PLAN PLAN PARA LA MEJORA DE LA SEGURIDAD, ESTABILIDAD Y FLEXIBILIDAD DE INTERNET (FY 11)

Septiembre de 2010

Tabla de Contenidos

Resumen Ejecutivo 1
El Rol de ICANN 3
Programas de Seguridad, Estabilidad y Flexibilidad de ICANN 4
Planes para Mejorar la Seguridad, Estabilidad y Flexibilidad 4
1. Propósito y Generalidades 9
2. Desafío y Oportunidad 11
3. El Rol de ICANN 13
4. Contribuyentes de ICANN para los Esfuerzos de Seguridad, Estabilidad y Flexibilidad 17
5. Programas Continuos de ICANN Relacionados con la Seguridad, Estabilidad y Flexibilidad 21
5.1 DNS Central/Abordando la Seguridad, Estabilidad y Flexibilidad 21
5.1.1 Operaciones de IANA....22
5.1.2 Operaciones del DNS 26
5.2 Seguridad, Estabilidad y Flexibilidad de los Registros y Registradores de TLD 28
5.2.1 gTLD Registries 29
5.2.2 New gTLDs and IDNs....30
5.2.3 gTLD Registrars 32
5.2.4 Whois....34
5.2.5 Contractual Compliance 35
5.2.6 Protecting gTLD Registrants 36
5.2.7 ccTLDs 38
5.2.8 IANA Technical Requirements 39
5.2.9 Collaborative Response to Malicious Abuse of Domain Name System 39
5.2.10 Enabling Overall DNS Security and Resiliency 41
5.2.11 Validity, right of use, and uniqueness of Internet number resources. 42
5.3 Global Security Outreach (Engagement, Awareness) 43
5.3.1 Global Partners and Activities 43
5.3.2 Regional Partners and Activities....45
5.3.3 Working with Governments 47
5.4 Engaging with the Regional Internet Registries 48
5.5 ICANN Corporate Security and Continuity Operations 49
5.6 Activities of ICANN Supporting Organizations and Advisory Committees 50
6. ICANN FY11 Plans to Enhance Security, Stability and Resiliency 58
6.1 Core DNS/Addressing Functions....59
6.1.1 IANA Operations 59

6.1.2 DNS Operations 60
6.2 Relationships with TLD Registries and Registrars 60
6.2.1 gTLD Registries 61
6.2.2 New gTLDs 61
6.2.3 IDNs 61
6.2.4 ccTLDs 62
6.2.5 Registrars 62
6.2.6 Contractual Compliance 63
6.2.7 Collaborative Response to Malicious Abuse of Domain Name System 63
6.2.8 Enabling Overall DNS Security 64
6.3 Global Security Outreach 64
6.3.1 Extend Existing Partnerships 64
6.3.2 Commercial Enterprise 64
6.3.3 Participation in Global Cyber Security Dialogue 65
6.4 ICANN Corporate Security and Continuity Operations 65
6.5 ICANN Support Organizations and Advisory Committees 66
7. Conclusion 68
Appendix A–FY 11 SSR Resourcing 69
Appendix B – Glossary of SSR Plan Terms and Acronyms 79

Resumen Ejecutivo

Internet ha prosperado como un ecosistema que involucra a muchas partes interesadas, organizadas a través de la colaboración para fomentar la comunicación, la creatividad y el comercio en pos del bien común mundial. La interoperabilidad de los bienes comunes globales depende del funcionamiento y coordinación de los sistemas de identificadores únicos de Internet[1]. Tanto la Corporación para la Asignación de Números y Nombres en Internet (ICANN) como los operadores de estos sistemas reconocen que el mantenimiento y la mejora de la seguridad, la estabilidad y flexibilidad de estos sistemas es un elemento fundamental en su relación de colaboración.

Este documento es una actualización del Plan para la Mejora de la Seguridad, Estabilidad y Flexibilidad de Internet publicado el 16 de mayo de 2009 (de aquí en adelante referido como el Plan SSR 2009: http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf). Para el Año Fiscal 2011, el Plan SSR ha sido actualizado para reflejar las actividades relacionadas con la Seguridad de Internet programadas por la Corporación para la Asignación de Números y Nombres en Internet (ICANN) desde Junio de 2010 a Julio de 2011. Las actualizaciones realizadas a partir del Plan SSR 2009 serán señaladas en letra itálica. El Plan SSR FY11 está siendo publicado para la recepción de comentarios públicos desde Agosto hasta Septiembre de 2010.

El Plan Estratégico 2010-2013 de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) (http://www.icann.org/en/strategic-plan/strategic-plan-2010-2013-19feb10-en.pdf) establece "La estabilidad y la seguridad del Sistema de nombres de dominio (DNS) son prioridades fundamentales para la comunidad de ICANN y para los usuarios de Internet de todo el mundo. Ellas constituyen los elementos clave de la misión de ICANN. El uso indebido del DNS y los ataques contra éste y contra otra infraestructura de Internet aumentan constantemente. A fin de garantizar dichos elementos fundamentales para el DNS, como la seguridad, la estabilidad y la flexibilidad, ICANN debe trabajar en asociación con otros que participen en los aspectos más generales de estas cuestiones."

[1] De acuerdo con los Estatutos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), la misma coordina la asignación y atribución de tres conjuntos de identificadores únicos para Internet, que son: nombres de dominio (formando un sistema que es referido como: Sistema de Nombres de Dominio —DNS—); direcciones de protocolo de internet ("IP") y números de sistema autónomo ("AS"); y números de parámetro y puerto del protocolo.

El Plan Estratégico identifica a la estabilidad y seguridad del Sistema de Nombres de Dominio (DNS) como una de las cuatro áreas estratégicas clave de enfoque de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Esto está alineado con la gran importancia dada a la seguridad, estabilidad y flexibilidad (SSR) en la Afirmación de Compromisos (http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm) celebrada el 30 de septiembre de 2009 entre la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y la Administración Nacional de Telecomunicaciones e Información de los EE.UU. (NTIA). El Plan Estratégico separa la amplia gama de responsabilidades relacionadas con la seguridad, estabilidad y flexibilidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en objetivos estratégicos, trabajo de la comunidad, proyectos estratégicos y trabajo del personal.

El funcionamiento seguro, estable y elástico de los sistemas de identificadores únicos de Internet es una parte central de la misión de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Al aumentar la frecuencia y sofisticación de los ataques y otras conductas maliciosas, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y su comunidad deben continuar mejorando la elasticidad del Sistema de Nombres de Dominio (DNS) y fortalecer su capacidad de afrontar a este tipo de eventos. Al ampliarse la variedad de los ataques y conductas maliciosas, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) debe trabajar con otras partes interesadas en este ámbito, con el fin de clarificar el rol de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y para encontrar soluciones a problemas que rebasan la misión de cualquier entidad.

Los objetivos estratégicos identificados para la seguridad y estabilidad del Sistema de Nombres de Dominio (DNS) son:

1. *Tiempo de actividad del DNS al 100%*
2. *Disminución del uso indebido del DNS*
3. *Operaciones más seguras en los Dominios de Alto Nivel (TLD)*
4. *Mejora en la flexibilidad/capacidad de recuperación del DNS ante ataques*

El día 12 de febrero de 2010, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) publicó una Propuesta de

Iniciativas Estratégicas para Mejorar la Seguridad, Estabilidad y Flexibilidad (SSR) del Sistema de Nombres de Dominio (DNS) (http://www.icann.org/en/topics/ssr/strategic-ssr-initiatives-09feb10-en.pdf). El documento describe los fundamentos, características clave y costos proyectados de dos iniciativas estratégicas relacionadas con la seguridad y estabilidad del Sistema de Nombres de Dominio (DNS).

En base a la retroalimentación recibida en dos períodos de comentario público, durante la reunión de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en Nairobi, el Taller de Colaboración y Requisitos Operacionales del Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) y durante la reunión de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en Bruselas, dicha Corporación no tiene previsto operar un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT); en su lugar, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) continúa participando en charlas con las partes interesadas para definir los requisitos operacionales para una capacidad de respuesta colaborativa del Sistema de Nombres de Dominio (DNS) y la evaluación de riesgo de todo el Sistema de Nombres de Dominio (DNS) y análisis de amenazas.

El Rol de ICANN

Para establecer sus políticas y programas —incluyendo aquellos relacionados con la seguridad, estabilidad y flexibilidad—, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) actúa de conformidad con sus estatutos en cuanto a la conducción de procesos basados tanto en el consenso como en sus múltiples partes interesadas.

- El rol de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) debe enfocarse en sus misiones centrales, relacionadas con los sistemas de identificadores únicos.
- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) no juega un rol de control policial en la función de combatir el comportamiento delictivo.
- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) no tiene ningún rol relacionado al uso del espionaje informático y guerra informática en Internet.
- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) no tiene ningún rol relacionado con la determinación de lo que constituye un contenido ilícito en Internet.

- El rol de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) incluye la participación en actividades de la comunidad más amplia de Internet para combatir el abuso de los sistemas de identificadores únicos que permiten la actividad maliciosa. Estas actividades involucrarán la colaboración con los gobiernos, en relación al abuso y protección de estos sistemas.

Programas de Seguridad, Estabilidad y Flexibilidad de ICANN

- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) es responsable por las operaciones de la Autoridad de Números Asignados en Internet (IANA). La prioridad más alta ha sido —y continuará siendo—, el garantizar el funcionamiento seguro, estable y flexible de la zona raíz del Sistema de Nombres de Dominio.
- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) es mediadora para el Sistema de Nombres de Dominio (DNS) y facilita los esfuerzos de la comunidad para fortalecer las bases de seguridad, estabilidad y flexibilidad del sistema. Tales esfuerzos incluirán el apoyo al desarrollo y despliegue de protocolos y tecnologías de soporte para autenticar los nombres y números de Internet.
- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) es mediadora y facilitadora de las actividades de seguridad, estabilidad y flexibilidad llevadas a cabo por los registros del Sistema de Nombres de Dominio (DNS), los registradores y otros miembros de la comunidad.
- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) es responsable por el funcionamiento seguro, estable y flexible de sus propios recursos y servicios.
- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) es participante en foros y actividades más amplias relacionadas con la seguridad, estabilidad y flexibilidad de los sistemas de identificadores únicos de Internet.

Planes para Mejorar la Seguridad, Estabilidad y Flexibilidad

Durante el año operativo 2011 (FY11), la Corporación para la Asignación de Números y Nombres en Internet (ICANN) planea

llevar a cabo los programas e iniciativas descriptas en el presente documento. El Apéndice A detalla los objetivos, socios, resultados y compromisos de recursos específicos para los programas y actividades.

- ***Operaciones de la Autoridad de Números Asignados en Internet (IANA)****– el 16 de julio de 2010, la Corporación para la Asignación de Números y Nombres en Internet (ICANN), VeriSign y la Administración Nacional de Telecomunicaciones e Información (NTIA) implementaron las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) para la zona raíz autoritativa. Este fue un hito significativo en la mejora de la seguridad y estabilidad de Internet. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará trabajando con la comunidad de Internet para remover los obstáculos para la adopción de dichas extensiones de seguridad. Otras iniciativas incluyen el mejoramiento de la gestión de la zona raíz a través de la automatización y una autenticación de comunicaciones mejorada mediante gestores de Dominios de Alto Nivel (TLD).*
- ***Operaciones del Servidor Raíz del Sistema de Nombres de Dominio (DNS)*** *– La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará sus esfuerzos para llevar a cabo planes y ejercicios de contingencia con los operadores raíz y para mejorar la flexibilidad/capacidad de respuesta de la Raíz-L y la infraestructura.*
- ***Registros de Dominios Genéricos de Alto Nivel (gTLD)*** – Asegurar que se continúe evaluando a los solicitantes de los nuevos Dominios Genéricos de Alto Nivel (gTLD) y solicitantes de Nombres de Dominio Internacionalizados (IDN) para lograr un funcionamiento seguro. *La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará buscando la implementación de medidas para combatir el potencial de conductas maliciosas que surjan a partir del establecimiento de nuevos Dominios Genéricos de Alto Nivel (gTLDs).* La Corporación para la Asignación de Números y Nombres en Internet (ICANN) madurará el plan de continuidad del registro de Dominios Genéricos de Alto Nivel (gTLD) y continuará probando el sistema de custodia de datos.
- ***Registros de Dominios de Alto Nivel con Código de País (ccTLD)*** *– A medida que se introduzcan los Dominios de Alto Nivel con Código de País de Nombres de Dominio Internacionalizados (IDN ccTLDs) mediante el Proceso de Avance Acelerado, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará sus*

esfuerzos para abordar la gestión de variantes y las preocupaciones sobre mitigación de seguridad. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará su colaboración con los registros de Dominios de Alto Nivel con Código de País (ccTLD) para el programa de Plan de Respuesta a Ataques y Contingencia (ACRP) y el Curso de Operaciones de Registro (ROC), establecido conjuntamente con la Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO), las asociaciones regionales de Dominios de Alto Nivel (TLD) y la Sociedad de Internet (ISOC).

- ***Cumplimiento Contractual*** – La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará mejorando el alcance de las actividades de cumplimiento contractual que involucren a los Dominios Genéricos de Alto Nivel (gTLDs) para incluir auditorías iniciales de las partes contratadas, como parte de la implementación de las enmiendas de marzo de 2009 al Acuerdo de Acreditación de Registradores (RAA) e identificar la posible participación de las partes contratadas en actividades maliciosas para la toma de acciones de cumplimiento. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) también continuará facilitando consideraciones de políticas sobre acerca de las actividades de cumplimiento, como parte de las posibles enmiendas al Acuerdo de Acreditación de Registradores (RAA) en FY11.
- ***Respuesta al Abuso Malicioso del Sistema de Nombres de Dominio*** – La Corporación para la Asignación de Números y Nombres en Internet (ICANN) fortalecerá sus esfuerzos colaborativos relacionados con la conducta maliciosa habilitada por el abuso del Sistema de Nombres de Dominio (DNS) y facilitará el intercambio de información para permitir una respuesta efectiva.
- ***Seguridad Corporativa de ICANN y Continuidad de Operaciones*** – La Corporación para la Asignación de Números y Nombres en Internet (ICANN) asegurará que sus programas de seguridad sean llevados a cabo dentro del conjunto de gestión corporativa de riesgo, gestión de crisis y programas de continuidad de negocios. Uno de los enfoques principales será el establecimiento de una base sólida de planes y procedimientos de apoyo documentados. *Estos programas incluyen*:
    - ***Plan de Seguridad para Información Corporativa*** – *La Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha elaborado un Plan de Seguridad*

para Información Corporativa tomando como referencia las normas ISO 27002. El plan está siendo implementado en FY11.

- ***Plan de Seguridad para Reuniones*** *– Se ha elaborado un Plan de Seguridad para Reuniones a partir de los esfuerzos para apoyar una planificación de seguridad mejorada para las reuniones internacionales de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), dicho plan será utilizado en la selección y preparación de las reuniones de dicha Corporación de FY11 en adelante.*
- ***Plan de Seguridad Físico y para Personal*** *– Como parte de los esfuerzos para mejorar la seguridad para el personal y las instalaciones, estos dos planes están siendo implementados en FY11.*
- ***Plan de Continuidad de Negocios y Gestión de Incidentes*** *– En 2010, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) condujo un Ejercicio de Continuidad de la Autoridad de Números Asignados en Internet (IANA)y los esfuerzos continuarán en FY11 con un ejercicio de comunicaciones en crisis e implementación del Plan de Continuidad de Negocios y Gestión de Incidentes de la Corporación para la Asignación de Números y Nombres en Internet (ICANN).*
- ***Programa de Gestión de Riesgo Empresarial*** *– En FY10, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) implementó las Directrices para la Gestión de Riesgo Empresarial (ERM) y estableció el un programa de Gestión de Riesgo Empresarial (ERM). En FY11, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará mejorando este programa con una evaluación de riesgos y apoyo al Comité de Riesgo de la Junta Directiva de dicha Corporación.*

- ***Asegurar Participación Mundial y Cooperación*** – La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará mejorando asociaciones con el Grupo de Trabajo en Ingeniería de Internet (IETF), la Sociedad de Internet (ISOC), los Registros Regionales de Internet (RIRs)y los Grupos de Operadores de Red (NOGs), las Operaciones del Sistema de Nombres de Dominio (DNS) y el Centro de Análisis y Respuesta Centro de Investigación, el Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio (DNS-OARC) y el *Foro para Equipos de Respuesta a Incidentes* (FIRST). La Corporación para la Asignación de Números y Nombres en Internet

(ICANN) también participará en diálogos internacionales para buscar el entendimiento en cuanto a los desafíos de seguridad, estabilidad y flexibilidad que enfrenta el ecosistema de Internet, y respecto a cómo abordar estos desafíos con un enfoque de múltiples partes interesadas.

1. Propósito y Generalidades

El Plan SSR actualizado esboza a una amplia gama de partes interesadas la manera en que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) contribuirá con los esfuerzos mundiales en el abordaje de la seguridad, estabilidad y flexibilidad como desafíos de Internet, enfocándose en su misión relacionada con los identificadores únicos de Internet. El plan explica los roles y límites de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) respecto a cómo participa en esta área; las visiones generales existentes en los programas de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en esta área; y los detalles de las actividades planificadas y recursos dedicados durante el próximo año operacional. El plan está organizado en siete secciones y un apéndice:

- Sección 1: Propósito y Generalidades
- Sección 2: Desafío y Oportunidad
- Sección 3: El Rol de la Corporación para la Asignación de Números y Nombres en Internet (ICANN)
- Sección 4: Contribuyentes de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para los Esfuerzos de Seguridad, Estabilidad y Flexibilidad
- Sección 5: Programas Continuos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) Relacionados con la Seguridad, Estabilidad y Flexibilidad.
- Sección 6: *Planes de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) del Año Fiscal 2011 (FY11) para Mejorar la Seguridad, Estabilidad y Flexibilidad*
- Sección 7: Conclusión
- *Apéndice A: Objetivos, Socios, Indicadores/Resultados y Recursos para los Programas de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) de FY11 en cuanto a Seguridad, Estabilidad y Flexibilidad.*

Tal como se señala en el Resumen Ejecutivo, la presente actualización está basada en el Plan SSR 2009 y la visión y los objetivos establecidos en el Plan Estratégico 2010-2013 de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Esta versión del plan está destinada a brindar actualizaciones adicionales sobre la base de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y su comunidad con respecto a su rol, así como a mejorar el marco para la organización de los esfuerzos relacionados con la seguridad, estabilidad y flexibilidad. El plan ha sido actualizado

como parte de la revisión anual realizada conjuntamente con los ciclos de planificación estratégica y operativa de la Corporación para la Asignación de Números y Nombres en Internet (ICANN).

