a energía redundante y conexión a red;
- Load Balancers
- High capacity routers y switches para cumplir con requerimientos del SLA
- Firewalls
- Almacenamiento

Software:

- RFC compliant EPP registry protocol
- Registrar Toolkit (RTK)
- Database (Oracle, PostgreSQL, or equivalent)
- Relational Database Management System (RDBMS) con Multi-Version Concurrency
- Control (MVCC) o equivalente;
- Solución de billing integrada
- Proveedores multi DNS

Instalaciones:

- Centros de datos con diversidad geográfica
- Conectividad entre instalaciones primarias y secundarias a través de conexiones VPN redundantes para asegurar la replicación de datos
- Bifurcación de SRS desde servicios WHOIS / RDDS
- Balanceo de carga en todas las operaciones de registro: puerta de enlace SRS, WHOIS / RDDS, DNS, etc.
- Conexiones redundantes de energía y conectividad a internet
- Instalaciones DDOS reforzadas con capacidades para manejar ráfagas de hasta 10 Gbps de capacidad
- Separar los recursos de OT&E para el registro a bordo independientemente de las instalaciones de producción
- Filtrado de ingreso a la red
- Soporte de IPv6
- Seguridad física

Protocolo Extensible Provisioning (EPP)

Es importante que el gobierno de Colombia garantice el cumplimiento futuro de las normas aplicables sobre este estándar. ICANN ha incorporado el siguiente lenguaje contractual en la Especificación 6 de su Acuerdo de Registro de línea de base para garantizar este resultado.

El Operador de registro cumplirá con las RFC existentes pertinentes y las publicadas en el futuro por el Internet Engineering Task Force (IETF), incluidas todas las normas sucesivas, modificaciones o adiciones relacionadas con el aprovisionamiento y la gestión de nombres de dominio utilizando el Protocolo de aprovisionamiento extensible (EPP) en conformidad con los RFC 5910, 5730, 5731, 5732 (si utiliza objetos host), 5733 y 5734. Si el Operador de registro implementa el Período de gracia del Registro (RGP), cumplirá con el RFC 3915 y sus sucesivas modificaciones. Si el Operador de registro requiere el uso de una funcionalidad fuera de los RFC EPP base, el Operador de registro debe documentar las extensiones de EPP en formato de borrador de Internet siguiendo las pautas descritas en RFC 3735. El Operador de registro proporcionará y actualizará la documentación relevante de todos los objetos y extensiones de EPP admitidos a la ICANN antes del despliegue.

El gobierno de Colombia debe garantizar que se incluya una disposición similar en cualquier acuerdo contractual final con el oferente ganador. El gobierno de Colombia puede desear consultar como parte de la Solicitud de Propuestas (RFP) de qué manera los oferentes proponen garantizar el cumplimiento futuro y proporcionar la experiencia de las actualizaciones anteriores.

Documentos de referencia similares

Existen dos documentos externos relacionados con ICANN que respaldan este enfoque para garantizar condiciones técnicas mínimas sobre los requisitos de hardware y software en relacion a la RFP, y permiten que cada oferente proporcione su propia configuración para cumplir con los requisitos de SLA.

a. Solicitud de información del operador de registro back-end de emergencia (EBERO RFI) Los EBERO son una clasificación de infraestructura de registro backend especial que ICANN ha designado para intervenir en el caso de una falla del registro de gTLD. En la RFI emitida por ICANN para identificar y seleccionar a múltiples proveedores de EBERO, no hubo ninguna referencia específica a los requisitos de hardware o software que no sean los RFC aplicables, por ejemplo PPE. [2]

b. Acuerdo de subcontratación de material: cambio de proveedor de servicios de registro. ICANN ha proporcionado un documento para los operadores de registro de gTLD existentes que buscan cambiar a los proveedores de infraestructura de registro backend que actualmente no operan "uno o más

registros de nuevos gTLD". [3] Las preguntas que se resumen en este documento resumen aquellas formuladas a los solicitantes durante el la ronda de nuevos gTLDs de 2012 y proporciona un excelente punto de referencia para preguntas que el gobierno de Colombia debe incluir en cualquier RFP.

RECOMENDACIONES:

El gobierno de Colombia debe evitar incluir cualquier requisito de hardware o software en en la RFP y, en su lugar, permitir que los oferentes detallan sus configuraciones de hardware, software e instalaciones para cumplir con el SLA requerido por el gobierno de Colombia.

El gobierno de Colombia tal vez pueda incluir una lista de las especificaciones de hardware y software utilizadas actualmente. Si bien la mayoría de las RFP no incluyen estos detalles, el gobierno de la India hizo esto en relación con la licitación .IN más reciente. Sin embargo, el requerimiento de la divulgación crea un riesgo de seguridad potencial durante la tramitación de la oferta o después del hecho si se retiene al operador de registro actual. Si bien el gobierno de Colombia podría tratar de restringir el acceso a esta información a través de un NDA o un instrumento legal equivalente, tiene poco valor que esta información se divulgue públicamente. De hecho, en las rondas de nuevos gTLD (2000 y 2004) y en la RFP .ORG de la ICANN de 2002, ICANN solía requerir la divulgación de detalles técnicos. Sin embargo, estos detalles ahora están fuera del alcance público. Por lo tanto, se recomienda NO incluir las especificaciones técnicas actuales del operador de registro .CO existente.

El gobierno de Colombia debe garantizar que el lenguaje aplicable se incluya en cualquier acuerdo de registro final con el postor vigente para garantizar el cumplimiento futuro de las mejoras al EPP u otras normas relevantes.

---

[1] Ver https://newgtlds.icann.org/en/applicants/advisories/epp-extensions-21dec12-en

[2] Ver https://www.icann.org/en/system/files/files/ebero-rfi-14sep11-en.pdf

[3] Ver https://www.icann.org/en/system/files/files/msa-technical-questions-25sep17-en.pdf

5.3. Establecer las condiciones mínimas para llevar a cabo una migración técnica entre concesionarios que garantice la prestación del servicio y el establecimiento de un calendario provisional de este proceso.

ANALISIS:

Este análisis se basa en dos requisitos previos. Primero se selecciona un oferente que no sea el operador de registro titular, de lo contrario no es necesaria la transición. Segundo, que cualquier postor ganador ya habrá cumplido o superado los otros criterios técnicos mínimos. Este análisis adicional de las "condiciones mínimas" necesarias para llevar a cabo una migración técnica es necesario, en parte, debido al estricto cronograma de transición propuesto por el MINTIC.

Durante las consultas con el gobierno de Colombia, se informó a los consultores expertos externos que se emitiría una RFP a principios de junio y que, según la ley nacional de Colombia, la fecha más temprana de la selección proyectada sería el 24 de septiembre de 2019. Dado que el contrato actual para los servicios de registro expirará el 9 de febrero de 2020, eso solo otorga 4 meses y 17 días para una transición. Una consideración adicional que se incluye en este análisis fue el hecho de que el acuerdo de registro actual no parecía tener ninguna disposición legal para que el MINTIC o el gobierno de Columbia continúen / extiendan los servicios con el operador de registro actual en caso de cualquier tipo de interrupción durante el proceso de transición

A modo de ejemplo, debido al inesperado cierre parcial del Gobierno de los Estados Unidos a principios de 2019, la NTIA extendió el contrato actual del operador del registro .US durante varios meses para permitir una revisión / implementación adecuada de la licitación de .US. Se le recomendaría al gobierno de Colombia que incorpore una disposición similar en cualquier contrato futuro para servicios de registro, ver el Anexo A. Esto proporcionará flexibilidad al gobierno en cualquier proceso de licitación de RFP futuro para maximizar las oportunidades de ingresos / innovación y, al mismo tiempo, garantizar la seguridad y estabilidad del .CO ccTLD.

A. Demostración potencial de migraciones de tamaño similar

Durante la visita in situ de los expertos a Bogotá, se discutió el tema de exigir a los licitantes que demuestren una prueba de una transición de tamaño similar. Se reconoció que esta podría ser una función / requisito importante para el gobierno de Colombia para maximizar la probabilidad de una transición sin problemas. Hasta la fecha, solo los expertos identificaron dos transiciones de ccTLD de tamaño similar: .AU (3,1 millones -2018) y .IN (2 millones - 2019). Es posible que Nominet también califique si agrega el número total de nombres de dominio que se hicieron la transición de Minds and Machine (MMX) en 2016. Sin embargo, no pudimos determinar el número exacto de los nombres de dominio que fueron transiciones y el período en el tiempo durante el cual tuvo lugar esta transición.

La razón por la cual esta experiencia es potencialmente una consideración importante para que el gobierno de Colombia la implemente es debido al marco de tiempo mencionado anteriormente. Según la información disponible en relación con las transiciones .AU y .IN, estas transiciones tuvieron lugar entre seis y siete meses. Por lo tanto, si .CO hace la transición a un nuevo backend siempre que sea una de las transiciones de TLD más grandes que se produzcan en corto tiempo. También se reconoció que cualquier posible transición se produciría durante el período de vacaciones de fin de año complicando aún más las cosas, aunque es importante tener en cuenta que tanto el .AU como el .IN se produjeron durante el mismo período de tiempo.

También se discutió sobre cómo la implementación de este criterio por parte del gobierno de Colombia podría limitar el grupo de postores calificados. Específicamente, parecía haber consenso entre los expertos en que VeriSign, aunque nunca antes había realizado la transición de un millón de registros de nombres entrantes, estaría calificado según su experiencia operativa de mantener más de 150 millones de nombres de dominio .COM y .NET. Por lo tanto, es posible que el gobierno de Colombia desee considerar la posibilidad de ampliar los criterios para que un licitador calificado incluya dos millones más de transiciones de registro anteriores, y aquellos licitantes calificados en los que el número total de nombres de dominio en transición (2,3 millones) representa una fracción (por ejemplo, menos más del 10%) del número total de nombres de dominio que ya están bajo administración.

B. Chinese MIIT Certification

Basado en una presentación de .CO Internet S.A.S. proporcionada a los expertos, se identificó que .CO había obtenido la licencia del gobierno chino (MIIT) en 2018. Si bien el gobierno chino solicitó esta licencia de TLD genérico, los expertos no tenían conocimiento de ningún otro ccTLD que hubiera obtenido esta licencia por parte del gobierno chino. Además, no se sabía si esta licencia era requerida por el gobierno chino o si .CO Internet S.A.S solicitó voluntariamente dicha licencia. El gobierno de Colombia debe divulgar este hecho al posible oferente y solicitar su respuesta sobre la forma en que proponen abordar cualquier problema de licencia en esta transición. El gobierno de Colombia, ya sea individualmente o en consulta con la UIT, tal vez desee consultar al gobierno chino sobre este tema para garantizar que no haya una interrupción en el servicio de .CO en China como resultado de esta transición.

C. Redelegación de IANA

Uno de los temas tratados por los expertos durante su visita a Bogotá fue la posible redelegación del ccTLD .CO de .CO Internet S.A.S. a MINTIC antes de cualquier transición. Se observó de qué manera los registros de la IANA para los ccTLD .IN y .AU, incluían a National Internet Exchange of India y a .au Domain Administration (auDA) como el administrador de ccTLD para cada TLD respectivo. El .CO ccTLD actualmente lista a .CO Internet S.A.S. como el Administrador de ccTLD, con Contacto Administrativo y Contacto Técnico. Estos tipos de delegaciones, aunque no se realizan con frecuencia, son un procedimiento operativo normal para IANA / ICANN. De hecho, una redelegación similar tuvo lugar en 2009 en relación con .CO cuando .CO Internet S.A.S. fue designado, se puede consultar en https://www.iana.org/reports/2009/co-report-24nov2009.html

Los expertos recomendaron completar este proceso de redelegación durante la tramitación del proceso de RFP para minimizar cualquier problema potencial, en caso de que el titular no sea seleccionado.

D. Temas de migración RDAP[39]

Durante el reciente Taller de Operaciones de Registros de la ICANN (ROW) en Bangkok, Tailandia, hubo una discusión sobre la posible interrupción de los servicios RDAP asociados con la transición de un operador de registro de back-end. Esto sigue siendo un área técnica en evolución, ya que solo se ha producido una transición conocida hasta la fecha. Sin embargo, como RDAP se implementa más ampliamente en el ecosistema de nombres de dominio, particularmente después de que ICANN haya ordenado a las partes contratantes implementar RDAP para agosto de este año, este puede ser un problema en el futuro. El gobierno de Colombia debe confirmar con .CO Internet S.A.S. si planean desplegar RDAP dentro del .CO en un futuro muy cercano. Si lo hacen, sería muy recomendable incluir esto como una pregunta adicional en la RFP para que los oferentes la aborden.

E. Sub delegaciones y reglas unicas del negocio

El nombre de dominio de nivel superior .CO es un TLD híbrido, que se comercializa globalmente como un gTLD en el segundo nivel, mientras que también sirve a un mercado nacional distinto con servicios de registro de nombres de dominio en el tercer nivel en varios subdominios, por ejemplo. COM.CO, GOV.CO, ORG.CO, EDU.CO y MIL.CO. El operador de registro actual, .CO Internet SAS, actúa como registrador exclusivo para el subdominio GOV.CO, .ORG.CO, EDU.CO y MIL.CO, cada uno de los cuales requiere la implementación de diferentes requisitos / certificación de negocios. La RFP debe exigir a todos los oferentes que proporcionen su experiencia detallada en relación con estos tipos de acuerdos de nombre de subdominio, en particular cuando se trata de una entidad integrada verticalmente que aplica diferentes requisitos comerciales en los subdominios.

F. Red de registrars (o registradores)

Dado el estricto cronograma de migración identificado anteriormente, una red de registradores existente del oferente es una consideración adicional para que el

[39] https://www.icann.org/rdap

gobierno de Colombia la incorpore en su análisis. Actualmente hay aproximadamente setenta registradores listados en .CO Internet S.A.S. Sin embargo, parece que hay un número mayor en la hoja de Excel proporcionada por el personal del MINTIC a los expertos. Se debe proporcionar a los encuestados una lista completa de las entidades autorizadas con acceso al Sistema de Registro Compartido (SAS) .CO. Los oferentes deben poder reconocer qué porcentaje de esa lista ya ha superado las pruebas de OTE en su sistema y cuál sería su enfoque para incorporar las entidades restantes.

RECOMENDACION:

Se recomienda que el gobierno de Colombia solicite a todos los oferentes de las RFP que incluyan en su respuesta los siguientes datos: experiencia relevante en migraciones; experiencia en licencias MIIT; migración RDAP; experiencia en gestión de nombres de subdominios; y la red de registradores existente. En relación con el peso otorgado a la experiencia de migración anterior, esta es una determinación que debe realizar el gobierno de Colombia en base a su propia evaluación de riesgo interna.

5.4. Determinar los aspectos mínimos necesarios para llevar a cabo una valoración de la concesión.

ANALISIS

Ver en reporte económico incluido en el anexo.

5.5. Calcule el valor inicial y / o la compensación económica para el Estado que debe asumir un posible nuevo concesionario del dominio .CO.

ANÁLISIS

Ver en reporte económico incluido en el anexo.