2. Desafío y Oportunidad

El animado ambiente de Internet se ve amenazado por los crecientes niveles de actividad maliciosa llevada a cabo por una variedad de actores que incluyen una fuerte participación de organizaciones criminales relacionadas con el fraude, la extorsión y otras actividades ilícitas en línea y un aumento en ataques de denegación de servicio (DoS) y otras actividades perjudiciales que se llevan a cabo a través de Internet. Cada vez más, la actividad en Internet refleja toda la gama de motivaciones y conductas humanas. En parte, tal actividad refleja la naturaleza abierta de Internet —la cual se ha logrado con éxito—, habiendo permitido tanto la innovación como la comunicación, la creatividad y el comercio en pos del bien común mundial. Sin embargo, la apertura también ha llegado con vulnerabilidades. Por ejemplo, la actividad que aprovecha las oportunidades de "suplantar datos" —*spoof*— o "envenenar" —*poison*— la resolución del Sistema de Nombres de Dominio (DNS) para orientar mal las conexiones de equipos informáticos de usuarios en forma involuntaria, está aumentando. Del mismo modo, la incidencia de secuestros de enrutamiento y dirección de registro así como el secuestro de registros de Números de Sistema Autónomo (ASN) continúa aumentando. Los ataques de denegación de servicio (DoS) pueden perjudicar a usuarios de todo tipo. Durante los últimos años se ha expresado una creciente preocupación por parte de toda la gama de partes interesadas de Internet: usuarios, empresas, estados soberanos, organizaciones involucradas en debates en torno a la Internet y la sociedad de la información más amplia. Los esfuerzos para hacer frente a estos desafíos deben abordar los riesgos para la seguridad y estabilidad que puedan provenir de la institución de nuevos controles que puedan ser maliciosamente utilizados por criminales o por diseños de red que hagan más difícil el logro de la estabilidad.

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) se ocupará de los riesgos para la seguridad, estabilidad y flexibilidad de Internet dentro de los límites de sus responsabilidades. El Artículo I de los Estatutos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) declara que su misión es: "coordinar, a nivel global, los sistemas mundiales de identificadores únicos de Internet y, en particular, garantizar el funcionamiento estable y seguro de los sistemas mundiales de identificadores únicos de Internet." Los programas y actividades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en esta área, se enfocan en la consecución de tres características principales dentro de los sistemas de identificadores únicos de Internet: seguridad,

estabilidad y flexibilidad/capacidad de respuesta. La seguridad es la capacidad para proteger y prevenir el mal uso de los sistemas de identificadores únicos de Internet. La estabilidad es la capacidad para garantizar que el sistema funciona como es esperado y que los usuarios de los sistemas de identificadores únicos tengan confianza en que el sistema funciona como es esperado. La flexibilidad/elasticidad es la capacidad de los sistemas de identificadores únicos para responder eficazmente a ataques maliciosos y otras actividades perjudiciales. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) trabaja con partes responsables de todos los sistemas de identificadores únicos para el logro de una apropiada implementación de sus políticas y acuerdos contractuales. Como organización guiada por múltiples partes interesadas, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) se asegura de que sus esfuerzos hagan el uso más eficaz de los recursos comunitarios disponibles en esta área, trabajando en estrecha colaboración con sus principales partes interesadas e identificando explícitamente los objetivos y métricas de desempeño en su planificación operativa, estratégica y financiera. Esta planificación brinda a la comunidad una hoja de ruta en cuanto a la forma en que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) cumple con sus responsabilidades. *El Apéndice A del plan proporciona los detalles sobre las actividades previstas para FY11, los indicadores/resultados y los recursos asociados. Un aspecto primordial de los objetivos para FY11 del personal de seguridad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) será el establecimiento de parámetros en la búsqueda de programas más amplios para mejorar la estabilidad, la seguridad y la flexibilidad globales de los sistemas de identificadores únicos*.

3. El Rol de ICANN

La Corporación para la Asignación de Números y Nombres en Internet (CANN) actúa de conformidad con sus estatutos en cuanto a la conducción de procesos basados tanto en el consenso como en sus múltiples partes interesadas, para establecer políticas y programas que incluyan aquellos relacionados con la seguridad, estabilidad y flexibilidad. La misión principal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) se centra en permitir un enfoque multilateral para el funcionamiento eficaz de las funciones de la Autoridad de Números Asignados en Internet (IANA); el establecimiento de políticas globales que garanticen la coordinación del Sistema de Nombres de Dominio (DNS), las direcciones de Protocolo de Internet (IP) y la asignación de IP; y el fomento de la competencia y elección dentro del ámbito de los Dominios Genéricos de Alto Nivel (gTLD), a través de un sistema de contratos con los Registros de los Dominios Genéricos de Alto Nivel (gTLD) y Registradores acreditados por la Corporación para la Asignación de Números y Nombres en Internet (ICANN).

Durante los últimos diez años y como parte de su misión, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha desempeñado un rol importante en cuanto a la contribución a la seguridad y estabilidad de los sistemas de identificadores únicos de Internet. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) y los operadores asociados de los sistemas de identificadores únicos, han reconocido y tomado conocimiento de que el mantenimiento y la mejora de la seguridad y la estabilidad de los servicios es un elemento fundamental de su relación. Este principio está manifiesto en el sistema de contratos y acuerdos entre la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y los operadores, en función de la naturaleza distintiva de sus relaciones, roles específicos y responsabilidades mutuas. Este esfuerzo colaborativo y su implementación, brindan una confianza esencial en que los identificadores únicos y las organizaciones que los proporcionan en todo el mundo garantizan la seguridad, estabilidad y flexibilidad a través de un sistema coordinado y cooperativo.

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) planea continuar contribuyendo a través de una amplia gama de actividades, para lograr que los sistemas de nombres y direcciones de Internet sean seguros, estables y flexibles ante la presencia de riesgos y amenazas en continua evolución. Del mismo modo, dedicará sus esfuerzos enfocados a su misión central relacionada con los sistemas de identificadores

únicos de Internet. No actuará como control policial en la función de combatir el comportamiento criminal ni comprometer a actores maliciosos La Corporación para la Asignación de Números y Nombres en Internet (ICANN) no se involucra en actividades o diálogos relacionados con el uso de Internet para el espionaje informático o guerra informática. Además, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) no se involucra en debates sobre qué constituye contenido ilícito que resida o transite Internet. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará participando con la comunidad de seguridad más amplia de Internet en los foros clave dedicados al combate de actividades maliciosas específicas (por ejemplo, suplantación de la identidad o correos electrónicos no deseados) que utilicen el sistema de identificadores únicos de Internet.

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) estructura sus actividades de seguridad, estabilidad y flexibilidad mediante la consideración de su rol: como responsable directo, como facilitador, como participante.

- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) es responsable directo de las operaciones de la Autoridad de Números Asignados en Internet (IANA) y colabora en la elaboración y distribución de la zona de la raíz con el Departamento de Comercio de los EE.UU. y VeriSign. El garantizar el funcionamiento seguro, estable y flexible de la zona raíz del Sistema de Nombres de Dominio (DNS) ha sido y continuará siendo su prioridad más alta. En forma adicional, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) es un facilitador primordial para los esfuerzos relacionados con el Sistema de Nombres de Dominio (DNS) que son llevados adelante por la comunidad, para autenticar los nombres y números de Internet. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) es partidaria de que uno de los pasos esenciales para abordar la seguridad del Sistema de Nombres de Dominio (DNS) es la implementación de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) (*El 16 de julio de 2010, la Corporación para la Asignación de Números y Nombres en Internet —ICANN—, VeriSign y la Administración Nacional de Telecomunicaciones e Información —NTIA— implementaron las Extensiones de Seguridad para el Sistema de Nombres de Dominio —DNSSEC— en la zona raíz*). Otros esfuerzos clave se enfocarán en la mejora de la comprensión de los riesgos a través de todo el sistema, permitiendo la implementación del Anclaje de Confianza Único (TA) de los Recursos de

Infraestructura de Clave Pública (RPKI) y cooperando con los asociados para mejorar las prácticas de seguridad y flexibilidad en la comunidad de los Dominios de Alto Nivel (TLD).

- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) funciona como un elemento facilitador de actividades relacionadas con la seguridad, la estabilidad y la flexibilidad, llevadas a cabo por los registros y registradores del Sistema de Nombres de Dominio (DNS). La naturaleza de las funciones y responsabilidades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) dependen de las características específicas de sus relaciones con estos operadores principales. En forma adicional a las actividades colaborativas, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha celebrado contratos con todos los registros de Dominios Genéricos de Alto Nivel (gTLD) y registradores por ella acreditados. Estos acuerdos se han convertido cada vez más en mecanismos para mejorar la seguridad, estabilidad y flexibilidad a través del Sistema de Nombres de Dominio (DNS). Los esfuerzos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para garantizar el cumplimiento y aplicar las disposiciones de esos acuerdos, constituyen un enfoque principal que continuará en el futuro. En lo que respecta a los registros de Dominio de Alto Nivel con Código de País (ccTLD), la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y los operadores de Dominios de Alto Nivel con Código de País (ccTLD) han expresado su compromiso de aumentar aún más la estabilidad, seguridad e interoperabilidad del Sistema de Nombres de Dominios (DNS), para el beneficio de la comunidad local y mundial de Internet y sobre la base de una relación entre pares. El intercambio de información, la asistencia mutua y el incremento de capacidad constituirán un enfoque principal de las futuras actividades. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) también se enfocará en respaldar las capacidades de respuesta colaborativa de la comunidad a fin de brindar un mejora en la seguridad del Sistema de Nombres de Dominio (DNS).
- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) participa en actividades con la Organización para Recursos de Numeración (NRO) y los Registros Regionales de Internet (RIRs), guiada por un entendimiento global de que los Registros Regionales de Internet (RIRs) y la Corporación para la Asignación de Números y Nombres en Internet (ICANN) deben mantener y mejorar la seguridad,

estabilidad y flexibilidad de Internet, para el beneficio de los usuarios de Internet tanto a nivel local como internacional.

- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) es directamente responsable por el funcionamiento seguro, estable y flexible de sus propios recursos y servicios, mientras conduce a la Autoridad de Números Asignados en Internet (IANA) y realiza otras funciones de coordinación; como lo es en su rol de operador del servidor raíz-L del Sistema de Nombres de Dominio (DNS).
- Las organizaciones de apoyo, comités asesores y personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), son participantes clave en los foros y las actividades más amplias cuyos objetivos varían desde la mejora de la flexibilidad en virtud de ataques perjudiciales hasta esfuerzos de colaboración enfocados en la lucha contra la actividad maliciosa en Internet, tales como la propagación de software malicioso y suplantación de la identidad, los cuales utilizan a los sistemas de identificadores únicos de Internet. Algunos ejemplos incluyen las sesiones detalladas sobre abuso del Sistema de Nombres de Dominio (DNS) y Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) llevadas a cabo en las recientes reuniones de la Corporación para la Asignación de Números y Nombres en Internet (ICANN).
- La Corporación para la Asignación de Números y Nombres en Internet (ICANN) tiene una misión de confianza pública respecto a su rol en la coordinación de los sistemas de identificadores únicos de Internet y desempeñará un rol de liderazgo en relación a los desafíos de lograr un ecosistema de Internet más seguro, estable y flexible, el cual también debe seguir siendo un ambiente vibrante para el diálogo, comercio e innovación a nivel mundial.

4. Contribuyentes de ICANN para los Esfuerzos de Seguridad, Estabilidad y Flexibilidad

El compromiso de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) relacionado con la seguridad, estabilidad y flexibilidad, involucra actividades llevadas a cabo a través del personal de la organización, de las organizaciones de apoyo y comités asesores. Los actores clave incluyen:

- ***Personal de la Autoridad de Números Asignados en Internet (IANA)*** – Responsable por llevar a cabo las funciones de la Autoridad de Números Asignados en Internet (IANA) para incluir la coordinación de la zona raíz del Sistema de Nombres de dominio (DNS), el funcionamiento del registro .arpa, la asignación de espacio de direcciones IP y el registro de protocolos y parámetros. Las actividades específicas relacionadas con la seguridad, estabilidad y flexibilidad están delineadas debajo.
- ***Personal de Operaciones del Sistema de Nombres de Dominio (DNS)*** – Responsable por el funcionamiento de la RAÍZ-L, una de los trece servidores de nombre raíz; la infraestructura de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) para los dominios y Dominios de Alto Nivel (TLDs) gestionados por la Corporación para la Asignación de Números y Nombres en Internet (ICANN); la firma de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) en la Raíz (KSK), instalaciones y ceremonias de KSK; alojamiento de Dominios de Alto Nivel con Código de País (ccTLD); servidores autoritativos del Sistema de Nombres de Dominio (DNS) de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y la carpeta de dominios de dicha Corporación. Los miembros del equipo de Operaciones del Sistema de Nombres de Dominio (DNS) asisten regularmente a reuniones tales como del Grupo de Operadores de Red de Norteamérica (NANOG), Redes IP Europeas (RIPE), Grupo de Operadores de Red de Medio Oriente (MENOG), Grupo de Operadores de Redes de Latinoamérica y el Caribe (LACNOG), Grupo de Operadores de Red de Nueva Zelanda (NZNOG), Grupo de Operadores de Red del Sur de Asia (SANOG) y Grupo de Operadores de Red de África(AFNOG) entre otras, para hablar acerca de varios aspectos relacionados con los proyectos para las actividades de Operaciones del Sistema de Nombres de Dominio (DNS) de la Corporación para la Asignación de Números y Nombres en Internet (ICANN).

- ***Personal de Servicios/Cumplimiento Contractual*** – Responsable por asegurar la coordinación y cumplimiento mediante los acuerdos realizados entre los registros de los Dominios Genéricos de Alto Nivel (gTLD) y los registradores acreditados por la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Las actividades específicas relacionadas con la seguridad, estabilidad y flexibilidad están delineadas debajo.
- ***Personal de Políticas*** – Responsable por asistir a las organizaciones de apoyo y comités asesores para llevar a cabo las actividades relacionadas con la formulación de políticas, incluyendo aquellos grupos de trabajo convocados por las organizaciones de apoyo.
- ***Personal de Asociaciones Internacionales (Global Partnerships)*** – Responsable por participar regional e internacionalmente con las partes interesadas de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para asegurar la participación mundial total en operaciones e implementación, de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). A este respecto, las actividades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) relacionadas con la seguridad, estabilidad y flexibilidad están integradas al trabajo general de *Global Partnerships* para la organización.
- ***Personal de Comunicaciones Corporativas*** – Responsable por asegurar la comunicación efectiva de los planes y programas de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y por representar a la organización en sus actividades ante la comunidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Las actividades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) relacionadas con la seguridad, estabilidad y flexibilidad están integradas al programa general de comunicaciones de la organización.
- ***Personal de Seguridad*** – Responsable por la planificación y ejecución diaria de los esfuerzos operativos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) relacionados con la seguridad y dirigidos por su Junta Directiva y Dirección Ejecutiva (CEO), en cumplimiento con los planes estratégicos y operativos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). El equipo coordina la amplia gama de esfuerzos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para participar efectivamente en temas relacionados con la seguridad, incluyendo la seguridad

informática y otros foros relacionados con la seguridad, estabilidad y flexibilidad.

- ***Comité Asesor de Seguridad y Estabilidad (SSAC)*** – Como Comité Asesor de la Corporación para la Asignación de Números y Nombres en Internet (SSAC) es responsable por la identificación de asuntos y desafíos clave que enfrenta la Corporación para la Asignación de Números y Nombres en Internet (ICANN) al asegurar la seguridad y estabilidad de los sistemas de identificadores únicos, e informándolos a la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y a la comunidad. El Comité lleva a cabo estudios sobre los asuntos clave —de acuerdo a lo solicitado por la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y de acuerdo a lo iniciado como parte de su mandato descripto debajo—, y colabora con otras organizaciones de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) tales como la Organización de Apoyo para Nombres Genéricos (GNSO).
- ***Comité Asesor en el Sistema de Servidores Raíz (RSSAC)*** – Como Comité Asesor de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), el Comité Asesor en el Sistema de Servidores de Raíz (RSSAC) brinda asesoría sobre los requisitos operativos de los servidores de nombre raíz al mismo tiempo que estudia y asegura sobre los aspectos de seguridad del sistema de servidores de nombre raíz y el desempeño, robustez y confiabilidad del sistema en su totalidad.

De acuerdo a lo descripto debajo, actividades más amplias relacionadas con la seguridad, estabilidad y flexibilidad toman lugar a través de las organizaciones de apoyo y comités asesores de la Corporación para la Asignación de Números y Nombres en Internet (ICANN).

El personal de seguridad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) tiene la responsabilidad general de una instrumentación efectiva a través de las actividades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y de establecer un plan integrado y un proceso de seguimiento para esas actividades garantizando su compatibilidad e integración a través de los distintos departamentos y partes interesadas. El Gráfico 1 representa la relación organizacional básica dentro de la estructura de la Corporación para la Asignación de Números y Nombres en Internet (ICANN).