5.6. Mitigación de riesgos

Riesgo	Efecto	Nivel	Mitigación
Deficiencia en la operación por parte del futuro administrador del ccTLD .CO	Problemas de calidad de servicio	Medio	Incluir un Acuerdo de nivel de servicio específico en el proceso de licitación y una referencia específica en los criterios de evaluación relacionados con este problema será clave.
La transición toma más tiempo de lo previsto	Termina el contrato con el actual concesionario y no hay proveedor de back-end	Medio	El ganador de la licitación debe definir una estrategia clara sobre cómo se puede llevar a cabo la transición. Se deben incluir medidas de seguridad específicas como parte de la licitación y en los criterios de evaluación para asegurarse de que la transición sea fluida (en caso de que el ganador sea diferente al administrador existente).
No se cumplen las expectativas de crecimiento del ccTLD . CO	La operación no es rentable para el concesionario	Medio	El mercado de dominios se comporta bastante predecible con una demanda que se ha mantenido bastante estable durante los últimos 10 años. Sin embargo, es importante que el ganador de la licitación dedique suficientes recursos a la comercialización y promoción del dominio .co.
Pérdida de imagen del ccTLD .co por ataques de seguridad	Afectación en el crecimiento del ccTLD de bajas de sitios con dominios .co	Medio	Incluir un Acuerdo de nivel de servicio específico en el proceso de licitación y una referencia específica en los criterios de evaluación relacionados con temas de estabilidad y seguridad
Pérdida de reputación de ccTLD .co debido a una mala mitigación del abusos	Impacto en el uso y aceptación del ccTLD en todo el mundo	Alto	Requerir que se coloquen medidas estrictas para monitorear y mitigar el abuso de los nombres de dominio, incluido el 100% del monitoreo de todos los nombres registrados
El titular actual (incumbente) no coopera con la	Inestablilidad en el ccTLD combinada con pérdida de	Alto	MINTIC debe obtener copias completas de la base de datos de registro, registros de facturación,

transición de ccTLD .co	ventas y baja en la reputación del Gobierno de Colombia		comunicaciones del registrador, problemas de servicio, del titular antes de cualquier transición o anuncios relacionados con la transición. También es necesario implementar una estrategia legal adecuada para contrarrestar los obstáculos legales que pueden ser implementados por el titular para frenar o evitar una transición ordenada.

Anexos

Indice de Anexos

ANEXOS

ANEXO sección 2.3

DATOS DE INVESTIGACION:

Administradores de ccTLD (código de país, registros de dominio de nivel superior): los más de 240 administradores nacionales de ccTLD administran suregistro de ccTLD correspondiente. Los administradores de ccTLD son muy diferentes en su naturaleza de un territorio a otro, e incluyen grupos informales, organizaciones sin fines de lucro, corporaciones con fines de lucro, asociaciones industriales, departamentos gubernamentales y, en algunos casos, incluso voluntarios. Solo los cambios propios del registro con respecto a la información del servidor de nombres que requieren cambios en el servidor raíz se informan a ICANN. Si bien todos los ccTLD tienen una entrada en el archivo de la zona raíz y se comunican con la IANA (que es anterior a ICANN), la mayoría aún debe unirse a la organización de apoyo de ICANN para los ccTLD (ccNSO) o firmar un contrato con ICANN. Las políticas de los ccTLD suelen ser definidas localmente por la comunidad local de Internet, no por ICANN ni por ningún otro organismo externo. En este contexto, se considera que la comunidad local de Internet incluye el gobierno local. Algunos países han estado regulando directamente el proceso de formulación de políticas, mientras que otros han dejado implícita o explícitamente la tarea al administrador de ccTLD a los foros nacionales de múltiples partes interesadas. A menudo, la autoridad de formulación de políticas está agrupadas en el llamado Órgano Asesor de Políticas, que, según el país, puede o no incluir a todas las partes interesadas.

Fuente: https://www.wgig.org/docs/WP-IPaddresses.pdf

LIR (registros locales de Internet): los LIR son miembros de sus respectivos registros regionales de Internet. Como consecuencia de su membresía, pueden obtener direcciones IP y números de ASN de su RIR regional y, posteriormente, asignar estos recursos a los usuarios finales de IP que pueden ser individuos u otras compañías que operan redes más pequeñas. Un LIR normalmente será un ISP (Proveedor de servicios de Internet), una organización de telecomunicaciones o una gran corporación.

(De hecho, en algunas regiones, la terminología utilizada es directamente es de ISP en lugar de LIR).

Fuente: https://www.wgig.org/docs/WP-IPaddresses.pdf

Proceso de desarrollo de políticas de RIR: Los RIR se estructuran de manera similar a las organizaciones sin fines de lucro, basadas en miembros. Facilitan el desarrollo de políticas basadas en el consenso bottom-up y autorregulada de la industria en respuesta a los requisitos de las muchas y diversas partes interesadas en sus respectivas comunidades. El desarrollo de esta política está abierto a todos, e incluye la participación activa de organismos del sector público y privado, así como de la sociedad civil. La estructura RIR permite que los RIR brinden servicio de manera justa, receptiva, neutral e imparcial. Los RIR tienen una política de membresía abierta. Cada RIR organiza reuniones de políticas públicas que están abiertas a cualquier persona, independientemente del estado de la membresía. Esto significa que cualquier persona puede participar en la discusión de problemas relacionados con la propiedad intelectual y en el desarrollo de políticas de administración de recursos numéricos. Estas reuniones, junto con las listas de correo abiertas al público, permiten a los RIR obtener una perspectiva amplia sobre los problemas que afectan a la comunidad. Los RIRs realizan esfuerzos concertados para ayudar a sus comunidades a construir políticas basadas en el consenso. Los RIR aseguran que estas políticas se apliquen de manera justa y coherente, incluidas aquellas que están en común con otras regiones. Los RIRs no desarrollan políticas; las políticas son desarrolladas por la comunidad e implementadas / ejecutadas por los RIR.

Fuente: https://www.wgig.org/docs/WP-IPaddresses.pdf

C.1.7 As the Internet and the DNS have evolved, so has the Internet policy making environment. Along those lines, the Contractor shall develop and maintain a constructive relationship with the usTLD stakeholder community, including but not limited to, locality space domain name holders, delegated managers, and domain name registrants, and implement processes to ensure input into, and feedback on, the quality performance of the requirements of the usTLD contract. Therefore, DOC seeks proposals that include a multistakeholder process to facilitate consultation with stakeholders to propose, comment, and provide input into management of the

usTLD. Any proposed mechanism for ongoing community consultation on matters related to management of the usTLD, including policy development, should reflect the tenets of the multistakeholder approach. The goals of the multistakeholder approach or process should, at a minimum, include ensuring that the needs of current usTLD domain name holders are considered, ensure stakeholders feel policies will enhance the user experience and utility of the usTLD space, and provide a platform for ongoing discussion of evolving and emerging DNS issues. The Contractor shall encourage the participation of delegated managers, locality registrants, second-level registrants, and all other interested usTLD stakeholders in any such process.

Source: US RFP

C.5 CORE POLICY REQUIREMENTS

C.5.1 The Contractor shall:

(i) Implement United States Nexus Requirement. The Contractor shall operate the usTLD as a country code top level domain intended to serve the Internet community of the United States, including businesses, consumers, individuals, not-for-profit organizations, and state and local governments with a residence or bona fide presence in the United States. In addition to the current policy set forth in RFC 1480 requiring that usTLD domain name registrations be hosted on computers located within the United States, the Contractor must implement a United States nexus policy for the locality-based usTLD structure and the second-level usTLD space.

(ii) Implement Registrar and Registrant Agreements. The Contractor shall establish contractual arrangements with all accredited usTLD registrars incorporating the requirements relating to usTLD policies such as nexus, WHOIS, and dispute resolution, and ensuring prompt, reliable, and effective technical and customer service. Such registrar agreements shall include a provision that will require registrars to offer DNSSEC services for new and renewed usTLD registrations. The Contractor shall require that each accredited usTLD registrar implement a registrant agreement that requires each registrant to agree to all applicable usTLD policies.

(iii) Implement a Uniform Domain Name Dispute Resolution Procedure and Sunrise Policy. The Contractor shall implement a uniform domain name dispute resolution

procedure intended to resolve "cybersquatting" disputes in the usTLD. The Contractor may base such policy on other existing Uniform Domain Name Dispute Resolution Procedures and modify it as necessary to make such policy applicable to the usTLD specifically. The Contractor shall also implement a "sunrise period" for qualified trademark owners to pre-register their trademarks as domain names in the second-level usTLD space prior to the wider registration for non-trademark owners in the event future developments necessitate such action.

(iv) Abide by Existing Policy Frameworks and Best Practices for the Administration of ccTLDs. The Contractor shall abide by existing policy frameworks in the principles and procedures for the delegation and administration of ccTLDs, such as RFC 1591 Domain Name System Structure and Delegation, the Governmental Advisory Committee (GAC) Principles and Guidelines for the Delegation and Administration of Country-Code Top Level Domains, any ccTLD related policies, and any further official clarification of these policies unless inconsistent with U.S. law or regulation or otherwise directed by the DOC.