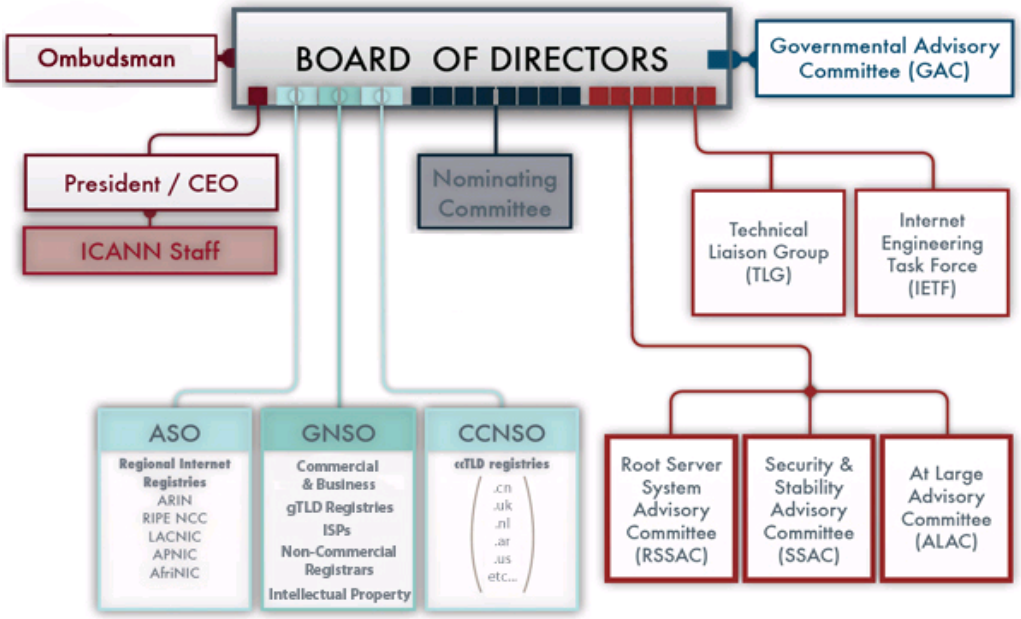


Gráfico 1 – Estructura organizacional de la Corporación para la Asignación de Números y Nombres en Internet (ICANN)

5. Programas Continuos de ICANN Relacionados con la Seguridad, Estabilidad y Flexibilidad

Esta sección describe los principales programas y actividades que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha llevado a cabo, los cuales contribuyen a la seguridad, estabilidad y flexibilidad de los sistemas de identificadores únicos de Internet, identificando a los principales socios operativos y proporcionando antecedentes sobre los esfuerzos existentes. El propósito de esta sección del plan es proporcionar un lineamiento básico de entendimiento de la amplia gama de actividades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) que contribuyen a la seguridad, estabilidad y flexibilidad de los sistemas de identificadores únicos. La mayoría de los principales elementos del personal, así como organizaciones de apoyo y comités asesores están involucrados en la búsqueda del cumplimiento eficaz de las responsabilidades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en esta área. En esta sección se presentan los antecedentes y la explicación de cómo los programas y actividades encajan en la estructura de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), así como la forma en que se entrecruzan con organizaciones externas.

La sección está organizada en torno al marco establecido en la Sección 3, comenzando con el Sistema de Nombres de Dominio (DNS) central/ funciones de direccionamiento; trabajo con las comunidades de registros y registradores de Dominios de Alto Nivel (TLD); participación con los Registros Regionales de Internet (RIRs) a través de la Organización de Apoyo para Direcciones (ASO); seguridad corporativa y continuidad de programas; actividades de las organizaciones de apoyo y comités asesores, y la participación en actividades regionales e internacionales sobre la seguridad, estabilidad y flexibilidad de Internet.

5.1 DNS Central/Abordando la Seguridad, Estabilidad y Flexibilidad

5.1.1 Operaciones de IANA

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) lleva adelante las funciones de la Autoridad de Números Asignados en Internet (IANA) en coordinación con el Departamento de Comercio de los EE.UU., VeriSign, Grupo de Trabajo en Ingeniería de Internet (IETF), Registros Regionales de Internet (RIRs) y operadores de Dominios de Alto Nivel (TLD), tal como se describe debajo. La conducción efectiva de estas actividades es la contribución fundamental de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para la estabilidad y flexibilidad de Internet. A través de la conducción de las funciones de la Autoridad de Números Asignados en Internet (IANA), la Corporación para la Asignación de Números y Nombres en Internet (ICANN) coordina y gestiona los registros de los identificadores clave permitiendo una Internet global e interoperable.

Mientras es bien conocido que Internet es una red mundial sin coordinación central, las operaciones clave del sistema de identificador único debe ser coordinado a nivel mundial, y esta función de coordinación está a cargo de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Específicamente, a través de las funciones de la Autoridad de Números Asignados en Internet (IANA), la Corporación para la Asignación de Números y Nombres en Internet asigna y mantiene sistemas de números y códigos únicos que se utilizan en las normas técnicas ("protocolos") que maneja Internet. Las diversas actividades de la Autoridad de Números Asignados en Internet (IANA) pueden ser ampliamente agrupadas en tres categorías:

- ***Nombres de Dominio*** – A través de las funciones de la Autoridad de Números Asignados en Internet (IANA) la Corporación para la Asignación de Números y Nombres en Internet (ICANN) gestiona la zona raíz, los dominios .int y .arpa y el recurso de prácticas de los Nombres de Dominio Internacionalizados (IDN). Las prácticas de gestión garantizan que cada cambio realizado en estas zonas es abordado de acuerdo a su impacto sobre la estabilidad y seguridad para los Dominios de Alto Nivel específicos, y para la zona raíz en general. El operar las funciones de la Autoridad de Números Asignados en Internet (IANA) también permite a la Corporación para la Asignación de Números y Nombres en Internet (ICANN) desempeñar un rol en permitir la seguridad del Sistema de Nombres de Dominio (DNS) y los sistemas de direcciones IP al desplegar y mantener anclajes de confianza en la raíz del Sistema de Nombres de Dominio (DNS) y sistemas de direcciones, los cuales pueden mejorar

enormemente la integridad de los datos de identificación única así como la integridad de las respuestas dentro del Sistema de Nombres de Dominio (DNS).

- ***Direcciones y Números de Sistema Autónomo*** – La Autoridad de Números Asignados en Internet (IANA) administra y gestiona el fondo mundial de direcciones IP (IPv4 e IPv6) y Números de Sistema Autónomo (ASNs). La Autoridad de Números Asignados en Internet (IANA) asigna estos recursos numéricos a los Registros Regionales de Internet (RIRs), conforme a las políticas globales de recursos de numeración que son elaboradas por las comunidades de los Registros Regionales de Internet a través de sus procesos de desarrollo de políticas y que son coordinadas a nivel mundial por la Organización de Apoyo para Direcciones (ASO). Este proceso de políticas participativo permite el consenso global por parte de los beneficiarios finales asegurando que la Autoridad de Números Asignados en Internet (IANA) y los Registros Regionales de Internet (RIR) actúan de manera justa, predecible y estable. *La Corporación para la Asignación de Números y Nombres en Internet (ICANN) está trabajando con los Registros Regionales de Internet (RIRs) —a través de la Organización de Apoyo para Direcciones (ASO)— y con el Grupo de Trabajo en Ingeniería de Internet (IETF) acerca del desarrollo de tecnología de Recursos de Infraestructura de Clave Pública (RPKI) para introducir la certificación de los recursos numéricos.*
- ***Asignaciones de Protocolo*** – Los registros de protocolos y parámetros son gestionados por la Corporación para la Asignación de Números y Nombres en Internet (ICANN) a través de la Autoridad de Números Asignados en Internet (IANA) y conjuntamente con el Grupo de Trabajo en Ingeniería de Internet (IETF). La Corporación para la Asignación de Números y Nombres en Internet (ICANN) implementa y mantiene los más de 700 registros de protocolos y parámetros de acuerdo a las normas elaboradas a través del proceso de consenso de larga data: la publicación de Solicitud de Comentarios (RFC). Trabajando en estrecha colaboración con el Grupo de Trabajo en Ingeniería de Internet (IETF) y los autores de las Solicitudes de Comentarios (RFCs), el personal encargado de las funciones de la Autoridad de Números Asignados en Internet (IANA) garantiza que los registros sean establecidos mediante procesos consistentes y cuenten con el mantenimiento pertinente para ser exactos y para estar disponibles. Las relaciones existentes entre el personal encargado de las funciones de la Autoridad de Números Asignados en Internet (IANA) y el Grupo de Trabajo en Ingeniería de Internet (IETF)

están documentadas en RFC 2860 y en el Acuerdo de Nivel de Servicio.

El personal encargado de las funciones de la Autoridad de Números Asignados en Internet (IANA)trabajó con la comunidad de Dominios de Alto Nivel (TLD) para realizar un seguimiento de la aplicación de mitigación dentro del sistema de Dominios de Alto Nivel (TLD) en respuesta a la vulnerabilidad de envenenamiento de caché del Sistema de Nombres de Dominio (DNS) descubierta en el verano de 2008 (véase la presentación "Vulnerabilidad al Envenenamiento de Caché del Sistema de Nombres de Dominio (DNS) 2008" en http://www. iana.org /about/presentations/ davies-cairo-vulnerability-081103.pdf). La Corporación para la Asignación de Números y Nombres en Internet (ICANN) se asegurará de que sus programas y actividades mejoren los procesos de seguridad, estabilidad y flexibilidad para los cambios/adiciones de la zona raíz y el funcionamiento de los anclajes de confianza para las consultas realizadas dentro del Sistema de Nombres de Dominio (DNS), como se detalla a continuación.

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) brinda anualmente al Departamento de Comercio de los EE.UU, un plan de información de seguridad relacionado con la conducción de las funciones de la Autoridad de Números Asignados en Internet (IANA) de acuerdo con el contrato de la Autoridad de Números Asignados en Internet (IANA) y como parte de su propia seguridad corporativa y planificación de contingencias. *En enero de 2010, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) llevó a cabo un exitoso Ejercicio de Continuidad de IANA, en el siguiente enlace véase el Informe Posterior a la Acción http://www.icann.org/en/security/iana-business-continuity-exercise-aar-23feb10-en.pdf.*

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) espera realizar las últimas asignaciones de espacio unicast IPv4 a los Registros Regionales de Internet (RIRs), durante el año calendario 2011. Las asignaciones se harán de acuerdo con la Política Global para la Asignación del Espacio de Direcciones IPv4 Remanente, la cual fue elaborada por las comunidades de los Registros Regionales de Internet (RIRs) y ratificada por la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), en marzo de 2009.

Si bien esta asignación vaciará el fondo del espacio de direcciones administrado por el Departamento de la Autoridad de Números

Asignados en Internet (IANA) de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), los Registros Regionales de Internet (RIRs) aún tendrán bloques de direcciones a partir de los cuales podrán repartir y asignar direcciones a los Proveedores de Servicios de Internet (ISPs) y otros operadores de red. Los Registros Regionales de Internet (RIRs) han estado trabajando en el establecimiento de políticas que garanticen el acceso a pequeños bloques de espacio de direcciones IPv4 para los recién llegados al mercado[2], durante el período posterior a que los últimos cinco/8s hayan sido asignados y antes de que el protocolo IPv6 haya sido adoptado por la mayoría de las redes conectadas a Internet.

Los Registros Regionales de Internet (RIRs) también han establecido políticas que permiten que el espacio de direcciones IPv4 sea transferido desde un operador de red a otro[3]. Estas políticas han sido diseñadas para permitir que las redes muevan las direcciones allí donde proporcionan mayor valor, permitiendo el crecimiento continuo de la red.

El Comité de Riesgos de la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) está trabajando en la evaluación de los riesgos que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) podría enfrentar como consecuencia de la menor disponibilidad de espacio de direcciones IPv4.

La solución a largo plazo es la adopción generalizada del protocolo IPv6. Si bien se han realizado progresos considerables y los Proveedores de Servicios de Internet (ISPs) —como XS4all en los Países Bajos—, están comenzando a ofrecer IPv6 como un servicio estándar a todos sus clientes, aún queda mucho camino por recorrer. En sus reuniones, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha realizado una serie de sesiones de sensibilización, mientras que los Registros Regionales de Internet (RIRs) tienen en funcionamiento programas de capacitación y sensibilización sobre IPv6. [4][5][6][7][8]

[2] http://www.nro.net/documents/comp-pol-201006.html#2-6

[3] http://www.nro.net/documents/comp-pol-201006.html#1-3-2

[4] http://www.afrinic.net/training/ipv6training.htm

[5] http://www.apnic.net/services/services-apnic-provides/training/courses/ipv6-essentials

La clave para recordar es que la Internet existente continuará funcionando incluso después de que los Registros Regionales de Internet (RIRs) hayan asignado sus reservas de IPv4. Habrá un período en el cual se podrá acceder a algunas redes mediante IPv6 y a otras no; sin embargo, IPv6 permitirá a los operadores continuar con el crecimiento de sus redes aún más allá de los límites impuestos por IPv4.

5.1.2 Operaciones del DNS

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha abogado por la necesidad de implementar las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) a nivel de la raíz. *Desde el Plan SSR inicial, la Corporación para la Asignación de Números y Nombres en Internet (ICANN), VeriSign y la Administración Nacional de Telecomunicaciones e Información (NTIA) han progresado en la implementación de dichas extensiones a través de una introducción a escala que conlleva a la firma de la raíz en su totalidad en el mes de julio de 2010. La primera ceremonia de Clave para Firma de la Llave (KSK) —de aquí en adelante referenciada como Ceremonia KSK—para las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) se llevó a cabo en Culpeper, Virginia el 16 de junio de 2010 (véase http://www.icann.org/en/announcements/announcement-4-16jun10-en.htm), y una segunda Ceremonia KSK fue realizada el día 12 de julio de 2010 en Los Ángeles, California, para permitir a la firma de la zona raíz. El despliegue de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) en la zona raíz proporciona beneficios para aquellos que publican información en el Sistema de Nombres de Dominio (DNS), permite a la comunidad de Internet y usuarios finales localizar el material de clave criptográfica "anclaje de confianza" en la zona raíz y proteger las resoluciones del Sistema de Nombres de Dominio (DNS) del envenenamiento de caché.*

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha comenzado a firmar .arpa y muchos de los dominios organizacionales propios de dicha Corporación. Los preparativos han incluido la implementación de un banco de pruebas para las Extensiones de Seguridad para el Sistema de

[6] https://www.arin.net/knowledge/v4-v6.html

[7] http://lacnic.net/en/eventos/ipv6/

[8] http://www.ripe.net/training/ipv6/outline.html

Nombres de Dominio (DNSSEC) desde junio de 2007, la colaboración con operadores de Dominios de Alto Nivel (TLD) y otros operadores del Sistema de Nombres de Dominio (DNS) en relación a los esfuerzos para implementar dichas extensiones, ganando habilidad técnica en la aplicación de enfoques criptográficos de conformidad con conformidad con estándares aplicables y asegurando que los esfuerzos para la implementación de Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) sean parte de los planes y presupuestos operativos. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha establecido un grupo de trabajo específicamente responsable del funcionamiento y seguridad en sus implementaciones de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), incluyendo la firma de icann.org y de iana.org. Finalmente, a los efectos de de generalizar aún más la implementación de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha establecido el Repositorio de Anclaje de Confianza Interino (ITAR) para Dominios de Alto Nivel (TLD) de la Autoridad de Números Asignados en Internet (IANA) como medida para asegurar que las claves de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) para los Dominios de Alto Nivel (TLDs) que hayan implementado Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) estén disponibles para aquellos que estén desplegando las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) en este momento.

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) colabora con los operadores de servidores de nombre raíz respecto a la coordinación segura y estable de la zona raíz, para garantizar una adecuada planificación de contingencia y mantener procesos claros en los cambios de la zona raíz. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará colaborando con los operadores de servidores de nombre raíz y otros operadores, respecto a la coordinación segura y estable del sistema de servidores raíz. El Comité Asesor en el Sistema de Servidores Raíz (RSSAC) ha sido un asesor clave en la manera en que los cambios de protocolo —tales como el agregado de registros IPv6 en la raíz—, afectan al sistema.

En forma adicional, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) administra el servidor de nombres raíz designado l.root-servers.net. A través de este rol operativo, el personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) también interactúa en el plano

operacional con los otros operadores de servidores raíz. Como operador de la raíz-L, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) también participa dentro de la comunidad del Sistema de Nombres de Dominio (DNS), incluyendo la contribución a esfuerzos de la comunidad, tales como el Sistema de Nombres de Dominio-Operaciones, el Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio (DNS-OARC) y el proyecto de investigación "Un Día en la Vida de Internet", de la Asociación Cooperativa para el Análisis de Datos en Internet Asociación Cooperativa para el Análisis de Datos de Internet (CAIDA). La Corporación para la Asignación de Números y Nombres en Internet (ICANN) se ha comprometido a utilizar sus operaciones para promover la diversidad y el entendimiento de las mejores prácticas recomendadas, buscando aprender y difundir lecciones.

El equipo de Operaciones del Sistema de Nombres de Dominio (DNS) también a respaldado el estudio de Escalamiento de la Raíz-L, http://www.icann.org/en/announcements/announcement-17sep09-en.htm.

En 2009, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) mejoró la flexibilidad/capacidad de respuesta de la Raíz L con instancias en Praga, República Checa y Estambul, Turquía. En 2010 y dentro del año fiscal 2011 están planeadas mejoras adicionales.

5.2 Seguridad, Estabilidad y Flexibilidad de los Registros y Registradores de TLD

Una responsabilidad fundamental y directa de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en relación a la seguridad, estabilidad y flexibilidad generales de Internet, es la gestión de acuerdos con los registros de Dominios Genéricos de Alto Nivel (gTLD) y registradores acreditados por la Corporación para la Asignación de Números y Nombres en Internet (ICANN), así como de la estructura del marco conceptual y de trabajo de los acuerdos utilizados para gestionar las relaciones con los registros de Dominio de Alto Nivel con Código de País (ccTLD). La Corporación para la Asignación de Números y Nombres en Internet (ICANN) tiene contratos con 16 registros de Dominios Genéricos de Alto Nivel (gTLD) y con más de 900 registradores acreditados que son responsables por la coordinación del registro de los nombres de dominio, garantizando la resolución del Sistema de Nombres de Dominio

(DNS). Las responsabilidades de estas partes contratadas están delineadas a través de Acuerdos de Registro (RA) y Acuerdos de Acreditación de Registradores (RAAs). A través de las disposiciones establecidas en esos acuerdos, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) busca proteger a los registrantes y contribuir al mantenimiento de la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio (DNS) y del entorno más amplio de Internet. Durante la década pasada, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha buscado fortalecer estos acuerdos para incluir disposiciones que mejoren la estabilidad y flexibilidad, tal como se describe debajo.