(v) Multistakeholder Consultation Process. The Contractor shall develop and implement a process using the multistakeholder approach to facilitate consultation with stakeholders to propose, comment, and provide input into the management of the usTLD, including policy development (see C.1.7).

(vi) Implement and enforce policies concerning:

(a) Data Rights and Use. The Contractor shall prohibit the use of registrant and other data obtained from registrars and delegated managers for purposes other than providing usTLD administration services;

(b) Publicly Accessible, Accurate, and Up-to-Date WHOIS Database. The Contractor shall implement a policy that addresses continued public access to accurate WHOIS information, including a prohibition of proxy and anonymous services offered by registrars, registrar affiliates and partners, and delegated managers. The Contractor shall regularly monitor the current practices of registrars and delegated managers to ensure compliance with this requirement; (c) Reserved Domain Names. The Contractor shall implement a policy to manage a list of permanently reserved names not available for registration, and if appropriate, the release of certain names that are currently reserved (see C.1.5 above);

(1) The Contractor shall post a list of all reserved names on a publicly accessible website.

(d) Domain Name Transfers. The Contractor shall implement a mechanism that facilitates the transfer of a domain name registration from one usTLD registrar to another usTLD registrar at the request of the domain name registrant.

(e) Redemption Grace Period. The Contractor shall implement a policy that allows registrants to restore domain name registrations within a reasonable time period after their expiration.

(f) Domain Name Review. The Contractor shall implement a policy that allows the Contractor the right to reasonably refuse registration of any domain name in the usTLD.

(g) Registration Abuse. The Contractor shall implement a policy that prevents and combats abuses of the usTLD registration system including practices that harm, mislead, or confuse consumers and that misuse intellectual property in the usTLD. This policy may include methods to curb the misuse of automated registration technologies and the add/drop grace period; and

(h) Other Policies. The Contractor may propose such other policies, amendments to current policies in this section (C.5.1), or additional procedures or mechanisms as are necessary to fulfill the Contract's requirements and increase the use of, or otherwise facilitate continued improvement of the usTLD.

(vii) Adhere to a Code of Conduct. The Contractor shall adopt a code of conduct requiring it to administer the usTLD impartially and without discriminating among or between eligible registrants, operate the usTLD in the public interest, and protect proprietary information of usTLD registrars.

---

[1] See https://www.nro.net/about/nro-faq/
[2] See https://www.icann.org/resources/pages/governance/bylaws-en/#article9
[3] See http://ipv6.br/
[4] See https://www.icann.org/resources/pages/help/dndr/udrp-en
[5] See https://www.wipo.int/amc/en/domains/cctld/

ANEXO Sección 3.1

Annex A – External Research Data Points

2018 .US RFP

C.12 SECURITY REQUIREMENTS

C.12.1 Secure Systems. The Contractor shall install and operate computing and communications systems in accordance with best business and security practices. The Contractor shall implement authenticated communications between it and its customers when performing all requirement of this Contract and shall document such practices and the configuration of all systems.

C.12.2 Secure Systems Notification. The Contractor shall implement and thereafter operate and maintain a secure notification system that is, at a minimum, capable of notifying all relevant stakeholders of such events as outages, planned maintenance, and new developments. In all cases, the Contractor shall notify the COR of any outages.

C.12.3 Secure Data. The Contractor shall ensure the authentication, integrity, and reliability of the data in performing all requirements of this contract.

C.12.4 Computer Security Plan. The Contractor shall develop and implement a computer security plan. The Contractor shall also update such plan annually and deliver such plan to the COR.

C.12.5 Director of Security. The Contractor shall designate a Director of Security, who shall be

responsible for ensuring technical and physical security measures, such as personnel access controls. The Contractor shall provide the name of the designee prior to contract award and this person shall be designated as Key Personnel in the proposal. The Contractor shall notify and consult with the COR before changing personnel in this position in accordance with the Key Personnel Clause of this contract.

9.6 System Security, Physical Security and Reliability

9.6.1 24x7x365 monitoring of the registry system and network by a Network Operations Centre (‘NOC’)

9.6.2 Compliance with applicable standards published by bodies such as IETF or ICANN, IIB and SSAC which are designed to ensure interoperability and improve the user experience

9.6.3 Protection against malicious software, DDoS attacks, system hacks, break-ins, data tampering, and other disruptions of services

9.6.4 Implement Security incident and event management system (SIEM)

9.6.5 Implement Network Security

9.6.6 Implement Information Security Policy

9.6.7 Implement Physical Security

9.6.8 Staff-in place with technical skills, expertise and experience to operate the registry in order

to maintain and enhance the current levels of performance

9.6.9 Detailed review processes for the integration of new requirements as well as subsequent compliance monitoring and periodic review

9.6.10 DNS information maintained by registrars shall comply with IT Act 2008 (Amendment). All the data belonging to registrants apart from DNS information like email ID, Aadhar details etc shall not be stored outside India.

9.6.11 TSP should implement a mechanism to mitigate “drop and catch” of domain names. Repeated requests to register a specific domain name should be throttled. TSP should implement a rate limiting mechanism such as limiting <X> (20) requests for a specific domain name registration from a specific registrar. After the occurrence

of this event there should be a sleep time of at least 1 hour after which registration of the same domain name should be allowed.

9.6.12 TSP shall provision for restricting Registrar for illegitimate blocking of domain name

9.6.13 There shall be mechanism to identify and report fraudulent domain registrations and associated incidents

.AU RFP – Annexure B

The supplier must have an arrangement in place (acceptable to auDA) with the Australian Government, Attorney-General's Department's Computer Emergency Response Team (CERT Australia) and the Agreement will include ongoing obligations on the part of the supplier to engage with CERT Australia in relation to cyber security and data protection issues.

The supplier must take all steps to protect the Registry Data, the EPP interface, the Registrar's registry portal, the WHOIS directory server and the domain name system server infrastructure against misuse, interference and loss, and from unauthorised access, modification or disclosure.

The supplier will be obliged to act in accordance with the "Strategies to Mitigate Cyber Security Incidents" (known as 'Essential Eight') published by the Australian Signals Directorate.

The Agreement will permit and set out the process by which auDA may conduct an independent audit of the supplier's compliance with the security requirements set out in the Agreement, including cooperation and assistance obligations on the part of the supplier.

In addition to any ad hoc compliance reviews, auDA and the supplier must meet at least once every 3 months to review performance of the security requirements.

ICANN – MSA Technical Questions

7. (A) SECURITY POLICY:

Provide a summary of the security policy for the proposed registry, including but not limited to:

Indication of any independent assessment reports demonstrating security capabilities, and provisions for periodic independent assessment reports to test security capabilities;

Description of any augmented security levels or capabilities commensurate with the nature of the applied for gTLD string, including the identification of any existing international or industry relevant security standards the Registry Operator commits to following (reference site must be provided);

List of commitments made to registrants concerning security levels.

Answers must also include:

Evidence of an independent assessment report demonstrating effective security controls (e.g., ISO 27001).

A summary of the above should be no more than 20 pages. Note that the complete security policy for the registry is required to be submitted in accordance with 8(b).