5.2.1 Registros de gTLD

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) colabora con los operadores de los Dominios Genéricos de Alto Nivel (gTLD) con respecto a la coordinación segura y estable de estos Dominios de Alto Nivel (TLDs). En forma adicional, cada uno de los registros de Dominios Genéricos de Alto Nivel (gTLD) tiene un contrato con la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Si bien algunos elementos de estos contratos pueden ser diferentes, las disposiciones relacionadas con la seguridad, estabilidad y flexibilidad, son coherentes a todos ellos. Estos acuerdos contienen una disposición que exige a los operadores de registro implementar especificaciones temporales o políticas establecidas por la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y políticas de consenso desarrolladas por la Organización de Apoyo para Nombres de Dominio (GNSO) y aprobadas por la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Otras disposiciones del acuerdo que contribuyen a un funcionamiento seguro y estable del registro, incluyen el requisito de custodia de datos y acuerdos de nivel de servicio para los servicios del Sistema de Nombres de Dominios (DNS) por una tercera parte, el sistema de registro compartido y las operaciones de servidor de nombres. Los contratos de Dominios Genéricos de Alto Nivel (gTLD) de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) especifican la disponibilidad, niveles de desempeño y requisitos del centro de datos. En 2007, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) puso en marcha un esfuerzo de planificación de continuidad de los Dominios Genéricos de Alto Nivel (gTLD), que ha resultado en el establecimiento de un plan de trabajo, así como en el compromiso a una serie de ejercicios anuales del plan para mejorar la capacidad de la comunidad de registros de

Dominios Genéricos de Alto Nivel (gTLD) para hacer frente a problemas o fallas dentro del sistema de registro/registrador.

En 2006, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) introdujo el Proceso de Evaluación de Servicios de Registros (RSEP) como un medio para facilitar un proceso oportuno y previsible para la introducción de nuevos servicios de registro. Un componente clave del Proceso de Evaluación de Servicios de Registros (RSEP) es la determinación de si el servicio propuesto tiene el potencial de plantear una cuestión de seguridad o estabilidad. Si se determina que el servicio propuesto podría plantear un problema de seguridad o estabilidad, la propuesta se refiere a un grupo independiente de expertos técnicos del Proceso de Evaluación Técnica de Servicios de Registro (RSTEP). El Proceso de Evaluación Técnica de Servicios de Registro (RSTEP) lleva a cabo la evaluación del servicio propuesto y hace una recomendación a la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) acerca de la conveniencia de aprobar o negar el servicio.

En el mes de octubre de 2009 se introdujo el proceso de Solicitud Acelerada de Seguridad del Registro (ERSR) (véase http://www.icann.org/en/registries/ersr/). Este proceso de solicitud fue desarrollado para brindar un proceso mediante el cual los registros de Dominios Genéricos de Alto Nivel (gTLD) informen a la Corporación para la Asignación de Números y Nombres en Internet (ICANN) acerca de incidentes de seguridad presentes o inminentes a sus Dominios de Alto Nivel (TLD) o al Sistema de Nombres de Dominio (DNS) para solicitar una exención contractual por acciones que pudiese tomar o hubiesen sido tomadas para mitigar o eliminar un incidente. Una exención contractual es una excepción de cumplimiento a una disposición específica del Acuerdo de Registro durante el período de tiempo necesario para responder al incidente. El proceso de Solicitud Acelerada de Seguridad del Registro (ERSR) ha sido diseñado para permitir que, en caso de incidente, se mantenga la seguridad operacional y se mantenga apropiadamente informadas a las partes relevantes (por ejemplo, la Corporación para la Asignación de Números y Nombres en Internet —ICANN—, otros proveedores afectados, etc.).

5.2.2 Nuevos gTLDs y Nombres de Dominio Internacionalizados (IDNs)

A través de FY10 y dentro del año fiscal FY11, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha

estado trabajando con la comunidad para mejorar la manera de abordar la mitigación de conductas maliciosas en los nuevos Dominios de Alto Nivel (TLDs) [Véase el Memorando Explicativo del 28 de mayo de 2010: Mitigando la Conducta Maliciosa, http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-memo-update-28may10-en.pdf].

Con el lanzamiento del Proceso de Avance Acelerado de Dominios de Alto Nivel con Código de País de Nombres de Dominio Internacionalizados (IDN ccTLD) en noviembre de 2009 y las preparaciones de los procesos de los nuevos Dominios de Alto Nivel (TLDs) a fin de incluir los Nombres de Dominio Internacionalizados (IDNs), la Corporación para la Asignación de Números y Nombres en Internet (ICANN) reconoce la necesidad de emprender esfuerzos para garantizar el funcionamiento seguro, estable y flexible de los nuevos operadores en el Sistema de Nombres de Dominio (DNS) y del sistema en su conjunto. La implementación de los nuevos Dominios Genéricos de Alto Nivel (gTLD) y el proceso de revisión incluyen una evaluación técnica de la capacidad del solicitante para operar un registro, así como la conformación de las cadenas de caracteres con los requisitos técnicos descriptos en las Solicitudes de Comentarios (RFCs), de acuerdo al protocolo de los Nombres de Dominio Internacionalizados en Aplicaciones (IDNA) y Directrices de los Nombres de Dominio Internacionalizados (IDN).

El 16 de noviembre de 2009, la Corporación para la Asignación de Números y Nombres en Interenet (ICANN) lanzó el Proceso de Avance Acelerado de Dominios de Alto Nivel con Código de País de Nombres de Dominio Internacionalizados (IDN ccTLD) (véase http://www.icann.org/en/topics/idn/fast-track/). Desde su lanzamiento, el programa ha recibido 34 solicitudes en 22 idiomas diferentes (véase http://www.icann.org/en/topics/idn/fast-track/string-evaluation-completion-en.htm). Estas cadenas de caracteres están actualmente transitando los pasos de delegación de la Autoridad de Números Asignados en Internet (IANA) y las primeras cadenas de caracteres correspondientes a Dominios de Alto Nivel con Código de País de Nombres de Dominio Internacionalizados (IDN ccTLD) han sido ingresadas en la zona raíz en el mes de mayo de 2010 para Egipto, Arabia Saudita, Emiratos Árabes Unidos y la Federación Rusa. En la reunión de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) celebrada en Bruselas en el mes de junio de 2010, la Junta Directiva de dicha Corporación aprobó la delegación de cadenas de caracteres para China, Hong Kong y Taiwán, y en el mes de agosto de 2010 fueron aprobadas cadenas de caracteres para Sri Lanka, Tailandia, Territorio Palestino Ocupado, Jordán y Túnez.

La introducción inicial de Dominios de Alto Nivel con Código de País de Nombres de Dominio Internacionalizados (IDN ccTLDs) en el Proceso de Avance Acelerado se limita a cadenas de caracteres no contenciosas que representan a nombres de países y territorios que corresponden a Dominios de Alto Nivel con Código de País (ccTLDs) ya existentes.

En el proceso de Avance Acelerado, un equipo de expertos independientes —el Panel de Estabilidad del Sistema de Nombres de Dominio (DNS)—,realiza una evaluación de la cadena de caracteres de Dominio de Alto Nivel con Código de País de Nombres de Dominio Internacionalizados (IDN ccTLDs) propuesta respecto a la confusión y posibles conflictos que pudiese tener con los requisitos de seguridad y estabilidad para las cadenas de caracteres de los Nombres de Dominio Internacionalizados (IDNs). Se espera que el proceso para los nuevos Dominios Genéricos de Alto Nivel (gTLD) tenga paneles expertos similares, disponibles para realizar la evaluación técnica de los solicitantes y sus Dominios de Alto Nivel (TLDs) propuestos. En forma adicional, el proceso de los nuevos Dominios Genéricos de Alto Nivel (gTLD) establece un Proceso de Evaluación de los Servicios de Registros (RSEP) por adelantado, a fin de evaluar posibles cuestiones de seguridad o estabilidad para los nuevos servicios de registro que son propuestos en la solicitud de Dominios Genéricos de Alto Nivel (gTLD).

Más aún, se requerirá que todos los solicitantes pasen una revisión técnica previa a la delegación, para comprobar que han cumplido con sus requisitos técnicos para operar un registro.

En FY11, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) tiene la intención de lanzar una revisión de la implementación del Proceso de Avance Acelerado de Dominios de Alto Nivel con Código de País de Nombres de Dominio Internacionalizados (IDN ccTLD).

5.2.3 Registradores de gTLD

La Corporación para la Asignación de Números y Nombres en Internet (CANN) colabora con los registradores en cuestiones relacionadas con la seguridad, estabilidad y flexibilidad. Contractualmente, la relación de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) con los registradores se rige por un Acuerdo de Acreditación de Registradores (RAA) estándar. El Acuerdo de Acreditación de Registradores (RAA) establece ciertas normas para la recolección, retención y custodia de datos. El Acuerdo de Acreditación de Registradores (RAA) también incorpora, mediante referencias, políticas de consenso desarrolladas por la comunidad de la

Corporación para la Asignación de Números y Nombres en Internet (ICANN), tales como la Política de Transferencia Entre Registros, la Política de Recordatorio de los Datos Whois y la Política de Exactitud de Nombres Restaurados, entre otros, que apoyan de diversas formas la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio (DNS). *En 2009 se introdujo un Acuerdo de Acreditación de Registradores (RAA) mejorado, y más del 95% de las registraciones de Dominios Genéricos de Alto Nivel (gTLD) ahora están cubiertas bajo dicho Acuerdo, mediante la adopción voluntaria de los registradores. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) también a publicado una Guía para No Abogados del Acuerdo de Acreditación de Registradores en respuesta a la solicitud de una guía, formulada por el Comité Asesor At-Large (véase http://www.icann.org/en/registrars/non-lawyers-guide-to-ra-agreement-15feb10-en.htm).*

El personal Responsable de Relaciones con los Registradores de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) actúa como primera línea en el control del cumplimiento de los registros respecto a los requisitos del Acuerdo de Acreditación de Registradores (RAA), realizado a diario y a través de la resolución informal de las quejas de los registrantes y de las disputas entre registradores así como mediante revisiones de acreditación en forma periódica (por ejemplo, ante la renovación de un Acuerdo de Acreditación de Registradores —RAA— de un registrador).

En respaldo de un sistema de nombres de dominio más estable, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha desarrollado programas y procedimientos para hacer frente a posibles fallos de los registradores. Por ejemplo, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha implementado su programa de Custodia de Datos de Registradores, el cual exige a los registradores depositar una copia de seguridad de los datos de registración en custodia, sobre una base diaria o semanal. El Procedimiento de Transición de Registrador Desacreditado facilita la transferencia en tiempo y forma de las registraciones desde un registrador desacreditado hacia un registrador acreditado por la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Además, el personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) utiliza varios procesos operativos internos que están destinados a ayudar a mantener un entorno saludable de registración de dominios y a evitar el perjuicio a los registrantes y usuarios de Internet, ante el evento de una falla de un registrador.

5.2.4 Whois

Los servicios Whois brindan acceso público a la base de datos sobre nombres de dominio registrados, la cual actualmente incluye información de contacto para los Titulares de Nombres Registrados. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) tiene un rol importante en la administración de reglas desarrolladas por la comunidad para el sistema Whois, dentro de los Dominios Genéricos de Alto Nivel (gTLD). Los cantidad de datos que se reúnen cuando se lleva a cabo la registración de un nombre de dominio, y la forma en la que se accede a la misma, se encuentran detallados en los contratos establecidos por la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para los nombres de dominio registrados dentro de los Dominios Genéricos de Alto Nivel (gTLD). Por ejemplo, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) requiere que los registradores acreditados colecten y brinden acceso público gratuito del nombre de dominio registrado y sus servidores de nombre y registradores, la fecha en que el dominio fue creado y cuándo vence su registro, así como la información de contacto del titular del nombre de registro y contactos técnico y administrativo.

Whois es utilizado por distintas comunidades para una serie de finalidades, entre ellas para facilitar la coordinación técnica y para ayudar a proporcionar información sobre las organizaciones e individuos que podrían estar implicados en el posible abuso del Sistema de Nombres de Dominio (DNS). Las actividades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) se centran en garantizar el cumplimiento de los registros y registradores de Dominios Genéricos de Alto Nivel (gTLD) acreditados por la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en cuanto a sus obligaciones contractuales. Al considerar los cambios de política relacionados con Whois, la comunidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) reconoce el uso legítimo del sistema Whois como ayuda en la lucha contra el abuso del Sistema de Nombres de Dominio (DNS), mientras busca lograr un equilibrio entre la amplia gama de intereses de las distintas partes interesadas respecto a la manera de operar del sistema Whois. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) reconoce las preocupaciones relacionadas con la privacidad y la seguridad que las personas han expresado acerca de hacer su información disponible a través de Whois. Dicha Corporación continúa los esfuerzos para abordar

estas preocupaciones. Reconociendo que el actual servicio Whois puede disminuir la fiabilidad y utilidad con el tiempo —y bajo la dirección de la Organización de Apoyo para Nombres Genéricos (GNSO)—, el personal de Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha recopilado un amplio conjunto de requisitos para la base de datos WHOIS, que incluyen las deficiencias conocidas del servicio actual así como los posibles requisitos que puedan ser necesarios para apoyar futuras iniciativas de políticas. [Referencia: Resoluciones del Consejo de la Organización de Apoyo para Nombres Genéricos (GNSO) de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), del mes de mayo de 2009.Marina Del Rey, CA: ICANN. Consultado el día 25 de octubre de 2009, de http://gnso.icann.org/resolutions/#200905]. El informe trata de identificar los requisitos técnicos que se necesitarían implementar para corregir las deficiencias y aplicar las futuras políticas Whois. Una serie de características en este inventario tienen su origen en las recomendaciones del Comité Asesor de Seguridad y Estabilidad (SSAC) a la Organización de Apoyo para Nombres Genéricos (GNSO), lo que demuestra que a través de consideraciones de medidas para mejorar Whois, realizadas en forma interdisciplinaria entre Organizaciones de Apoyo y Comités Auxiliares (SO/AC), la Corporación para la Asignación de Números y Nombres en Internet (ICANN) está comprometida a hallar soluciones que mantengan la utilidad de la base de datos WHOIS a la vez que considera la privacidad y la seguridad de la información de WHOIS.

5.2.5 Cumplimiento Contractual

El Departamento de Cumplimiento Contractual asegura que tanto la Corporación para la Asignación de Números y Nombres en Internet (ICANN) como sus partes contratadas cumplan con los requisitos establecidos en los acuerdos entre las partes. Sus actividades incluyen la gestión del sistema de recepción de reclamos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), el cual permite al público registrar quejas relacionadas con los nombres de dominio que pueden tener relación con cuestiones de seguridad, estabilidad y flexibilidad. Vea el sitio web en http://reports.internic.net/cgi/registrars/problem-report.cgi. Las denuncias sobre eventuales infracciones a Acuerdos de Acreditación de Registros (RAA) son investigadas por el personal de cumplimiento contractual y cuando se descubren infracciones contractuales, se toman acciones de acatamiento. Aunque la

mayoría de las denuncias recibidas a través de este sistema se refieren a cuestiones ajenas a la autoridad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) (por ejemplo, a correos no deseados, contenidos de sitios web, servicio al cliente de registradores), la Corporación para la Asignación de Números y Nombres en Internet (ICANN) remite las quejas a los registradores para que las mismas sean atendidas.

El Departamento de Cumplimiento Contractual también gestiona el Sistema de Informe de Problemas de Datos de WHOIS (WDPRS), al que se puede acceder en: http://wdprs.internic.net/. El Sistema de Informe de Problemas de Datos de WHOIS (WDPRS) está diseñado para ayudar a los registradores en el cumplimiento de su obligación de investigar las supuestas inexactitudes de datos de Whois. Este sistema, desarrollado en 2002, permite al público el registro de reclamos relacionados con la inexactitud de datos Whois y esos reclamos son transmitidos a los registradores para que tomen las acciones apropiadas. En consulta con la comunidad, el Sistema de Informe de Problemas de Datos de WHOIS (WDPRS) fue rediseñado en 2008 para hacer frente a varias inquietudes relacionadas con la escasa funcionalidad, capacidad limitada y falta de cumplimiento en el seguimiento. El nuevo diseño del Sistema de Informe de Problemas de Datos de WHOIS (WDPRS) fue lanzado en diciembre de 2008 y el equipo de Cumplimiento continúa mejorando este sistema, con el objetivo de aumentar la precisión de los datos Whois.

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) encargó al Centro de Investigaciones de Opinión Nacional de la Universidad de Chicago, realizar un estudio sobre la precisión de los datos de Whois. El día 15 de febrero de 2010 se publicó un informe preliminar.
http://www.icann.org/en/announcements/announcement-3-15feb10-en.htm.

5.2.6 Protección de Registrantes de gTLD

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) también se esfuerza por garantizar que los registrantes tengan confianza en la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio (DNS), en una variedad de maneras. Estas protecciones incluyen disposiciones en los contratos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), los acuerdos y la ejecución de programas. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) proporciona información a los registrantes acerca de las obligaciones de los registradores en virtud del Acuerdo de Acreditación de Registradores (RAA) y un

medio para la presentación de quejas a través del sitio web InterNIC, http://www.internic.net/. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) también ha conducido actividades de extensión con la comunidad de registradores, alentando el apoyo del protocolo IPv6 para los registrantes de dominios.

Además, el trabajo de las organizaciones de apoyo y comités asesores de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) se ha centrado en las preocupaciones de seguridad, estabilidad y flexibilidad de las registraciones. Asesorías pasadas del Comité Asesor de Seguridad y Estabilidad (SSAC) han identificado prácticas de los registradores deben considerar para proteger a los nombres de dominio y cuentas de registración de dominios contra el acceso no autorizado, y para proteger la información de configuración del Sistema de Nombres de Dominio (DNS) contra el uso indebido9. Los proyectos del Comité Asesor de Seguridad y Estabilidad (SSAC) en 2010 incluyen un informe complementario que identifica prácticas que los registrantes pueden implementar directamente para realizar un monitoreo proactivo y para proteger las cuentas de registración de dominios y la información de configuración del Sistema de Nombres de Dominio (DNS) contra el uso indebido. Otras actividades del Comité Asesor de Seguridad y Estabilidad (SSAC) incluyen documentos sobre la prohibición de la redirección por parte de los Dominios de Alto Nivel (TLDs) [SAC041], el despliegue de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), contactos documentados para casos de abuso [SAC038] y el tratamiento de los registros huérfanos del Sistema de Nombres de Dominio (DNS).

El Comité Asesor At-Large (ALAC) ha planteado varias cuestiones relativas a la protección de los registrantes. El Comité Asesor At-Large (ALAC) planteó por primera vez la cuestión de la prueba de dominio, la cual condujo al Consejo de la Organización de Apoyo para Nombres de Dominio (GNSO) y a la Junta Directiva a la aprobación de una nueva política de consenso destinada a eliminar el abuso del agregado del período de gracia para la prueba de dominio. *Más recientemente, el Comité Asesor At-Large (ALAC) abordó las preocupaciones del Consejo de la Organización de Apoyo para Nombres Genéricos (GNSO) acerca de la recuperación de nombres de dominio luego de su vencimiento, por*

[9] Véase SAC 40, Medidas para Proteger los Servicios de Registración de Dominios Contra la Explotación o el Uso Indebido, 19 de agosto de 2009 (http://www.icann.org/en/committees/security/sac040.pdf).

parte de los registrantes (PEDNR) y la responsabilidad y transparencia en la registración de los nombres de dominio. [http://www.atlarge.icann.org/announcements/announcement-19jul10-en.htm]. La Organización de Apoyo para Nombres de Dominio (GNSO) está llevando a cabo una serie de iniciativas que tienen el potencial de resultar en una mejor protección de los registrantes tales como las mejoras en la Política de Transferencia Entre Registros, las cuales incluyen la consideración de la necesidad de una autenticación electrónica y desarrollos de políticas en áreas de alojamiento fast flux y políticas de abuso de registración.

5.2.7 Dominios de Alto Nivel con Código de País (ccTLDs)

La interacción de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) con los registros de Dominio de Alto Nivel con Código de País (ccTLD) está guiada por el entendimiento general de que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y los registros de Dominios de Alto Nivel con Código de País (ccTLD) han de mantener y mejorar la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio (DNS) para el beneficio de los usuarios de Internet, tanto locales como internacionales. Esto se refleja en el programa de marco conceptual y de trabajo sobre responsabilidad, que conforma la base para una serie de acuerdos entre los distintos registros individuales de Dominios de Alto Nivel con Código de País (ccTLD) y la Corporación para la Asignación de Números y Nombres en Internet (ICANN). El enfoque principal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para promover la mejora de la seguridad, estabilidad y flexibilidad en los Dominios de Alto Nivel con Código de País (ccTLD) a través del trabajo conjunto con otros, consiste en proporcionar una plataforma para el intercambio de información y la acción común, capacitación técnica de sensibilización y capacidad de construir planes de respuesta a ataques y contingencias. El personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) trabaja en colaboración estrecha con los operadores de Dominios de Alto Nivel (TLD) para darles a conocer las cuestiones de seguridad a través del Personal de la Autoridad de Números Asignados en Internet (IANA), el Plan de Respuesta a Ataques y Contingencia (ACRP) y los esfuerzos de los responsables de relaciones regionales de Asociaciones Internacionales —*Global Partnerships*—. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha desarrollado una relación de confianza con los operadores de Dominios de Alto Nivel (TLD) a través de la mejora en el desempeño y difusión para la comunidad

de operadores de Dominios de Alto Nivel (TLD), la cual asiste en facilitar una respuesta colaborativa ante situaciones que requieren de coordinación mundial en relación con el Sistema de Nombres de Dominio (DNS).

5.2.8 Requisitos Técnicos de IANA

A través de la gestión de la función del Personal de la Autoridad de Números Asignados en Internet (IANA), la Corporación para la Asignación de Números y Nombres en Internet (ICANN) también ayuda a asegurar que los Dominios de Alto Nivel (TLDs) cumplan con los requisitos técnicos para apoyar operaciones estables y seguras. Los requisitos específicos del servidor de nombres aseguran la disponibilidad de dominios del Sistema de Nombres de Dominios (DNS), y el personal de la Autoridad de Números Asignados en Internet (IANA) trabaja en estrecha colaboración con los administradores de los Dominios de Alto Nivel (TLD) para resolver cualquier problema que pueda surgir en el mantenimiento de esos estándares técnicos. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) no participa en sí misma en las operaciones de los Dominios de Alto Nivel con Código de País (ccTLD), pero está lista para ayudar ante situaciones en las que se efectúen cambios en sus datos de zona raíz para que se realice en forma rápida y fiable. El objetivo general de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) es garantizar la estabilidad y la seguridad de la zona de Dominios de Alto Nivel (TLD) y de la zona raíz.

5.2.9 Respuesta Colaborativa al Abuso Malicioso del Sistema de Nombres de Dominio

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) coopera con una serie de organizaciones en distintos emprendimientos para garantizar que las partes interesadas puedan analizar la actividad que podría involucrar el abuso del Sistema de Nombres de Dominio (DNS). Desde fines de 2008 ha ocurrido un gran incremento en la actividad que involucra el aprovechamiento del Sistema de Nombres de Dominio (DNS). Uno de los más notables de dichos incidentes fue el gusano informático Conficker [Revisión y Resumen sobre Conficker, http://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf]. La Corporación para la Asignación de Números y Nombres en Internet (CANN) participó en una respuesta global y colaborativa para contener a Conficker, conjuntamente con las comunidades de seguridad, operadores de registros de Dominios de Alto Nivel (TLD) y fuerzas de orden público. La Corporación para

la Asignación de Números y Nombres en Internet (ICANN) publicó un informe, Revisión y Resumen sobre Conficker, el cual documenta los eventos relacionados con la contención de Conficker en forma cronológica, analiza las lecciones aprendidas y sugiere formas para mejorar futuros esfuerzos de colaboración (por ejemplo, el proceso de Solicitud Acelerada de Seguridad del Registro —ERSR— de ICANN). La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continúa trabajando con los registros y registradores para garantizar la toma de consciencia y sensibilización sobre este respecto, así como para facilitar la difusión de información cuando se producen incidentes de seguridad a escala mundial que involucran la participación del Sistema de Nombres de Dominio (DNS). El mandato de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) es limitado en este ámbito y por lo tanto ha participado como par en las discusiones realizadas acerca de cómo habilitar una respuesta eficaz cuando surgen determinadas situaciones operativas.

Para facilitar una mayor colaboración en este ámbito, el personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha brindado apoyo a esfuerzos realizados dentro de la Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO) para la respuesta a incidentes de los Dominios de Alto Nivel con Código de País (ccTLDs). En el mes de febrero de 2010, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) publicó un Caso Concreto de Negocios a nivel Mundial para un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) (http://www.icann.org/en/topics/ssr/dns-cert-business-case-19mar10-en.pdf) que funcione en la comunidad de Internet. El caso concreto de negocios contiene una descripción de los requisitos y posibles costos, incluyendo la opción de que otros miembros de la comunidad operen la función de dicho Equipo. A partir de la publicación del Caso Concreto de Negocios a nivel Mundial para un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT), de la consideración de los comentarios públicos recibidos (http://www.icann.org/en/public-comment/summary-analysis-strategic-ssr-initiatives-and-dns-cert-business-case-24may10-en.pdf) y de los debates que tomaron lugar en las reuniones que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) celebró en Nairobi y en Bruselas, dicha Corporación ahora está trabajando con las partes interesadas en la identificación de maneras de abordar una capacidad de respuesta colaborativa del Sistema de Nombres de Dominio (DNS), que no sea operada por la Corporación para la Asignación de

Números y Nombres en Internet (ICANN) sino que sea elaborada en colaboración con la comunidad.

5.2.10 Facilitar la Seguridad y Flexibilidad General del DNS

Si bien ninguna entidad tiene la responsabilidad general, el personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), las organizaciones de apoyo y los comités asesores juegan un rol importante en posibilitar la estabilidad, seguridad y flexibilidad generales del Sistema de Nombres de Dominio (DNS). Desde su creación, el Comité Asesor de Seguridad y Estabilidad (SSAC) ha proporcionado análisis y recomendaciones a la comunidad del Sistema de Nombres de Dominio (DNS). La Asesoría 004 de dicho Comité: *Asegurando el Límite* brinda un análisis sobre los fundamentos relacionados con los desafíos de seguridad para los sistemas de identificación única[10]. Los esfuerzos clave incluyeron el análisis y recomendaciones relacionadas con los ataques de Denegación de Servicio Distribuido por el Sistema de Nombres de Dominio (DDoS), implementación de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) agregando los registros IPv6 a la raíz del Sistema de Nombres de Dominio (DNS), front running de nombres de dominio, alojamiento fast flux y secuestro de nombres de dominio. En forma adicional, los miembros del Comité Asesor de Seguridad y Estabilidad (SSAC) participan en el Comité de Políticas de Internet del Grupo de Trabajo sobre Suplantación de la Identidad (Phishing) —APWG— y han sido coautores de documentos sobre la manera en que los phishers explotan los nombres de dominio y sub dominios, la manera en que las organizaciones deben responder a un ataque de sitio web y están colaborando con la Unidad Constitutiva de Propiedad Intelectual (IPC) para estudiar las vulnerabilidades de los sitios web comúnmente explotados.

[10] SAC 004, Asegurando el límite, 17 de octubre de 2002, http://www.icann.org/en/committees/security/sac004.pdf.

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará con su rol de facilitador en la búsqueda de identificación de oportunidades de colaboración de toda la comunidad, y para identificar y mitigar los riesgos para los sistemas. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha iniciado esfuerzos para mejorar el entendimiento y la mitigación de los riesgos del Sistema de Nombres de Dominio (DNS) durante su Simposio sobre Seguridad, Estabilidad y Flexibilidad del Sistema de Nombres de Dominio (DNS) celebrado en el mes de febrero de 2009 y realizado en forma conjunta con el centro de seguridad Georgia Tech Information Security Center (GTISC). El simposio se enfocó en el entendimiento de los riesgos relacionados con el Sistema de Nombres de Dominio (DNS) en grandes empresas, los desafíos de la seguridad y las operaciones seguras, estables y flexibles del Sistema de Nombres de Dominio (DNS) en ambientes de recursos limitados y en abordar el uso indebido del Sistema de Nombres de Dominio (DNS) para actividad maliciosa. Este informe se encuentra disponible en http://www.gtisc.gatech.edu/icann09. *En el mes de febrero de 2010 se realizó un Segundo Simposio sobre Seguridad, Estabilidad y Flexibilidad en Kyoto, Japón, véase http://dns-srr.e-side.co.jp/, y el informe fue publicado en abril de 2010 en http://www.icann.org/en/announcements/announcement-26apr10-en.htm.*

Además, el personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), las organizaciones de apoyo y los comités asesores han iniciado una mayor colaboración mediante una serie de esfuerzos de partes interesadas a fin de mejorar la capacidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para conducir efectivamente la formulación de políticas, el cumplimiento contractual y otras iniciativas, de un modo que aborden los desafíos de seguridad y flexibilidad planteados para y mediante el Sistema de Nombres de Dominio (DNS).

5.2.11 Validación, derecho a uso y singularidad de los recursos numéricos de Internet

A través de la gestión de las funciones de la Autoridad de Números Asignados en Internet (IANA), la Corporación para la Asignación de Números y Nombres en Internet (ICANN) adquiere la estrategia y la responsabilidad de la estabilidad, seguridad y flexibilidad del sistema de asignación numérica de Internet y, en definitiva, a través de la aplicación de Recursos de Infraestructura de Clave Pública (RPKI), del sistema de enrutamiento global de

Internet. Esta responsabilidad pone de manifiesto la necesidad de implementar una aplicación técnicamente ideal de anclaje de confianza único de Recursos de Infraestructura de Clave Pública (RPKI), tal como fuese señalado por el Comité de Arquitectura de Internet (IAB) [11] y la Organización de Recursos Numéricos (NRO) [12], y resulta en la capacidad de certificar plenamente la validez, el derecho de uso y la singularidad de los recursos numéricos de Internet. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) y su personal han realizado importantes esfuerzos de trabajo con el Grupo de Trabajo en Ingeniería de Internet (IETF) y otros grupos de enfoque mediante la participación en el proceso de normas, la comunicación con las partes interesadas y la implementación de una prueba (ahora retirada) para la aplicación de Recursos de Infraestructura de Clave Pública (RPKI).

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) está comprometida a trabajar con todas las partes interesadas de los Recursos de Infraestructura de Clave Pública (RPKI) y el Personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha iniciado los procesos de una manera que garantice que la implementación técnica más sensible sea realizada y esté disponible para la comunidad de Internet conforme a los plazos y demanda de consideración apropiados.

5.3 Extensión de la Seguridad a Nivel Mundial (Participación, Toma de Consciencia)

5.3.1 Asociados y Actividades Internacionales

El enfoque central de la estrategia de participación mundial de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en relación con la seguridad, estabilidad y flexibilidad consiste en construir y utilizar el trabajo existente realizado por el equipo de asociaciones internacionales. Muchos de estos esfuerzos están dirigidos por el equipo de Asociaciones Internacionales (*Global Partnerships*) de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). La Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha sido un participante activo en una amplia

[11] http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html

[12] http://www.nro.net/news/nro-declaration-rpki.html

gama de foros mundiales relacionados con Internet, incluyendo varios que abordan cuestiones de seguridad, estabilidad y flexibilidad de Internet. La gama de asociados y las actividades que se listan a continuación no son exhaustivas, y la Corporación para la Asignación de Números y Nombres en Internet (ICANN) buscará el compromiso de otras al surjir la oportunidad. Los asociados mundiales clave incluyen:

- ***Grupo de Trabajo en Ingeniería de Internet (IETF)/Consejo de Arquitectura de Internet (IAB):*** Conduce los esfuerzos para establecer enfoques tecnológicos para promover la seguridad en Internet, centrada en el desarrollo de protocolos y prácticas operativas más fuertes. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) trabaja con el Grupo de Trabajo en Ingeniería de Internet (IETF) en el establecimiento de estos protocolos relacionados con nombres y direccionamiento, y se esfuerza para garantizar su despliegue dentro del núcleo de Internet para ayudar a lograr un ambiente general seguro. En particular, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) participará en los esfuerzos para establecer protocolos que proporcionen una base para más segura para Internet, enfocada en esfuerzos tales como las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) y Recursos de Infraestructura de Clave Pública (RPKI).
- ***Sociedad de Internet (ISOC)***: Promueve la sensibilización/conciencia de las preocupaciones de seguridad informática y la necesidad de establecer confianza en Internet para los usuarios a nivel mundial, particularmente en el mundo en desarrollo; en colaboración con otros, proporciona capacitación técnica para mejorar la seguridad y flexibilidad de Internet. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) trabaja con la Sociedad de Internet (ISOC) para ayudar a garantizar la toma de consciencia y capacidades mejoradas relacionadas con la seguridad, estabilidad y flexibilidad. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) tiene previsto colaborar en la maduración del actual programa conjunto de la Sociedad de Internet (ISOC)/Corporación para la Asignación de Números y Nombres en Internet (ICANN) para impartir capacitación a los operadores de Dominios de Alto Nivel (TLD) para incluir formación técnica sobre la manera de mejorar la seguridad y mitigar los ataques y perjuicios informáticos.
- ***Foro de Gobernanza de Internet (IGF)***: El Foro de Gobernanza de Internet (IGF) patrocina diálogos entre las múltiples partes

interesadas sobre la seguridad y confianza en Internet. Además, el Foro de Gobernanza de Internet (IGF) ha desarrollado un enfoque en la gestión de recursos críticos de Internet y delitos informáticos. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará participando en el Foro de Gobernanza de Internet (IGF), inclusive brindando sensibilización/toma de conciencia de su rol en cuanto a la seguridad, estabilidad y flexibilidad en relación al sistema de identificador único de Internet, y contribuyendo al diálogo mundial en este Foro.

- ***Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio (DNS-OARC)***: La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará apoyando como patrocinador y participante activo a través de toda la gama de actividades del Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio (DNS-OARC).

5.3.2 Asociados y Actividades Regionales

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha establecido lazos regionales a través de una serie de asociaciones y actividades. A continuación se destacan los aspectos clave de las actividades regionales de la Corporación para la Asignación de Números y Nombres en Internet (ICANN):

- ***Asociaciones Regionales de Dominios de Alto Nivel con Código de País (ccTLD)*** – Además de colaborar en el programa de Plan de Respuesta a Ataques y Contingencia (ACRP), como se especifica debajo, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará brindando asistencia y experiencia para las actividades patrocinadas por estas organizaciones.
- ***Centros de Información de Redes (NICs)/Grupos de Operadores de Redes (NOGs) Regionales***– La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará participando en estos foros a fin de garantizar que sus actividades facilitan del mejor modo las operaciones seguras y flexibles de red, incluyendo la coordinación con las actividades del personal de la Autoridad de Números Asignados en Internet (IANA).
- ***Asia*** – En el mes de mayo de 2008, en Kuala Lumpur, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) inició el programa de capacitación sobre seguridad y flexibilidad de los Dominios de Alto Nivel con Código de País (ccTLD), en colaboración con la Asociación de Administradores de Registros de Dominios de Alto Nivel de

Asia-Pacífico (APTLD) y a partir de entonces ha estado recibiendo un fuerte apoyo continuado para la actividad en esa región. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará participando en foros regionales tales como Recursos Esenciales de Gestión de Internet para proporcionar asesoramiento operacional y capacitación relacionados con la seguridad y flexibilidad del Sistema de Nombres de Dominio (DNS), al surgir la oportunidad.