(b) Security Policy: Provide the complete security policy and procedures for the proposed registry, including but not limited to:

System (data, server, application/services) and network access control, ensuring systems are maintained in a secure fashion, including details of how they are monitored, logged and backed up

Resources to secure integrity of updates between registry systems and nameservers, and between nameservers, if any;

Independent assessment reports demonstrating security capabilities (submitted as attachments), if any;

Provisioning and other measures that mitigate risks posed by denial of service attacks;

Computer and network incident response policies, plans, and processes;

Plans to minimize the risk of unauthorized access to its systems or tampering with registry data;

Intrusion detection mechanisms, a threat analysis for the proposed registry, the defenses that will be deployed against those threats, and provision for periodic threat analysis updates;

Details for auditing capability on all network access;

Physical security approach;

Identification of department or group responsible for the registry's security organization;

Background checks conducted on security personnel;

Description of the main security threats to the registry operation that have been identified; and

Resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

ICANN's Template RRA Data Processing Addendum

6. SECURITY

a) The Disclosing Party shall be responsible for the security of transmission of any Shared Personal Data in transmission to the Receiving Party by employing appropriate safeguards and technical information security controls.

b) All Parties agree to implement appropriate technical and organizational measures to protect the Shared Personal Data in their possession against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, including but not limited to:

i. Ensuring IT equipment, including portable equipment is kept in lockable areas when unattended;

ii. Not leaving portable equipment containing the Shared Personal Data unattended;

iii. Ensuring use of appropriate secure passwords for logging into systems or databases containing Shared Personal Data;

iv. Ensuring that all IT equipment is protected by antivirus software, firewalls, passwords and suitable encryption devices;

v. Using industry standard 256-bit AES encryption or suitable equivalent where necessary or appropriate;

vi. Limiting access to relevant databases and systems to those of its officers, staff, agents, vendors and sub-contractors who need to have access to the Shared Personal Data, and ensuring that password security mechanisms are in place to prevent inappropriate access when individuals are no longer engaged by the Party;

vii. Conducting regular threat assessment or penetration testing on systems as deemed necessary, considering the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, with due regard to the nature of the data held, the cost of implementation, and the state of the art;

viii. Ensuring all authorized individuals handling Shared Personal Data have been made aware of their responsibilities with regards to handling of Shared Personal Data; and

ix. Allowing for inspections and assessments to be undertaken by the Controller as to the security measures taken, or producing evidence of those measures, if requested.

7. SECURITY BREACH NOTIFICATION

a) Notification Timing. Should a Party become aware of any Data Security Breach by a subprocessor in relation to Shared Personal Data, and where such a Breach is of a material impact to this Data Processing Addendum, or is likely to have a material impact on the Parties, the relevant Party should immediately notify the Parties, and the relevant Party shall provide immediate feedback about any impact this incident may/will have on the affected Parties, including the anticipated impacts to the rights and freedoms of Data Subjects if applicable. Such notification will be provided as promptly as possible, but in any event no later than 24 hours after detection of the Data Security Breach. Nothing in this section should be construed as limiting or changing any notification obligation of a Party under Applicable Laws.

b) Notification Format and Content. Notification of a Data Security Breach will be in writing to the information/administrative contact identified by the Parties, though communication may take place first via telephone. The notifying Party must be provided the following information, to the greatest extent possible, with further updates as additional information comes to light:

i. A description of the nature of the incident and likely consequences of the incident;

ii. Expected resolution time (if known);

iii. A description of the measures taken or proposed to address the incident including, measures to mitigate its possible adverse effects the Parties and/or Shared Personal Data;

iv. The categories and approximate volume of Shared Personal Data and individuals potentially affected by the incident, and the likely consequences of the incident on that

Shared Personal Data and associated individuals; and

v. The name and phone number of a representative the Party may contact to obtain incident updates.

c) Security Resources. The Parties' may, upon mutual agreement, provide resources from its security group to assist with an identified Data Security Breach for the purpose of meeting its obligations in relation to the notification of a Data Security Breach under Applicable Laws or other notification obligations or requirements.

d) Failed Security Incidents. A failed security incident will not be subject to the terms of this Data Processing Addendum. A failed security incident is one that results in no unauthorized access or acquisition to Shared Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

e) Additional Notification Requirements. For the purpose of this section, a Party is also required to provide notification in accordance with this section in response to:

i. A complaint or objection to Processing or request with respect to the exercise of a Data

Subject's rights under Applicable Laws; and ii. An investigation into or seizure of Shared Personal Data by government officials, regulatory or law enforcement agency, or indications that such investigation or seizure is contemplated.

Source: https://www.icann.org/en/system/files/files/rra-amendment-terms-temp-spec-02jul18-en.pdf
[1] See https://www.icann.org/en/system/files/files/msa-technical-questions-25sep17-en.pdf

ANEXO 3.2 - DATOS DE INVESTIGACION ADICIONAL

.CO WHOIS ACTUAL

Nombre del Dominio	go.co
ID del dominio del registro	D740798-CO
Fecha actualizada	2015-08-18T14:08:36Z
Fecha de creación	2010-04-26T07:53:29Z
Fecha de caducidad del registro	2020-04-25T23:59:59Z
Registrador	.CO Marketing Names
Registrador IANA ID	30730759
URL del Registrador	www.go.co
Registrar WHOIS servidor	
Correo electrónico de contacto de abuso de Registrador	
Teléfono de contacto de abuso de Registrador	
Estado del dominio	serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Estado del dominio	serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Estado del dominio	serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
ID del Registrador del Registro	
Nombre del Registrante	
Organización de Registrantes	.CO Internet S.A.S.
Calle Registrante	
Calle Registrante	
Calle Registrante	
Ciudad Registrante	
Registrante Estado / Provincia	
Código Postal del Registrante	
País Registrante	CO
Teléfono del Registrante	
Registrante Teléfono Ext	

Fax Registrante	
Registrant Fax Ext	
Correo electrónico del registrante	Para información de contactos, consulte el servicio RDDS del Registrador para obtener datos del Solicitante, Administrador o Técnico del nombre de dominio consultado.
ID del administrador del registro	
Nombre del administrador	
Organización de administración	
Admin Street	
Admin Street	
Admin Street	
Admin City	
Administración Estado / Provincia	
Admin Código Postal	
País del administrador	
Teléfono del administrador	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Correo electrónico del administrador	Para información de contactos, consulte el servicio RDDS del Registrador para obtener datos del Solicitante, Administrador o Técnico del nombre de dominio consultado.
ID de Tech de Registro	
Nombre de la tecnología	
Organización Tecnológica	
Tech Street	
Tech Street	
Tech Street	
Tech City	
Tech Estado / Provincia	
Tech Código Postal	
Tech Country	

Teléfono de tecnología	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Correo electrónico técnico	Para información de contactos, consulte el servicio RDDS del Registrador para obtener datos del Solicitante, Administrador o Técnico del nombre de dominio consultado.
Nombre del servidor	pdns196.ultradns.co.uk
Nombre del servidor	pdns196.ultradns.biz
Nombre del servidor	pdns196.ultradns.org
Nombre del servidor	pdns196.ultradns.com
Nombre del servidor	pdns196.ultradns.info
Nombre del servidor	pdns196.ultradns.net
DNSSEC	unsigned
>> Last update of WHOIS database:2019-05-14T23:42:49Z <<<	

CENTR Research on the collection and publication of Whois Registrant Data Elements

Analysis of European ccTLD and select other TLD in connection with the processing of registrant data involving a distinction between nature and legal persons:

Country	ccTLD	Natural/Legal Whois Distinction	Notes
Ascension Island	AC	No	Both National and Legal person Whois data output contain a thin data set (no contact information) for both Natural and Legal person Registrants
Austria	AT	Yes	It appears that differentiated Whois public output is dependent upon the appearance of a data element in the Organization field. No data element assumes that the Registrant is a Natural Person. However, the Registry Operator provides information on how a Natural Person could opt-in to the publication of their data by contacting their Registrar/ISP.
Belgium	BE	Yes	The ccTLD Manager provides differentiated access for Natural Person Registrants.

Bulgaria	BG	Yes	The ccTLD Manager does not publishing contact data for Admin and Tech for any type of Registrant. For both Natural and Legal Persons, the Name of the Registrant is published, however, only contact data for Legal Persons is automatically published.
Crotia	HR	Yes	The ccTLD Manager publishes absolutely NO contact information for Natural Persons, in connection with Legal Persons, only the Registrant name, address and email is published.
Cyprus	CY	No	The only Whois information publicly disclosed is the nameserver information for both Natural/Legal persons
Czechia/Czech Republic	CZ	Yes	An initial Whois query for a domain name will produce the name and NIC-Handle of the Holder and the Admin Contacts for both Natural and Legal Persons. However, when you click on the corresponding NIC Handles an address (both no other contact information) is provided for the Legal Person. No contact information other than the Name is provided for a Natural Person.
Denmark	DK	No	There does not appear to be any Whois output display differences based upon the nature of the Registrant, e.g. Natural/Legal Person. However, the ccTLD Manager appears to use NemID which is a digital identity that would distinguish between Registrant types.
European Union	EU	Yes	The public Whois output distinguishes between Natural and Legal persons, although an email address is published for all Registrant types.
Estonia	EE	Yes	For Natural Persons no Registrant, Admin or Tech contact details are published. For Legal Persons all Contacts (Registrant/Admin/Tech) are published even if those contact details are associated with an employee
Finland	FI	Yes	There is a distinction in the Whois public output based upon the Registrant type. For Legal Person registrants, full contact details are provided for the Holder (name, address, & phone), whereas for the Tech contact only name and email is provided. For Natural Persons only the name of the Holder is provided. No Tech Contact is provided.
France	FR	Yes	Full contact details (name, address, email & phone) are provided for Admin and Tech Contacts. However, there is no information provided in connection with Natural Person Registrants (Holders), whereas full contact details for Legal Person Registrants (name, address, email & phone) are provided.
Germany	DE	No	The only Whois information publicly disclosed is the nameserver information for both Natural/Legal persons
Greece	GR	No	There appears to be no distinction in the Whois outputs between Registrant types, e.g. Natural/Legal
Hungary	HU	Yes	Full contact details (name, address, phone & fax) are provided in connection with Registrants for Legal Persons, an email for a Tech Contact is also provided. For Nature