- ***Europa*** – la Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará participando en los esfuerzos de la Agencia Europea de Seguridad de Redes (ENISA) relacionados con las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) y mejora de la flexibilidad del Sistema de Nombres de dominio (DNS), como parte del esfuerzo de la Comisión Europea en el área de protección de infraestructuras críticas. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) colaborará con el Consejo de los Registros Nacionales Europeos de Dominios de Alto Nivel (CENTR) para llevar a cabo sesiones de capacitación sobre la seguridad y flexibilidad de los Dominios de Alto Nivel con Código de País (ccTLD), las cuales se iniciaron conjuntamente con la reunión de mayo de 2009, RIPE 58, en Ámsterdam. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará su colaboración con el Instituto de Cuestiones de Seguridad de la Información (IISI) de la Universidad Estatal de Moscú, en el fomento del diálogo mundial sobre seguridad en Internet. Específicamente, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y el Instituto de Cuestiones de Seguridad de la Información (IISI) celebraron seminarios conjuntos en Garmisch, Alemania —en 2008 y 2009—, con el apoyo del centro germano/americano Centro Marshall para Estudios Estratégicos, y ambos planean continuar con la colaboración en 2011.
- ***África y América Latina*** –la Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará las actividades relacionadas con la seguridad informática, conjuntamente con las organizaciones regionales de la Sociedad de Internet (ISOC), así como en otros foros apropiados. En 2009 y 2010 la Corporación para la Asignación de Números y Nombres en Internet (ICANN) brindó capacitación relacionada con la seguridad y flexibilidad a los Dominios de Alto Nivel con Código de País (ccTLD) conjuntamente con la Asociación de Dominios de Alto Nivel de Latinoamérica y el Caribe (LACTLD). La Corporación para la Asignación de Números y Nombres en Internet ICANN)

también brindó capacitación a los Dominios de Alto Nivel con Código de País (ccTLD) conjuntamente con la Organización de Dominios de Alto Nivel de África (AFTLD), la Sociedad de Internet de África (ISOC-África) y con Ala sociación de Dominios de Alto Nivel de Asia Pacífico (APTLD) en Asia.

5.3.3 Trabajando con los Gobiernos

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) colabora con los gobiernos de todo el mundo en la búsqueda de la seguridad, estabilidad y flexibilidad de los sistemas de identificadores únicos de Internet. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará brindando su perspectiva técnica y operativa en cuanto a la mejora de la seguridad, la estabilidad y la flexibilidad del sistema de identificación única de Internet. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) entiende que estos sistemas deben ser tratados como infraestructuras críticas. Dentro de la estructura de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), el Comité Asesor Gubernamental (GAC) recibirá actualizaciones periódicas sobre los esfuerzos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) relativos a la seguridad, estabilidad y flexibilidad, y brindará aportes a estos programas como parte del proceso de planificación estratégica. A nivel de organizaciones intergubernamentales, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) seguirá activa en la definición de su papel en debates mundiales respecto a la seguridad y las implicaciones para la gestión de la seguridad y flexibilidad en relación a los sistemas de identificación única. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) trabajará con las Naciones Unidas (UN) y con organizaciones internacionales, intergubernamentales y regionales orientando sus esfuerzos a posibilitar actividades regionales diseñadas para mejorar la seguridad y flexibilidad del Sistema de Nombres de Dominio (DNS). Estas actividades se basarán en los memorandos de entendimiento que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) tiene con una serie de dichas organizaciones. Por ejemplo, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará participando en los foros relacionados a la seguridad informática, tal como los actuales esfuerzos de la Organización para la Cooperación y el Desarrollo Económicos (OECD) para combatir el software malicioso. La Corporación para la Asignación de Números y Nombres en

Internet (ICANN) también seguirá participando en el esfuerzo de los asociados de la Corporación Económica de Asia-Pacífico (APEC) y otras organizaciones dentro de este ámbito.

El Comité Asesor Gubernamental (GAC) también proporciona orientación a la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en forma de Comunicados, en las reuniones públicas internacionales que celebra dicha Corporación.

5.4 Compromiso con los Registros Regionales de Internet

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) se compromete con la Organización de Apoyo para Direcciones (ASO) al interactuar con la Organización de Recursos Numéricos (NRO). A través de esta interacción la Corporación para la Asignación de Números y Nombres en Internet (ICANN) trabaja con los Registros Regionales de Internet (RIRs), permitiéndoles a ambos mantener y mejorar la seguridad, estabilidad y flexibilidad de la Internet para el beneficio de los usuarios locales e internacionales. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) participa en una serie de actividades con estas organizaciones relacionadas con la seguridad en Internet, estabilidad y flexibilidad. Específicamente, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha estado trabajando con estas organizaciones para firmar las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) en subdominios dentro de .arpa, incluyendo Ip6.arpa e in-addr.arpa. Los Registros Regionales de Internet (RIRs) están desarrollando los medios para permitir la certificación de las direcciones IP y Números de Sistema Autónomo (ASNs) mediante el esfuerzo de Recursos de Infraestructura de Clave Pública (RPKI). Los Registros Regionales de Internet (RIRs) también son responsables de las asignaciones de Números de Sistema Autónomo (ASNs) y la Corporación para la Asignación de Números y Nombres en Internet (ICANN) debe tratar de colaborar con ellos en cuanto a la integridad de esas asignaciones. En el corto plazo, este esfuerzo otorgará una correlación validada entre el titular del recurso numérico y el recurso numérico en sí. Este sistema de certificación jerárquico puede servir como base para el desarrollo de un medio que valide las rutas del Protocolo de Pasarela Frontera (BGP). La Corporación para la Asignación de Números y Nombres en Internet (ICANN) continuará intentando asociarse en estos esfuerzos.

5.5 Seguridad Corporativa de ICANN y Continuidad de Operaciones

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) garantiza que sus propias operaciones sean seguras, estables y flexibles, mediante la conducción de la Autoridad de Números Asignados en Internet (IANA) y otras funciones esenciales que desempeña, como parte del Sistema de Nombres de Dominio (DNS) y sistemas de direccionamiento, así como también garantiza el cumplimiento de sus responsabilidades corporativas y como contribuyente de la comunidad para la seguridad, estabilidad y flexibilidad generales de los sistemas de identificación única de Internet. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) tendrá la capacidad para responder con eficacia y trabajar con las autoridades correspondientes si sus propios activos fuesen sujetos a alguna actividad maliciosa.

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) está dedicada a un programa de seguridad de amplio espectro, orientado a gestionar riesgos contra sus recursos de información, de personal y activos físicos. En el otoño de 2008, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) contrató a un Director de Operaciones de Seguridad, responsable/encargado de estos programas. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) proporciona recursos de información, servicios y tecnología en apoyo a la Autoridad de Números Asignados en Internet (IANA) y a otras operaciones críticas. Los esfuerzos recientes se han enfocado en la reasignación, documentación y despliegue de procesos y políticas de seguridad más robustos.

El Plan de Seguridad de Información de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) está referenciado en las normas ISO 27002 y mejoras para procedimientos de apoyo y procedimientos que están en curso. El Plan de Seguridad de Información de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) también incluye el abastecimiento del Plan de Seguridad de Información de la Autoridad de Números Asignados en Internet (IANA) al Departamento de Comercio de los EE.UU. y la gestión de realizar auditorías externas de su programa. El Plan de Seguridad Físico y del Personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) se centra en la protección del personal de dicha Corporación y de las instalaciones necesarias para que la misma llevar a cabo el conjunto de actividades globales, incluyendo la garantía de la seguridad en las Reuniones

Internacionales de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). La Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha establecido un proceso de planificación para gestionar los riesgos de seguridad relacionados con la corporación en su totalidad y aprovecha su propio equipo de seguridad interna, así como el apoyo de consultores en seguridad.

Los programas de seguridad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) caben dentro de un programa global de gestión de riesgos corporativos supervisado por la Junta Directiva de la dicha Corporación, así como programas de continuidad de negocios corporativos de apoyo mutuo. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha madurado sus procesos de gestión de riesgos con el establecimiento de las Directrices para la Gestión de Riesgos para la organización, un Equipo de Gestión para la Supervisión de Riesgos y llevando a cabo con regularidad evaluaciones de riesgo sobre los principales riesgos organizacionales y presentación de informes sobre gestión de riesgos, en las iniciativas centrales de la Corporación para la Asignación de Números y Nombres en Internet (ICANN).

A medida que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) crece, su base de activos crece conjuntamente con la actividad mundial y el perfil público. Como parte fundamental de sus procesos corporativos, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) continúa haciendo hincapié en una sólida gestión del riesgo, la continuidad de los negocios y la seguridad.

5.6 Actividades de Organizaciones de Apoyo y Comités Asesores de ICANN

La comunidad más amplia de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) también desempeña un rol esencial en facilitar la seguridad, estabilidad y flexibilidad de los sistemas de identificación única a través de un proceso de políticas de abajo hacia arriba. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) cuenta con tres organizaciones de apoyo: la Organización de Apoyo para Nombres de Dominio (GNSO), la Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO) y la Organización Auxiliar de Direcciones (ASO), responsables por la elaboración de políticas a fin de incluir las cuestiones relacionadas con la seguridad y estabilidad. Más especificaciones respecto a cada organización de

apoyo y sus procesos, puede encontrarse en: http://gnso.icann.org, http://ccnso.icann.org/ y http://aso.icann.org/. Estas organizaciones hacen recomendaciones que deberán ser aprobadas por la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), con el fin de ser implementadas mediante una variedad de contratos, acuerdos, Memorandos de Entendimiento (MoU) y actividades del personal. Las áreas clave en el ámbito de la Organización de Apoyo para Nombres de Dominio (GNSO) incluyen las políticas relacionadas con los registros de Dominios Genéricos de Alto Nivel (gTLD) y acuerdos de registradores, para incluir la consideración de cualquier política de cambios en Whois de los Dominios Genéricos de Alto Nivel (gTLD), el estudio de cuestiones planteadas por el alojamiento fast flux, cuestiones relacionadas con el vencimiento de los nombres de dominio, transferencias entre registradores de nombres de dominio y abuso de las políticas de registración, entre otros.

Actualmente, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) está trabajando con la comunidad para revisar los Procesos de Desarrollo de Políticas (PDP) de Dominios Genéricos de Alto Nivel (gTLD) vigentes a fin de hacerlos más eficaces y sensibles a las necesidades del desarrollo de políticas de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Entre las numerosas revisiones al actual Proceso de Desarrollo de Políticas (PDP) que se prevé, están los cambios orientados a lograr una mayor experiencia técnica y de investigación; la determinación de hechos desde el principio del proceso para ayudar a definir y abordar desafíos difíciles de políticas de una manera más informada y con mejores conocimientos; y el desarrollo de mejores formas de evaluación de la eficacia de las nuevas políticas.

La Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO) facilita la colaboración de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) con los Dominios de Alto Nivel con Código de País (ccTLDs) para incluir el intercambio de información relacionado con la seguridad, estabilidad y flexibilidad.

La Organización Auxiliar de Direcciones (ASO) coordina el desarrollo de políticas relacionadas con la asignación de direcciones IP y Números de Sistema Autónomo (ASN) a los Registros Regionales de Internet (RIRs), por parte de la Autoridad de Números Asignados en Internet (IANA). Distintas comunidades de los Registros Regionales de Internet (RIRs) elaboran estas políticas a nivel mundial. La Organización Auxiliar de Direcciones (ASO) tiene la función de tomar estas políticas elaboradas

regionalmente y coordinarlas dentro de una única política global, la cual luego es transmitida a la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para ser ratificada.

En forma adicional, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) tiene cuatro comités asesores que brindan asesoría a la Junta Directiva y a la comunidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN): el Comité Asesor At-Large (ALAC), el Comité Asesor Gubernamental (GAC), el Comité Asesor en el Sistema de Servidores Raíz (RSSAC) y el Comité Asesor de Seguridad y Estabilidad (SSAC). Más especificaciones relacionadas con las funciones, procesos y actividades de estos comités, puede encontrarse en: http://www.icann.org/en/committees/. Estos comités asesores a menudo colaboran en esfuerzos a través de la estructura de organizaciones de apoyo/comités asesores, particularmente el Comité Asesor de Seguridad y Estabilidad (SSAC). Los comités reciben el apoyo del personal de políticas de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en la conducción de estudios, emprendimiento de deliberaciones y realización de recomendaciones.

El Comité Asesor de Seguridad y Estabilidad (SSAC) asesora a la comunidad y Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) sobre asuntos relativos a la seguridad y estabilidad de los sistemas de asignación de nombres y direcciones en Internet. Esto incluye asuntos relativos al funcionamiento correcto y fiable del sistema de nombres raíz, la asignación de direcciones y números en Internet y los servicios de los registros y registradores de Dominios Genéricos de Alto Nivel (gTLD), tales como Whois. El Comité Asesor de Seguridad y Estabilidad (SSAC) participa en la permanente evaluación de amenazas y análisis de riesgos de los servicios de asignación de nombres y direcciones en Internet, para determinar dónde residen las principales amenazas a la estabilidad y seguridad, de acuerdo a lo cual asesora a la comunidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Más detalles sobre las actividades del Comité Asesor de Seguridad y Estabilidad (SSAC) pueden encontrarse en: www.icann.org/en/committees/security.

Además de las mencionadas, las actividades continuas dentro de las organizaciones de apoyo y comités asesores incluyen debates conjuntos entre estos grupos en las reuniones de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), donde se debaten cuestiones de interés común en relación a la seguridad y estabilidad, la organización de talleres y sesiones

informativas sobre seguridad y cuestiones relacionadas con la estabilidad, y se realizan actividades relacionadas con la comunicación de políticas a la comunidad, a través de la Actualización Mensual de Políticas (http://www.icann.org/en/topics/policy/).

Los trabajos relevantes sobre políticas realizados por la Organización de Apoyo para Nombres Genéricos (GNSO) incluyen los siguientes:

Fast Flux: En el mes de septiembre de 2009 se finalizó un Proceso de Desarrollo de Políticas (PDP) de la Organización de Apoyo para Nombres Genéricos (GNSO) sobre Alojamiento Fast Flux. El informe del Grupo de Trabajo exploró quién se beneficia y quién se perjudica a partir del fast flux así como el modo en que los usuarios de Internet se ven afectados por el alojamiento fast flux y si los cambios técnicos y de política realizados en el Sistema de Nombres de Dominio (DNS) reducen los efectos negativos del alojamiento fast flux. El Consejo de la Organización de Apoyo para Nombres Genéricos (GNSO) adoptó una moción en septiembre de 2009 para crear un equipo de redacción para elaborar un plan de trabajo para implementar las recomendaciones propuestas por el grupo de trabajo.

Transferencias:

El Consejo de la Organización de Apoyo para Nombres Genéricos (GNSO) tiene un grupo de trabajo enfocado en el tercero de los seis esfuerzos planificados para el desarrollo de políticas para abordar los distintos aspectos de las transferencias entre registradores. Este Grupo de Trabajo, la Parte B de la Política de Transferencia entre Registradores (IRTP), está abordando cinco temas y centrándose en las cuestiones relacionadas con el secuestro de nombres de dominio, el regreso urgente de un nombre de dominio transferido de manera inapropiada y el uso de "estados de bloqueo". El día 29 de mayo, el Grupo de Trabajo de la Parte B de la Política de Transferencia entre Registradores (IRTP) publicó su informe inicial (http://www.icann.org/en/announcements/announcement-05jul10-en.htm). Entre otras cosas, el informe incluye una propuesta de una Política Rápida de Transferencia Inversa y la propuesta de solicitar un Informe de Cuestiones Relacionadas sobre la necesidad de un Whois extenso ('thick Whois') para todos los Dominios Genéricos de Alto Nivel (gTLD). Tras el cierre del período de comentarios públicos el día 8 de agosto, el Grupo de

Trabajo revisará los comentarios recibidos por parte del público y comenzará a trabajar en la finalización de su informe para que el mismo sea considerado por el Consejo de la Organización de Apoyo para Nombres Genéricos (GNSO).

Abuso de Registración:

El Grupo de Trabajo sobre Políticas de Abuso de Registración (RAP), que se puso en marcha en el mes de febrero de 2009, se encargó de examinar las políticas de abuso de registración. El Grupo de Trabajo sobre Políticas de Abuso de Registración (RAP) consideró cuestiones tales como definir la diferencia entre el abuso de registración y el uso indebido de los nombres de dominio, definiendo loa abusos existentes e identificando los posibles beneficios o desventajas de contar con un enfoque más uniforme en los contratos, y qué áreas —si las hubiese— serían adecuados para el desarrollo de políticas de la Organización de Apoyo para Nombres Genéricos (GNSO) a fin de hacer frente a los abusos. El Grupo de Trabajo sobre Políticas de Abuso de Registración (RAP) emitió su informe final al Consejo de la Organización de Apoyo para Nombres Genéricos (GNSO), el 29 de mayo de 2010 [http://www.icann.org/en/announcements/announcement-29may10-en.htm]. El informe incluye recomendaciones concretas para hacer frente al abuso de registración de nombres de dominio en los Dominios Genéricos de Alto Nivel (gTLD). Se incluyen recomendaciones relativas a:

- *Ciberocupación: recomendando el inicio de un Proceso de Desarrollo de Políticas para investigar el estado actual de la Política Uniforme de Disputa y Resolución de Conflictos de Nombres de Dominio (UDRP).*
- *Problemas para acceder a WHOIS: buscando maneras de garantizar que los datos de WHOIS estén accesibles de un modo confiable, ejecutable y coherente; y solicitando que el Departamento de Cumplimiento de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) publique información acerca de la accesibilidad de WHOIS.*
- *Uso Malicioso de nombres de dominio: recomendando la creación de prácticas recomendadas p ara ayudar a los registradores y registros a abordar el uso ilícito de los nombres de dominio.*

- *Notificaciones falsas de renovación: recomendando posibles acciones de aplicación por parte del área de Cumplimiento de la Corporación para la Asignación de Números y Nombres en Internet (ICANN).*

- *Estafas de registración entre Dominios de Alto Nivel (TLD): recomendando que la supervisión/monitoreo e investigación sean coordinadas con la comunidad.*

- *Uniformidad de contratos: recomendando la creación de un Informe de Cuestiones Relacionadas para evaluar si una base mínima de disposiciones de abuso de registración debe ser creada en todos los acuerdos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) de alcance correspondiente.*

- *Prácticas en toda la Organización de Apoyo para Nombres Genéricos (GNSO) para la asignación y diseminación de prácticas recomendadas y para la uniformidad en la presentación de informes.*

- *Front running*

- *Domain kiting (registración sucesiva de dominios durante un período de prueba o período de gracia)*

- *Nombres de dominio engañosos u ofensivos*

Al considerar las recomendaciones, el Consejo de la Organización de Apoyo para Nombres Genéricos (GNSO) decidió conformar un grupo de voluntarios para redactar un enfoque propuesto para las recomendaciones contenidas en el informe, el cual podría incluir el calendario para la formación de grupos a fin de considerar algunas de las recomendaciones en el informe final, así como la manera de hacer frente a aquellas recomendaciones que no lograron el consenso unánime.

Recuperación de nombres de dominio en forma posterior a su vencimiento: En el mes de mayo de 2009 el Consejo de la Organización de Apoyo para Nombres Genéricos (GNSO) inició un Proceso de Desarrollo de Políticas (PDP) sobre la Recuperación de Nombres de Dominio Post Vencimiento. Este Grupo de Trabajo está abordando cuestionamientos relacionados con la medida en la cual los registrantes deberían poder reclamar sus nombres de dominio después de vencidos. Lo que está bajo cuestionamiento es si las políticas actuales de los registradores respecto a las renovaciones, transferencias y eliminación de los nombres de dominio vencidos son adecuadas.

Mejoras al Acuerdo de Acreditación de Registradores (RAA): En el mes de mayo de 2009 la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) aprobó un Acuerdo de Acreditación de Registradores (RAA) revisado (http://www.icann.org/en/topics/raa/). El nuevo Acuerdo de Acreditación de Registradores (RAA) incluye un aumento de la debida diligencia en los registradores y sus afiliados, la identificación de registradores que pudiesen estar implicados en la ciberocupación y otras conductas maliciosas, mayores requisitos y obligaciones de WHOIS para los proveedores de servicios de privacidad/proxy y requisitos para identificar puntos de contacto dedicados a abusos a fin de informar casos de conducta maliciosa que involucren al Sistema de Nombres de Dominio (DNS). *Representantes del orden public, el Comité Asesor At-Large (ALAC) y otros grupos de partes interesadas están participando en la búsqueda de mayores mejoras al Acuerdo de Acreditación de Registradores (RAA) (véase http://www.icann.org/en/announcements/announcement-28may10-en.htm), y en la reunión que la Organización de Apoyo para Nombres de Dominio (ICANN) celebró en Bruselas en el mes de junio de 2010, presentaron las modificaciones sugeridas.*

Datos de Registración Internacionalizados: Currently, no standards or guidelines define how internationalized domain registration data should be composed and displayed. A joint SSAC-GNSO Working Group was convened by the ICANN Board to study the feasibility and suitability of introducing display specifications to deal with the internationalization of registration data. The group will be soliciting input from interested constituencies including ccTLD operators, the CCNSO, the ASO, ALAC, and the GAC during its discussions to ensure broad community input. The initial set of goals of the IRD-WG are to gain an understanding of, and achieve consensus on, the types, kinds, and encodings of registration data that contracted parties would collect, display and maintain. En la actualidad, no existen normas o directrices definen cómo los datos de registro de dominio internacionalizados debe estar compuesto y se muestra. Una misión conjunta del SSAC-GNSO Grupo de Trabajo fue convocada por la Junta de la ICANN para estudiar la viabilidad y conveniencia de introducir las especificaciones de la pantalla para hacer frente a la internacionalización de los datos de registro. El grupo se solicita el aporte de grupos interesados, entre ellos los operadores de ccTLD, la CCNSO, la ASO, ALAC y el GAC durante sus deliberaciones para asegurar la participación amplia de la comunidad. El conjunto inicial de objetivos de la IRD-GT son para obtener un entendimiento de, y lograr un consenso sobre los

tipos, clases y tipos de codificación de los datos de registro que contrajo partes recoger, mostrar y mantener.

6. ICANN FY11 Plans to Enhance Security, Stability and Resiliency

Strategic and operational planning processes guide ICANN activities relating to enhancing security, stability and resiliency, and the resources allocated to these efforts. In FY 11, ICANN activities will include a number of key initiatives, such as:

- ***IANA Operations*** – Advocate, educate and complete DNSSEC implementation at the root level as called for in the ICANN 2010-2013 Strategic Plan as well as improving root zone management through automation; improved authentication of communications with TLD managers.
- ***DNS Root Server Operations –*** Continuing to seek mutual recognition of roles and responsibilities and initiate a voluntary effort to conduct contingency planning and exercises.
- ***gTLD Registries –*** Ensure applicant evaluation of new gTLD and IDN applicants continues to provide for secure operations. ICANN will mature the gTLD registry continuity plan and test the data escrow system.
- ***ccTLD Registries –*** ICANN will enhance its collaboration on maturing the DNS Capacity Building program, including the joint Attack and Contingency Response Planning (ACRP) and Registry Operations Curriculum program that has been established in conjunction with the ccNSO and the regional TLD associations.
- ***Contractual Compliance –*** ICANN will continue to enhance the scope of contractual enforcement activities involving gTLDs to include initiating audits of contracted parties as part of implementing the 2009 RAA and identify potential involvement of contracted parties in malicious activity for compliance action.
- ***Response to Malicious Abuse of Domain Name System –*** ICANN will build on its collaborative efforts related to malicious conduct enabled by the use of the DNS and facilitate information sharing to enable effective response.
- ***Internal ICANN Security and Continuity Operations*** – ICANN will ensure its security programs are conducted within overall corporate risk management, crisis management, and business continuity programs. A major focus will be the implementation of documented plans and supporting procedures.
- ***Ensure Global Engagement and Cooperation*** – ICANN will enhance partnerships to include the Internet Engineering

Task Force (IETF), Internet Society (ISOC), regional internet registries and network operators groups, the DNS–Operations, Analysis and Response Center (DNS–OARC) and the Forum for Incident Response Team (FIRST). ICANN will also engage in global dialogues to foster understanding of the security, stability, and resiliency challenges that face the Internet ecosystem and how to engage these challenges with multi-stakeholder approaches.

The full range of activities is explained further below. Appendix A provides details on specific objectives, partners, deliverables, and resource commitments planned during FY 11.

6.1 Core DNS/Addressing Functions

6.1.1 IANA Operations

ICANN will continue conducting IANA functions and working to improve the operational excellence of these operations in collaboration with the US Department of Commerce, VeriSign, the RIRs and TLD operators.

Specific IANA functions improvement initiatives include:

- Improving root zone management through automation (eIANA/RZM software); improved authentication of communications with TLD managers; and reviews of processes and practices for security and optimization considerations.
- Supporting the development and implementation of certified IP address allocations and assignments through RPKI or other mechanisms adopted by the RIRs and the Internet routing community to include continued support of the IETF Secure Inter-Domain (SIDR) working group.
- Working with the technical and operational communities to identify, analyze, and potentially implement additional technical requirements or standards to improve DNS security, stability and resiliency.

As part of overall resiliency improvements, ICANN conducted an IANA Continuity Exercise in January 2010, testing the failover of IANA services from Marina del Rey, California to Reston, Virginia. The test exercise demonstrated IANA failover capabilities and communications mechanisms to ensure the availability of IANA services. ICANN will enhance resiliency of IANA services in 2010-2011.

6.1.2 DNS Operations

ICANN, the US Department of Commerce and VeriSign achieved a significant milestone in 2010 with the implementation of DNSSEC in the root zone. Per the priority laid out in the 2010–2013 strategic plan, ICANN will continue efforts to support the introduction of DNSSEC by TLD operators and others in FY 11.

ICANN will also pursue a range of activities to enable broader DNSSEC implementation throughout the DNS globally, collaborating with DNS experts and experienced operators. ICANN will ensure that its programs including inter-registrar transfers and escrow account for such implementations and continue stakeholder discussions on implementations. ICANN will continue maintaining the IANA Trust Anchor Repository for Top Level Domains (ITAR) until the root zone is signed. ICANN will continue to seek authorization to sign the .int and .arpa zones. ICANN will support the implementation of DNSSEC by signing ICANN managed zones (including icann.org and iana.org), and facilitating lessons learned effort among those involved in DNSSEC implementation.

ICANN seeks to enable the establishment of more robust mechanisms for coordination as part of the root operator community regarding measures that would contribute to security, stability and resiliency. ICANN, in its role as L-operator, plans to collaborate with other root operators in initiating a voluntary effort to conduct planning and exercises to improve the resiliency of the root server systems against a range of stressing contingencies.

ICANN plans to continue enhancements to the operation of L-root. Additionally, ICANN has contracted the DNS-OARC to study the impact of changes including the implementation of new gTLDs and IDNs, implementing IPv6, and possible implementation of DNSSEC signing of the root zone on the operation of a single root-server operation based on the L-root model. More broadly, the RSSAC and SSAC are conducting a joint study of root server security and stability in light of projected changes detailed in Section 6.6.

6.2 Relationships with TLD Registries and Registrars

6.2.1 gTLD Registries

ICANN will continue contractual coordination related to gTLD operations to include vetting applications for new services via RSEP. Once the new gTLD process is operational, ICANN expects reviews to include proposals that require activation of the RSTEP to evaluate security, stability and resiliency concerns. ICANN will continue its efforts to encourage community collaboration and use of best practices related to security, stability and resiliency through the conduct of ICANN regional registry/registrar workshops, participation in a range of community forums, and sharing of information on its own web site. In 2010, ICANN introduced enhanced reporting of data on gTLD registries on its Dashboard for community use (http://www.icann.org/idashboard/public/).

6.2.2 New gTLDs

The potential implementation of processes related to establishing new gTLDs will provide the primary security, stability and resiliency focus in the upcoming year. In February 2009, the ICANN Board tasked the RSSAC and SSAC to jointly study the potential security, stability and resiliency implications for the root server system as a whole, with regard to a series of potential changes within the DNS including the implementation of new gTLDs and IDNs, along with possible implementation of DNSSEC signing of the root zone. Their reports are expected in 2010. As part of the new gTLD process, ICANN will also establish the provisions for the evaluation of applicants to ensure they can implement operations that are technically secure, are compliant with Whois provisions, can provide for sound contingency planning, and ensure the protection of registrants. ICANN will continue to mature the gTLD registry continuity plan and exercise program. ICANN will also ensure that the automated TLD Applicant System is established and operated in a secure fashion.

6.2.3 IDNs

In a similar vein, ICANN's effort to enable the implementation of IDN TLDs (ccTLDs and gTLDs) will ensure these new domain names represented by local language characters will be secure, stable, and resilient. ICANN is supporting work to update the IDN Guidelines to be followed by the operators of IDN TLDs and operation of second-level IDNs. ICANN will continue to facilitate registries' efforts in working with vendors to ensure that IDN tables are established which limit as much as possible string conflicts and confusions, and reduce opportunities for misuse of the system for malicious purposes. An IDN focused support

function will be made available for those parties interested in becoming an IDN TLD operator and in need of assistance and expertise in the field.

ICANN is also engaged with experts to ensure the stable introduction of IDN TLDs for countries and territories that have more than one appropriate language or script and need to have a synchronized implementation. This also includes collaborating with stakeholders such as browser and application developers, IDN registry operators and others to support the introduction of IDNs.

6.2.4 ccTLDs

ICANN will continue its efforts related to enhancing ccTLD security, stability and resiliency through collaboration with ccTLD operators. In the upcoming year these activities will focus on maturing DNS Capacity Building program, which includes the joint Attack and Contingency Response Planning (ACRP) workshop program that has been established in conjunction with the ccNSO and the regional TLD associations. The DNS Capacity Building program focuses on improved security and resiliency through proactive planning and strong response capabilities against a full range of disruptive threats and risks. The program will expand in the upcoming year to include technical training to improve security and resiliency in response to advancing threats and to provide assistance in the development of exercise and evaluation programs for ccTLD security and contingency planning.

6.2.5 Registrars

The community is preceding with further consideration of enhancements to registrar accreditation and data escrow requirements through improvements to the RAA. In addition to supporting these efforts, ICANN staff will continue to develop procedures and processes within the existing contractual and policy frameworks to protect registrants and ultimately enhance the security, stability, and resiliency of the DNS. In particular, work is under way to tighten accreditation application procedures, establish heightened RAA eligibility requirements and disqualification rules, and develop procedures to allow registrars to exit the registrar marketplace in a responsible manner. Previous work in developing data escrow and registrar termination procedures will also strengthen ICANN's ongoing and future compliance enforcement efforts, allowing for termination of registrar accreditation in cases where registrar actions threaten the security and stability of the DNS. ICANN will continue to build a strong registrar community through outreach events that permit sharing of industry best practices, and will begin implementing

new channels of communication to assist registrars in timely reporting and responding to critical security threats.

6.2.6 Contractual Compliance

ICANN will continue to increase the scope of contractual enforcement activities. Activity will include audits of contracted parties as part of implementing the 2009 RAA. Additionally, Contractual Compliance staff will work collaboratively with ICANN's Security team to identify contracted parties who may be engaged in malicious activity. In those cases where contracted parties have engaged in malicious activity, contract enforcement action may be taken. In all other cases, law enforcement or other appropriate agencies will be notified for proper handling of such matters.

The Contractual Compliance Department has conducted to assess Whois data contact information accuracy within the gTLD system and to assess the extent to which registrants are using privacy and proxy services to shield their identity. In an effort to encourage contract compliance and to provide public confidence, the Contractual Compliance Department is developing a system to publically identify compliant parties. This system is in the early stages of development, and consultation with the registrar and registry communities will be sought before it is implemented.

6.2.7 Collaborative Response to Malicious Abuse of Domain Name System

ICANN staff will also continue to build on collaborative efforts that have emerged in response to recent events involving the Domain Name System since late 2008 such as activities surrounding the Szirbi botnet and Conficker worm in late 2008/early 2009. ICANN envisions such collaboration to involve DNS registries and registrars, the security research community and software and anti-virus vendors. Specifically, ICANN plans to work with registry and registrar communities to enhance collaborative approaches to combat the spread of malware, worms and botnets that use the DNS for propagation and control. ICANN will seek to delineate procedures for communication and validation of registry and registrar activities as well as how it will participate in information sharing with security researchers, technology vendors and law enforcement as appropriate. ICANN will provide for public comment on its procedures for conducting collaborative response activities. These procedures will be submitted to the Board for approval. These approaches will ensure ICANN can be responsive to the full range of global stakeholders that may seek its engagement and collaboration.

6.2.8 Enabling Overall DNS Security

ICANN staff will seek to build on the February 2009 and February 2010 DNS Security, Stability, and Resiliency Symposiums by assisting key collaborative efforts related to mitigating operational risks to the operators and users of the DNS. Plans include convening an annual symposium to review DNS-wide risks and enhancing collaborative opportunities with an ongoing focus of meeting the challenges of ensuring DNS security and stability in the developing world. ICANN also plans to collaborate with DNS-OARC and the Forum of Incident Response and Security Teams (FIRST) with a focus of how to orchestrate effective responses to significant contingencies and events within the DNS community. Additionally, ICANN staff will continue to track the evolution of plans for establishing an Object Naming System (ONS) and how such plans might involve the DNS to ensure that identification of potential issues related to security, stability and resiliency are identified early.

6.3 Global Security Outreach

6.3.1 Extend Existing Partnerships

The core of ICANN's global engagement strategy in relation to security, stability and resiliency is to build upon and use the existing work conducted by Global Partnerships and to further extend strong partnerships. Specific activities planned for FY 11 with these partners include:

- ***Internet Society (ISOC)*** – ICANN plans to collaborate in maturing the ongoing joint ISOC/ICANN program to provide training to TLD operators with additional plans to include technical training in how to improve security and mitigate cyber attacks and disruptions.
- ***DNS-OARC*** – ICANN will continue collaboration with DNS-OARC and other interested stakeholders in support of the SSR Strategic Initiatives and DNS-CERT concept. ICANN has also engaged with organizations in order to conduct education and training in partnership with others to improve understanding of the functioning of the unique identifier systems, ICANN's role, and challenges to managing risks to these systems.

6.3.2 Commercial Enterprise

ICANN will build on the February 2009 and 2010 DNS Security, Stability, and Resiliency Symposium on understanding enterprise reliance on, and risks associated with the DNS. In the upcoming

year, efforts in security, stability and resiliency will be incorporated as part of the ICANN CEO outreach program in seeking to ensure incorporation of a broad range of corporate perspectives.

6.3.3 Participation in Global Cyber Security Dialogue

ICANN will engage these dialogues seeking to ensure a clear understanding of its specific role and contributions. Specific activities envisaged by ICANN in this area during the next year include:

- ***Forum of Incident Response and Security Teams (FIRST)*** – ICANN and FIRST conducted a joint cyber security workshop in Nairobi, Kenya in March 2010 for African incident response teams. ICANN is collaborating with FIRST on a survey of Computer Emergency Response Teams in FY 11, and participating in FIRST programs.
- ***European Network and Information Security Agency (ENISA)*** – ICANN plans to collaborate with ENISA in a European cyber exercise and on cyber incident response activities.
- ***Internet Governance Forum (IGF)*** – ICANN will participate at the IGF meeting in Vilnius, Lithuania in September 2010 and supports the continuation of the IGF by the United Nations General Assembly.

ICANN will actively pursue opportunities with other entities and academic institutions on leadership in identifying challenges regarding security, stability and resiliency.

ICANN plans to continue collaboration with the ASO (and through the ASO, the NRO and RIRs) and to participate in activities of mutual concern related to security, stability and resiliency. ICANN staff will seek to engage the NRO on which collaborative activities to enhance to ensure the security, stability and resiliency of the DNS. These discussions will include understanding NRO's intent regarding the possible misuse of legacy IPv4 address space and the potential need for regional or possibly global policy to address identified concerns.

6.4 ICANN Corporate Security and Continuity Operations

ICANN staff will ensure its security programs are conducted within overall corporate risk management, crisis management and business continuity programs. A major focus continues to be the establishment of a sound foundation of documented policies,

processes and supporting procedures. Recent initiatives have focused on improvements to ICANN enterprise level risk management and continuity posture, including creation of formal ICANN business continuity/crisis management plans and conducting ICANN internal exercises in conjunction with other activities to include gTLD continuity exercises and meeting preparations. ICANN has initiated use of physically distributed alternative operations sites to enhance business continuity and disaster recovery capability for ICANN's IT infrastructure.