			Person Registrants NO contact information is provided other than an email for the Technical contact.
Iceland	IS	Yes	Full contact details (name, address, email & phone) are provided for Legal Person Registrants, whereas this information is masked I connection with Natural Persons
Ireland	IE	Yes	The Domain Holder field is masked in connection with Whois information associated with a Natural Person
Italy	IT	Yes	The Whois output for Legal Persons contains the full contact details (employee name, org, address, phone, fax, email) . However, the Registrant, Admin and Tech Contacts for Natural Person Registrants are all masked
Latvia	LV	Yes	The Whois output delineated the domain name Holder as either a Natural or Legal person. For a Legal Person full contact details are provided (name, address, phone and email). For a Natural Person no information is provided. The only other contact listed in the Whois out is the Tech Contact, however, that information is masked if it is associated with a Natural Person.
Liechtenstein	LI	No	There appears to be no distinction in the Whois outputs between Registrant types, e.g. Natural/Legal
Lituania	LT	Yes	For a Legal Person, the full Registrant contact details are provided (name, address, phone + email). There is no contact information provided for a Natural Person Registrant, instead full contact details of the Tech Contact are provided (name, address, phone + email)
Luxembourg	LU	Yes	The Admin and Tech Contact details are masked. However, the name and address of Legal Person Domain Name Holders are published, where as the details of Natural Person Domain Name Holders are masked.
Malta	MT	No	There appears to be no distinction in the Whois outputs between Registrant types, e.g. Natural/Legal. Full contact details (name, address, phone, & email) are provided for Holder, Admin, Tech & Billing contacts. However, ccTLD Manager does provide the ability for a Registrant to "appoint an Administrative Agent whose details would appear on your behalf."
Netherlands	NL	Yes	An email address for the Admin Contact is provided for both Natural and Legal Persons, however, the identity of the Registrant is only shown for the Legal person.
Norway	NO	Yes	Registry Operator is unique in that it provides three classes of Registrants: private individuals; legal person and sole proprietorship. Because an email contact appears to be provided for all classes of Registrants, the Registry Operator provides explicit notification of this fact and actively encouarges the usage of role accounts and/or third-party anymonous services.
Poland	PL	Yes	Registry Operator Whois FAQ states that "data registrants, who are natural persons, are not published"

Portugal	PT	Yes	Natural Person Registrants have their information withheld from publication in the public Whois unless they provide their explicit consent.
Romania	RO	Yes	The Whois ouput includes a designated Person Type: Private Person/Company
Slovakia	SK	Unclear	Have written to ccTLD manager to seek further clarification. The legal documentation suggests that there is a natural/legal distinction (and even a potential third class natural entrepenuer) as well as a consent feature. However, this did not appear to be reflected operationally. It is possible that these inconsistencies are associated with the CentralNic migration/acquisition.
Slovenia	SI	Yes	While the Registry Operator makes a distinction in connection with Natural/Legal Persons in connection with Whois ouput data, the email address and country of the Registrant appears in ALL queries.
Spain	ES	Yes	Whois data elements associated with Natural Person Registrant, e.g. Registrant, Admin & Tech Contact all restricted. However, it appears that PII associated with employees of Legal Person Registrants is published.
Sweden	SE	Yes	.SE has a two part Whois lookup. The first part will show the NIC Handle equivalent for a Legal Person Registrant, but not other contact types. One then needs to click on the NIC-Handle equivalent to obtain additional information about that contact. There is no NIC Handle equivalent for Natural Person Registrant.
Switzerland	CH	No	There appears to be no distinction in the Whois outputs between Registrant types, e.g. Natural/Legal
United Kingdom	UK	No	There appears to be no distinction in the Whois outputs between Registrant types, e.g. Natural/Legal
Generic TLD (Spain)	CAT	Yes	There is no Whois data shown in connection with Natural Person Registrant. Although Registry has a policy to publish Natural Person Registrants engaged in commercial activity with a .CAT domain name, no specific example could be found to document.
Generic TLD (USA)	NYC	Yes	There is a NYC Nexus Category RDDS field where ORG is used in conjunction with Legal Persons and INDIV is used in conjunction with Natural Persons

[1] See https://edpb.europa.eu/about-edpb/about-edpb_en
[2] .CO INTERNET S.A.S – December 2018 Update – Page 7
[3] See https://www.icann.org/dataprotectionprivacy

ANEXO Sección 3.5 – SLA

Anexo A B C D

ANNEX A – ICANN Specification 10

REGISTRY PERFORMANCE SPECIFICATIONS

1. **Definitions**

1.1. **DNS**. Refers to the Domain Name System as specified in RFCs 1034, 1035, and related RFCs.

1.2. **DNSSEC proper resolution**. There is a valid DNSSEC chain of trust from the root trust anchor to a particular domain name, e.g., a TLD, a domain name registered under a TLD, etc.

1.3. **EPP**. Refers to the Extensible Provisioning Protocol as specified in RFC 5730 and related RFCs.

1.4. **IP address**. Refers to IPv4 or IPv6 addresses without making any distinction between the two. When there is need to make a distinction, IPv4 or IPv6 is used.

1.5. **Probes**. Network hosts used to perform (DNS, EPP, etc.) tests (see below) that are located at various global locations.

1.6. **RDDS**. Registration Data Directory Services refers to the collective of WHOIS and Web-based WHOIS services as defined in Specification 4 of this Agreement.

1.7. **RTT**. Round-Trip Time or RTT refers to the time measured from the sending of the first bit of the first packet of the sequence of packets needed to make a request until the reception of the last bit of the last packet of the sequence needed to receive the response. If the client does not receive the whole sequence of packets needed to consider the response as received, the request will be considered unanswered.

1.8. **SLR**. Service Level Requirement is the level of service expected for a certain parameter being measured in a Service Level Agreement (SLA).

2. Service Level Agreement Matrix

	Parameter	SLR (monthly basis)
DNS	DNS service availability	0 min downtime = 100% availability
	DNS name server availability	£ 432 min of downtime (» 99%)
	TCP DNS resolution RTT	£ 1500 ms, for at least 95% of the queries
	UDP DNS resolution RTT	£ 500 ms, for at least 95% of the queries
	DNS update time	£ 60 min, for at least 95% of the probes
RDDS	RDDS availability	£ 864 min of downtime (» 98%)
	RDDS query RTT	£ 2000 ms, for at least 95% of the queries
	RDDS update time	£ 60 min, for at least 95% of the probes
EPP	EPP service availability	£ 864 min of downtime (» 98%)
	EPP session-command RTT	£ 4000 ms, for at least 90% of the commands
	EPP query-command RTT	£ 2000 ms, for at least 90% of the commands
	EPP transform-command RTT	£ 4000 ms, for at least 90% of the commands

Registry Operator is encouraged to do maintenance for the different services at the times and dates of statistically lower traffic for each service. However, note that there is no provision for planned outages or similar periods of unavailable or slow service; any downtime, be it for maintenance or due to system failures, will be noted simply as downtime and counted for SLA purposes.

3. DNS

3.1. **DNS service availability**. Refers to the ability of the group of listed-as-authoritative name servers of a particular domain name (e.g., a TLD), to answer DNS queries from DNS probes. For the service to be considered available at a particular moment, at least, two of the delegated name servers registered in the DNS must have successful results from "**DNS tests**" to each of their public-DNS registered "**IP addresses**" to which the name server resolves. If 51% or more of the DNS testing probes see the service as unavailable during a given time, the DNS service will be considered unavailable.

3.2. **DNS name server availability**. Refers to the ability of a public-DNS registered "**IP address**" of a particular name server listed as authoritative for a

domain name, to answer DNS queries from an Internet user. All the public DNS-registered "**IP address**" of all name servers of the domain name being monitored shall be tested individually. If 51% or more of the DNS testing probes get undefined/unanswered results from "**DNS tests**" to a name server "**IP address**" during a given time, the name server "**IP address**" will be considered unavailable.

3.3. **UDP DNS resolution RTT**. Refers to the **RTT** of the sequence of two packets, the UDP DNS query and the corresponding UDP DNS response. If the **RTT** is 5 times greater than the time specified in the relevant **SLR**, the **RTT** will be considered undefined.

3.4. **TCP DNS resolution RTT**. Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the DNS response for only one DNS query. If the **RTT** is 5 times greater than the time specified in the relevant **SLR**, the **RTT** will be considered undefined.

3.5. **DNS resolution RTT**. Refers to either "**UDP DNS resolution RTT**" or "**TCP DNS resolution RTT**".

3.6. **DNS update time**. Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, until the name servers of the parent domain name answer "**DNS queries**" with data consistent with the change made. This only applies for changes to DNS information.

3.7. **DNS test**. Means one non-recursive DNS query sent to a particular "**IP address**" (via UDP or TCP). If DNSSEC is offered in the queried DNS zone, for a query to be considered answered, the signatures must be positively verified against a corresponding DS record published in the parent zone or, if the parent is not signed, against a statically configured Trust Anchor. The answer to the query must contain the corresponding information from the Registry System, otherwise the query will be considered unanswered. A query with a "**DNS resolution RTT**" 5 times higher than the corresponding SLR, will be considered unanswered. The possible results to a DNS test are: a number in milliseconds corresponding to the "**DNS resolution RTT**" or, undefined/unanswered.

3.8. **Measuring DNS parameters**. Every minute, every DNS probe will make an UDP or TCP "**DNS test**" to each of the public-DNS registered "**IP addresses**" of the

name servers of the domain name being monitored. If a "**DNS test**" result is undefined/unanswered, the tested IP will be considered unavailable from that probe until it is time to make a new test.

7. Emergency Escalation

Escalation is strictly for purposes of notifying and investigating possible or potential issues in relation to monitored services. The initiation of any escalation and the subsequent cooperative investigations do not in themselves imply that a monitored service has failed its performance requirements.

Escalations shall be carried out between ICANN and Registry Operators, Registrars and Registry Operator, and Registrars and ICANN. Registry Operators and ICANN must provide said emergency operations departments. Current contacts must be maintained between ICANN and Registry Operators and published to Registrars, where relevant to their role in escalations, prior to any processing of an Emergency Escalation by all related parties, and kept current at all times.

7.1. Emergency Escalation initiated by ICANN

Upon reaching 10% of the Emergency thresholds as described in Section 6 of this Specification, ICANN's emergency operations will initiate an Emergency Escalation with the relevant Registry Operator. An Emergency Escalation consists of the following minimum elements: electronic (i.e., email or SMS) and/or voice contact notification to the Registry Operator's emergency operations department with detailed information concerning the issue being escalated, including evidence of monitoring failures, cooperative trouble-shooting of the monitoring failure between ICANN staff and the Registry Operator, and the commitment to begin the process of rectifying issues with either the monitoring service or the service being monitoring.

7.2. Emergency Escalation initiated by Registrars

Registry Operator will maintain an emergency operations department prepared to handle emergency requests from registrars. In the event that a registrar is unable to conduct EPP transactions with the registry for the TLD because of a fault with the Registry Service and is unable to either contact (through ICANN mandated methods of communication) the Registry Operator, or the Registry Operator is unable or

unwilling to address the fault, the registrar may initiate an emergency escalation to the emergency operations department of ICANN. ICANN then may initiate an emergency escalation with the Registry Operator as explained above.

7.3. **Notifications of Outages and Maintenance**

In the event that a Registry Operator plans maintenance, it will provide notice to the ICANN emergency operations department, at least, twenty-four (24) hours ahead of that maintenance. ICANN's emergency operations department will note planned maintenance times, and suspend Emergency Escalation services for the monitored services during the expected maintenance outage period.

If Registry Operator declares an outage, as per its contractual obligations with ICANN, on services under a service level agreement and performance requirements, it will notify the ICANN emergency operations department. During that declared outage, ICANN's emergency operations department will note and suspend emergency escalation services for the monitored services involved.

8. **Covenants of Performance Measurement**

8.1. **No interference**. Registry Operator shall not interfere with measurement **Probes**, including any form of preferential treatment of the requests for the monitored services. Registry Operator shall respond to the measurement tests described in this Specification as it would to any other request from an Internet user (for DNS and RDDS) or registrar (for EPP).

8.2. **ICANN testing registrar**. Registry Operator agrees that ICANN will have a testing registrar used for purposes of measuring the **SLR**s described above. Registry Operator agrees to not provide any differentiated treatment for the testing registrar other than no billing of the transactions. ICANN shall not use the registrar for registering domain names (or other registry objects) for itself or others, except for the purposes of verifying contractual compliance with the conditions described in this Agreement. Registry Operator shall identify these transactions using Registrar ID 9997.

Appendix A: Service Level Agreements

Describe how your organization will meet the minimum service level agreements outlined below. Include in your description all measurable aspects of these service levels. If necessary, provide alternative measures which meet or exceed the service levels noted below.

#	Area	Requirement	Measure
1	Account Management	Review of service level performance and contractual requirements	Weekly, monthly, and quarterly
2	Account Management	Review of ICANN compliance measures	Weekly and monthly
3	Account Management	Survey of registrar satisfaction	Annually, or as agreed upon between parties, at a minimum.
4	Account Management	Comprehensive documentation for enterprise-wide processes and systems	Reviewed and updated monthly
5	Compliance	Provide audited Financial Statements for most recent fiscal year.	Annually, within 90 days of close of calendar year.
6	Compliance	Provide SSAE16 Type 2 or ISAE 3402 Type 2 annual report that covers registry operations.	Annually, within 90 days of close of calendar year.
7	Compliance	Processing court orders	Within 48 hours unless otherwise mandated, with confirmation to Public Interest Registry immediately following completion of action.
8	Compliance	An established intrusion detection system (IDS) must be used to provide continuous monitoring over the organisation's network or systems for malicious activity or policy violations. Any detected activity or violation must be collected centrally using a security information and event management (SIEM) system and notifications of security	24X7 continuous monitoring and intrusion detection Notifications of all security events provided to Public Interest Registry within 24 hours of discovery

		events must be promptly reported to Public Interest Registry.	

#	Area	Requirement	Measure
9	Registrar Support	Registrar technical support	Call center availability 24x7 Automatic ticket response to initial email inquiry Email response from technical support within 30 minutes of inquiry Chat response within 30 seconds Call average speed of answer within 30 seconds Call abandonment rate less than 1%

10	Registrar Support	Technical support ticket resolution	**Support Tier 1 - Standard Tickets**: One hour response and resolved within 48 hours, daily update should be sent to Registry and Public Interest Registry on status. If not resolved and closed, it follows the escalation path. **Support Tier 2 - Critical Tickets**: Immediate response from vendor and resolved within 24 hours, update should be sent to Registry and Public Interest Registry on status. If not resolved and closed, it follows the escalation path. Ticket status reviewed and updated twice daily Report on technical support tickets daily by 0500 UTC

#	Area	Requirement	Measure
11	Reporting	**Monthly Deferred Revenue and Revenue Recognised Reports**: This report identifies deferred revenue/revenue to be recorded/recognised for the current month by TLD and transaction type.	Report available no later than the 5th calendar day after the end of the month.
12	Reporting	**Monthly Deferred Revenue and Revenue Recognition Forecast Reports**: These reports identify deferred revenue/revenue to be recognised for future month by TLD and transaction type.	Report available no later than the 5th calendar day after the end of the month.
13	Reporting	**Annual Deferred Revenue and Revenue Recognition Forecast Reports**: This report identifies deferred revenue/revenue to be recognised for future month by domain name, TLD and transaction type.	Report available no later than the 10th calendar day after the end of the year.
14	Reporting	**Monthly Billable Transactions Detail Report**: This report includes all domain name registration data (such as: create, renew, delete, transfers, redemption and reversal, and auto renew-related, discount program transactions) listed by transaction date, registrar, registrant and TLD.	Report available no later than the 5th calendar day after the end of the month.
15	Reporting	**Monthly Rebate Report**: This report includes all rebate data by domain name, promotion program, transaction date, registrar, registrant and TLD.	Report available no later than the 5th calendar day after the end of the month.

16	Reporting	**Monthly ICANN Fee Report**: This report lists ICANN fees by domain name, transaction date, registrar, registrant and TLD.	Report available no later than the 5th calendar day after the end of the month.
17	Reporting	**Monthly Registrar Invoicing**: Every registrar account receives an invoice and detail statement for the prior month.	Invoices are distributed electronically to registrars no later than the 5th calendar day after the end of the month.
#	**Area**	**Requirement**	**Measure**
18	Reporting	**Monthly Registration Data Access Report.** This report summarizes (a) service activity—requests for access to registration data using WHOIS, RDAP, bulk access, or other means; and (b) complaints—both those submitted through the formal mechanism established by ICANN (https://whois.icann.org/en/whoiscomplaints) and those submitted through any other means. In addition to these summaries, the report should describe any privacy, proxy, regulatory, or other issue that arose during the reporting period.	Report available no later than the 5th calendar day after the end of the month.
19	System	Registrar relationship and technical support systems	At a minimum, available 99.9% of the time.
20	System	Deferred Revenue System platform	At a minimum, available 99.9% of the time.
21	System	Deferred Revenue System Data Escrow frequency	Daily

22	System	Deferred Revenue System source code escrow	Monthly
23	System	DNS query response rate for all root delegated service address combined	Minimum 10,000/sec
24	System	DNS query response rate for each nameserver	Minimum 300%
25	System	Business Intelligence platform	At a minimum, data should be refreshed by 0500 UTC and available 99.9% of the time.
26	System	Web-Based Billing and Reporting platform	At a minimum, available 99.9% of the time.
27	System	Website uptime	Availability uptime 100%, except agreed upon maintenance windows Website response time 2 seconds

SCHEDULE A – DNS SERVICE LEVEL STANDARDS

The DNS Service Level Standards are provided to ensure .vu is always available and accessible though the DNS. The Service Level Standard targets specified in this contract are measured over a calendar month. The following table is a summary of Service Level Standards, which are further defined in later sections:

Service Level Standard	Target
DNS Practice Statement Acceptance	DNS Practice Statement to be accepted by the community that .vu serves.
DNS Performance	For UDP – handle 100 qps with ≤ 5 ms average latency For TCP – handle 100 qps with ≤ 50 ms average latency
DNS Server Planned Outages	Single outages ≤ 4 hours Total outages ≤ 8 hours / month No more than two .vu Name Servers should be scheduled for a planned outage at the same time
DNS Integrity	100 % correct and consistent outside Zone Push window
DNS Server Availability	≥ 99 % availability over the month. ≥ 95 % availability over any 24 hour period. respond to ≥ 99 % of queries. No more than two .vu Name Servers may be unavailable at any one time, whether for planned or unplanned outages.
DNS Zone Push (from primary to secondary DNS Servers)	≥ 6 Zone Pushes per day ≤ 60 minutes DNS Zone Push Window

ANNEX D – AUSTRAILIA RFP

2.2.1. Registration Service Performance and Availability

The following performance and availability criteria are to be met by the registry database. Definitions for performance criteria are provided in Appendix A:

a) *Service availability:* At least 99.9% per calendar month;

b) *Processing time:* At least 95% of queries serviced within 0.5 seconds. At least 95% of create/modify/delete requests serviced within one second;

c) *Planned outage:* limited to a maximum of 4 hours per calendar month; between 0001 and 1200 AEST Sundays. 3 days' notice is to be given to registrars; and

d) *Extended planned outage:* limited to a maximum of 12 hours per quarter; between 0001 and 2400 AEST Sundays. 28 days' notice is to be given to registrars.

2.3.4. DNS Service Performance and Availability

The following performance and availability criteria are to be met by the authoritative nameservers. The registry operator shall arrange independent monitoring and auditing of performance and availability and those monitoring and auditing reports shall be provided to auDA on a monthly basis. Definitions for performance criteria are provided in Appendix A:

a) *Overall DNS service availability:* 100% per calendar month;

b) *Service availability per registry operator nameserver site*: At least

99% per calendar month;

c) *Processing time – nameserver resolution:* At least 95% to be

processed in less than 0.25 seconds;

d) *Update delay time:* At least 95% of updates to the registry

database available to the nameserver service within 5 minutes;

e) *Overall registry operator DNS service planned outages:* nil; and

f) Cross-network nameserver round trip time: Under 300ms.

2.4.5. WHOIS Service Performance and Availability

The following performance and availability criteria are to be met by the WHOIS service. Definitions for performance criteria are provided in Appendix A:

a) *Service availability:* At least 99.9% per calendar month;

b) *Processing time:* At least 95% of enquiries serviced within one

second;

c) *Update delay time:* At least 95% of updates to the Registry

Database available to the WHOIS service within 5 minutes;

d) *Planned outage:* Limited to a maximum of 4 hours per calendar month; between 0001 and 1200 AEST Sundays. 3 days' notice is to be given to Registrars;

e) *Extended planned outage:* Limited to a maximum of 12 hours per quarter; between 0001 and 2400 AEST Sundays. 28 days' notice is to be given to Registrars; and

f) *WHOIS query limits:* Maximum number of matches to be returned in response to a query: 10. Maximum number of queries to be accepted from a single host: 20 per hour and 200 in any 24-hour period. Blacklist period: 24 hours.

ANEXO Sección 5.1

Registrant Verification – .AU RFP

2.2.7. Registration data validation

To improve the data quality in the .au registry, the registry operator must implement the following data field validation for key fields that have been supplied during the registration process:

• validate that the Registrant ID (e.g. Australian Company Number (ACN) or Australian Business Number (ABN)) matches the Registrant Name. This can be done using data available from the Australian Business Registry (https://abr.business.gov.au), the Australian Securities and Investment Commission (http://www.asic.gov.au) and the Australian Charities and Notfor-profits Commission Register (http://www.acnc.gov.au); and

• validate that Australian postal addresses provided by registrants match available addresses in the Australian Postal Corporation's address file (https://auspost.com.au/business/marketing-andcommunications/access-data-and-insights/address-data).

Any errors can be detected after registration and reported to auDA and the registrar responsible for the registration as a daily report.

auDA is committed to improving data quality in the .au registry, and may request further registry data fields be validated over the duration of the registry agreement. auDA expects the registry operator to contribute to improving data quality as part of its commitment to innovation.

Registrant Verification - .US RFP

C.9.6. The Contractor shall ensure the accuracy of the contact information submitted by registrants and retained by registrars in the kids.us domain by maintaining and updating the WHOIS database for such domain as described above (see section C.7).

Registrant Verification - .IN RFP

9.4.7 The deployed Software/ Application/ System should be able to support e-KYC

ANEXO Sección 5.3

ANEXO A – Investigación adicional

RFP de Estados Unidos - Provisión de extensión

OPCIÓN PARA AMPLIAR EL PLAZO DEL CONTRATO

(a) El Gobierno puede extender el término de este contrato mediante notificación por escrito al Contratista en cualquier momento antes de la expiración del contrato, siempre que el Gobierno le dé una notificación preliminar por escrito de su intención de prorrogar al menos 10 días antes de que expire el contrato. El aviso preliminar no compromete al Gobierno a una prórroga.

(b) Si el Gobierno ejerce esta opción, se considerará que el contrato extendido incluye esta cláusula de opción.

(c) La duración total de este contrato, incluido el ejercicio de cualquier opción bajo esta cláusula, no deberá exceder los 126 meses.