As part of ongoing operations in 2010, ICANN staff continues to improve the full spectrum of corporate information, personnel, and security processes. As with risk management and continuity planning, a major focus will be the establishment of a sound foundation of documented plans and supporting procedures. Specific initiatives underway in 2010 to improve ICANN's security posture include improvements to logical and physical access controls, change management, logging/auditing and data backup procedures, security awareness training for staff, building incident response capabilities and improvements to mobile device security. Documented security plans for personnel and ICANN Global Meetings have been prepared and outside validation and review of those plans is scheduled for late 2010. ICANN will ensure that evolving community collaboration and outreach IT tools are developed and deployed with proper security controls in place.

ICANN plans to have an outside review and audit of its security and continuity programs conducted during the second half of 2010.

6.5 ICANN Support Organizations and Advisory Committees

SSAC plans to focus its upcoming efforts on DNSSEC deployment, protection of domain registration, and reduction in misuse of domain names and address system stability.

In January 2009, the GNSO Council issued an Initial Report on fast flux hosting for public comment and further council action and is also considering numerous possible studies of related Whois. The GNSO Council has a working group focusing on the second of six planned policy development efforts addressing various aspects of inter-registrar transfers. The GNSO has convened a Registration Abuse Working Group and is considering an initiative related to post-expiration domain name recovery. To bring the wide range of ICANN stakeholders with interests in these topics together, several ICANN international public meetings have included an

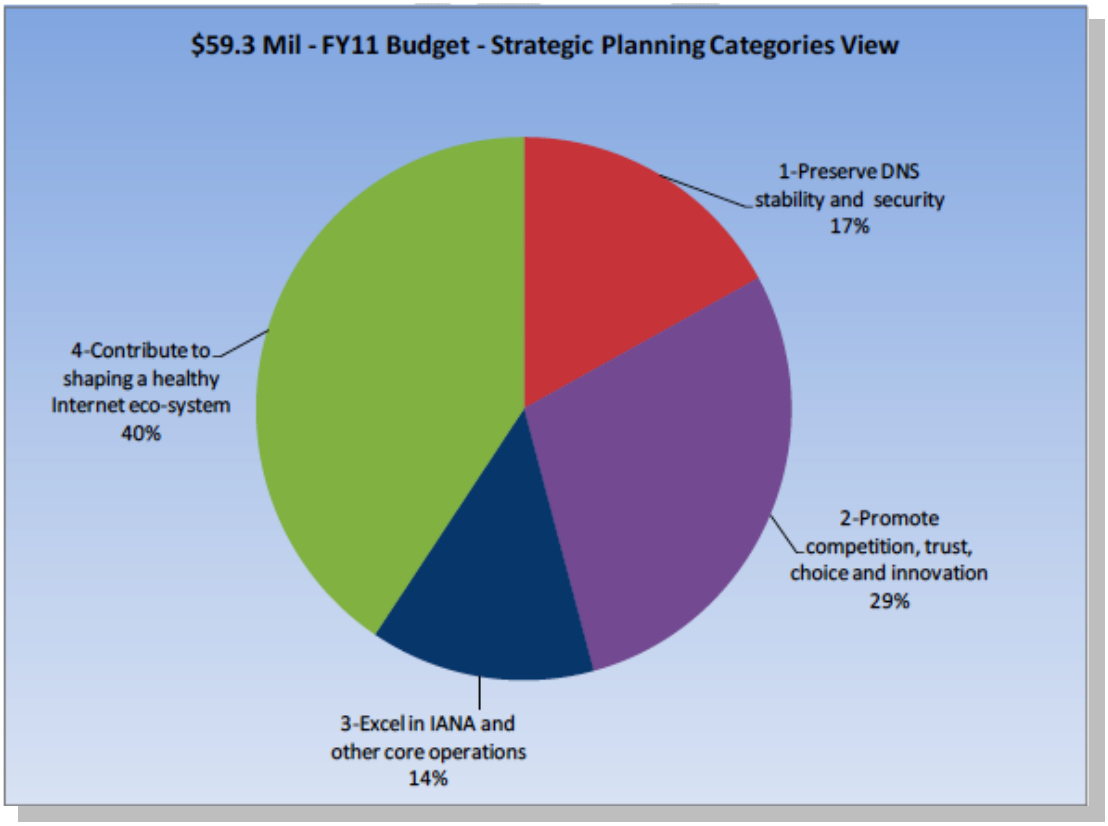
extended workshop on e-crime and registration abuse (in Mexico City, Seoul, Nairobi, Brussels).

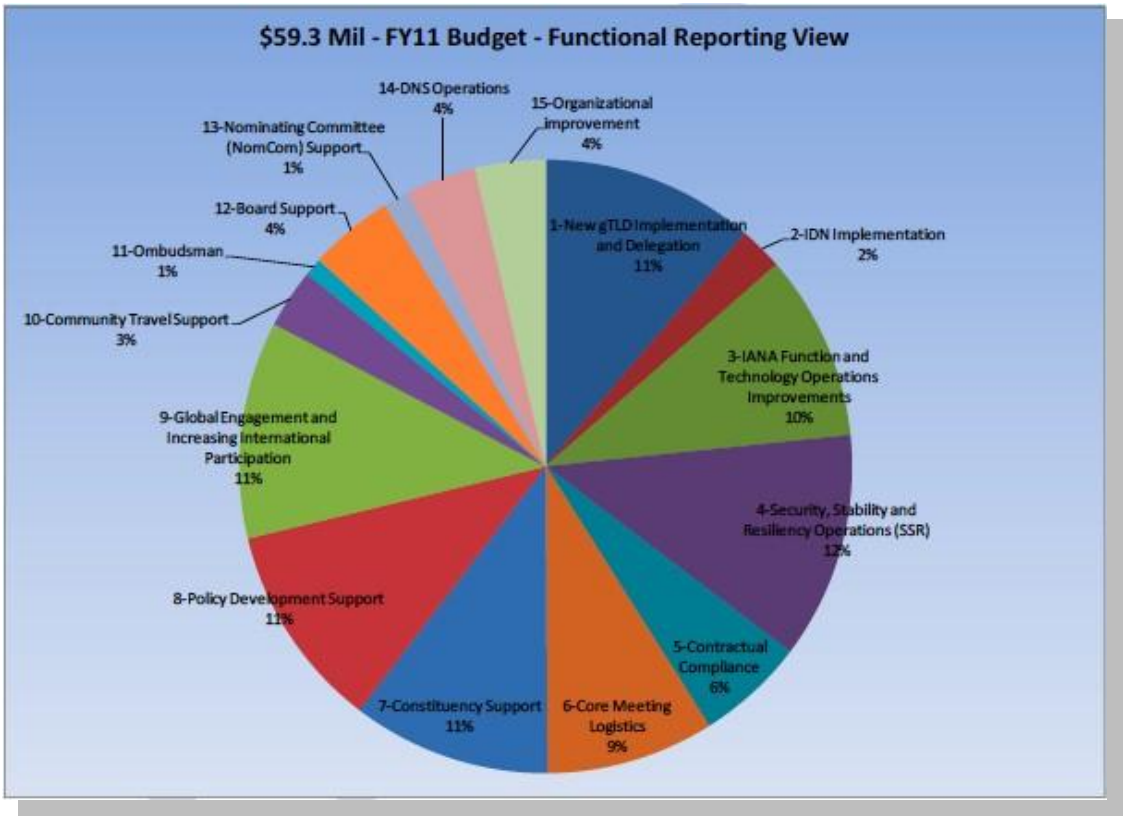
7. Conclusion

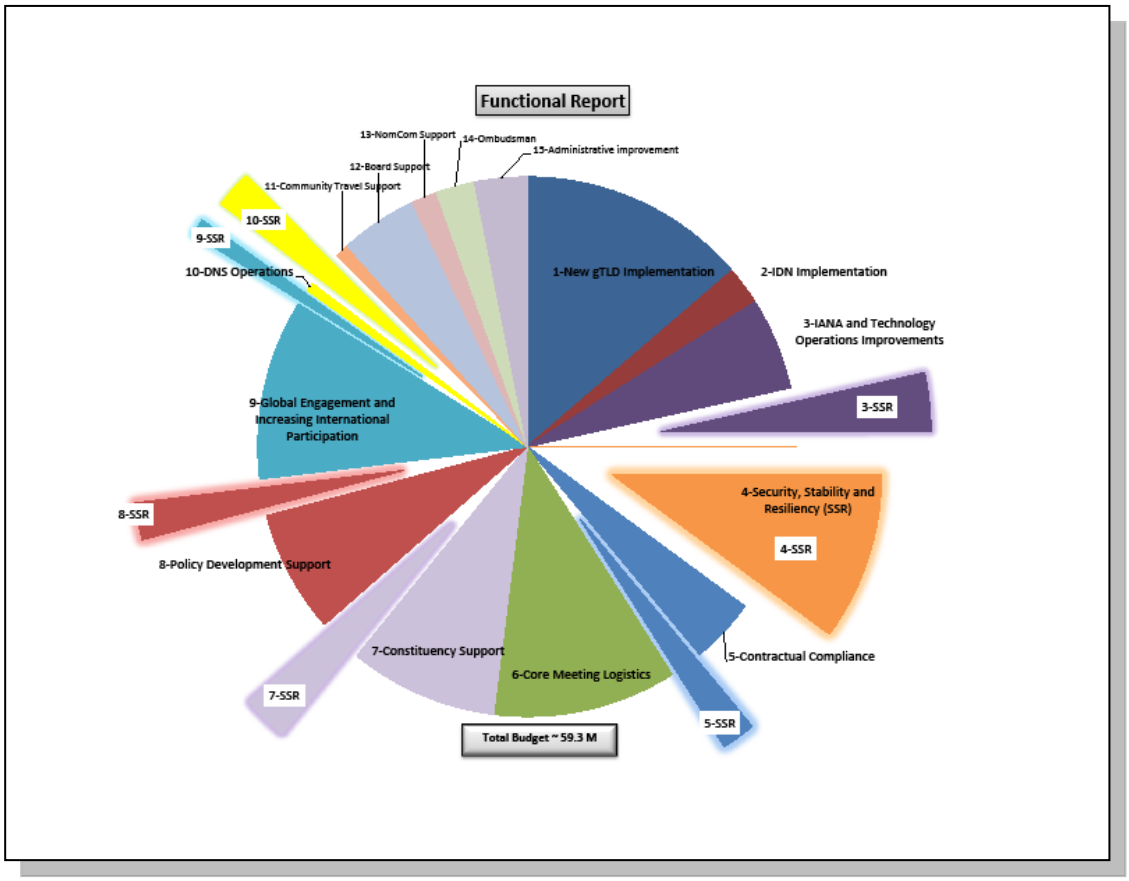
ICANN understands that, as a crucial aspect of its mission of public trust, its programs and activities must contribute to making the unique identifier systems a core aspect of a more secure, stable and resilient Internet environment. Challenges are growing and ICANN's efforts in this area are becoming more vigorous. ICANN also recognizes the limits to its role and resources, and plans its strategy in this area to rely heavily on collaboration. The Internet has thrived as a global environment, fostering innovation, and relying on multi-stakeholder coordination. ICANN's contribution to improving security, stability and resiliency of its unique identifier systems will rely on the same approach.

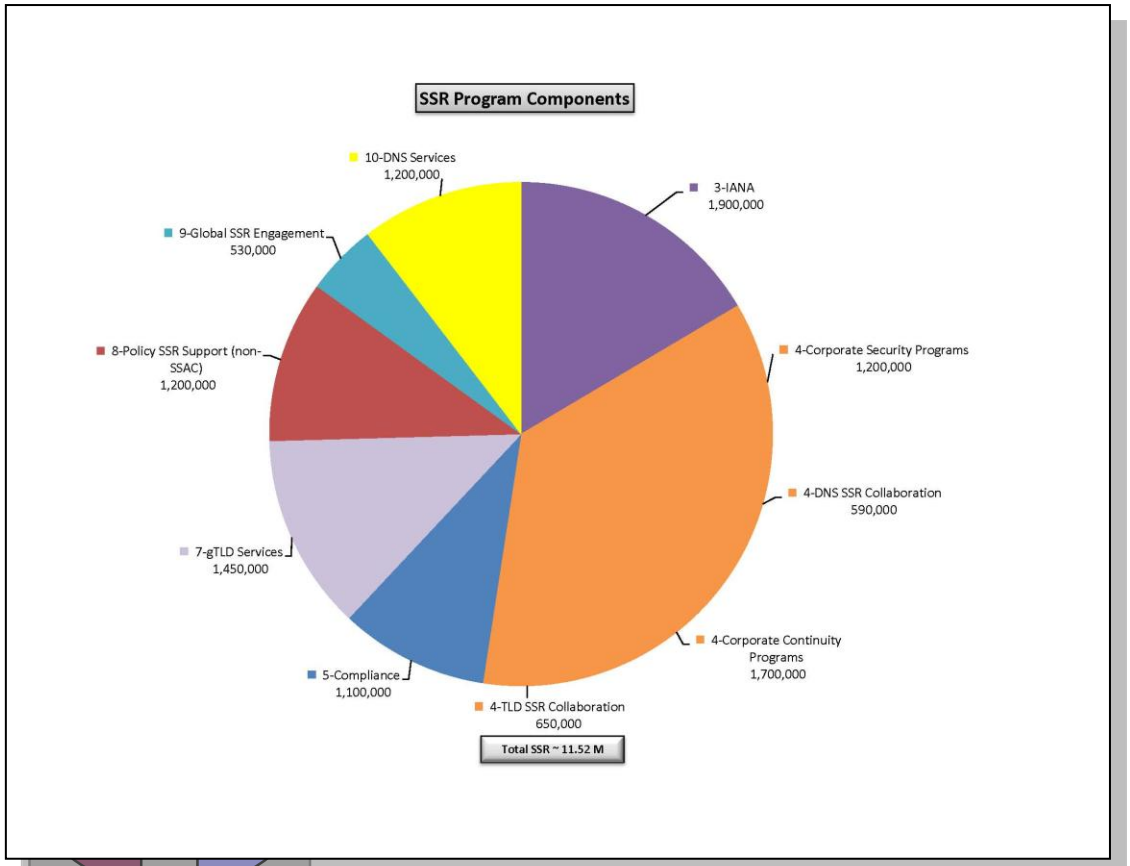
Since its inception ICANN has conducted programs and activities to improve the security, stability and resiliency of the Internet that include efforts related to core DNS/addressing functions; working with the TLD registry and the registrar communities; engagement with the NRO and RIRs; corporate security and continuity programs; activities of the supporting organizations and advisory committees, and participation in global and regional Internet security, security and stability activities. The intent of this first version of the plan is to provide a foundation on which to develop ICANN's role and the framework around which ICANN organizes its security, stability and security efforts. The plan will evolve over time as part of the ICANN strategic and operational planning process allowing ICANN efforts to remain relevant and to ensure its resources are focused on its most important responsibilities and contributions.

Appendix A–FY 11 SSR Resourcing




$59.3 Mil - FY11 Budget - Functional Reporting View
14-DNS Operations 4%
15-Organizational improvement 4%
13-Nominating Committee (NomCom) Support 1%
12-Board Support 4%
11-Ombudsman 1%
10-Community Travel Support 3%
1-New gTLD Implementation and Delegation 11%
2-IDN Implementation 2%
3-IANA Function and Technology Operations Improvements 10%
4-Security, Stability and Resiliency Operations (SSR) 12%
5-Contractual Compliance 6%
6-Core Meeting Logistics 9%
7-Constituency Support 11%
8-Policy Development Support 11%
9-Global Engagement and Increasing International Participation 11%


Functional Report
13-NomCom Support
14-Ombudsman
15-Administrative improvement
12-Board Support
11-Community Travel Support
10-SSR
9-SSR
10-DNS Operations
1-New gTLD Implementation
2-IDN Implementation
3-IANA and Technology Operations Improvements
3-SSR
9-Global Engagement and Increasing International Participation
4-Security, Stability and Resiliency (SSR)
4-SSR
8-SSR
8-Policy Development Support
7-Constituency Support
6-Core Meeting Logistics
5-Contractual Compliance
7-SSR
5-SSR
Total Budget ~ 59.3 M


SSR Program Components
10-DNS Services
1,200,000
3-IANA
1,900,000
9-Global SSR Engagement
530,000
8-Policy SSR Support (non-SSAC)
1,200,000
4-Corporate Security Programs
1,200,000
4-DNS SSR Collaboration
590,000
7-gTLD Services
1,450,000
4-Corporate Continuity Programs
1,700,000
5-Compliance
1,100,000
4-TLD SSR Collaboration
650,000
Total SSR ~ 11.52 M

Overview of Major Components of ICANN Security, Stability, Resiliency (SSR) Program

- IANA - $1.9 M
- DNS Services - $1.2 M
- DNS SSR Collaboration - $590 K
- gTLD Services - $1.45 M
- Compliance - $1.1 M
- TLD SSR Collaboration - $650K
- Global SSR Engagement - $530K
- Corporate Security Programs - $1.2 M
- Corporate Continuity Programs - $ 1.7M
- Policy SSR Support (non-SSAC) - $550K
- SSAC Support – $650K

OVERALL SSR - $11.52M

IANA Security, Stability and Resiliency (IANA)

Objectives	Deliverables (milestones)
- Automation of key elements in root zone change process - DNSSEC management - Test rPKI implementation - Business continuity	- Implementation of automated RZM (dependent on partners NTIA & VeriSign) - Implement DNSSEC signing of .ARPA (date depends on coordination with IAB & NTIA) - Coordination with rPKI testers - IANA Continuity Plan (exercised in Jan 2010, on-going exercise of plan in FY 11)
Key Stakeholders	**Resources**
- IANA, Security, IT - DOC/USG; Verisign - SSAC; RSSAC - IETF; DNS operator community - RIRs; routing operational community	- Staffing – 6.5 FTE (including 2.5 FTE for related IT and other staff support) - Financial – $1.9 M to support FTEs; staff support/travel; professional services; application development

ICANN DNS Operations

Objectives	Deliverables (milestones)
- DNSSEC activities and periodic key rollover - Implement ICANN signing .arpa and zones - Trust Anchor Repository (TAR) - Secure, resilient L-root operation	- Key rollover in FY 11, at Culpeper and LAX facilities - DNSSEC signed ICANN zones - Trusted repository in operation - L-root improvement
Key Stakeholders - ICANN DNS Ops, IT Teams - ICANN IANA staff, DoC, VeriSign - ICANN Security Team	**Resources (FY 11)** Human – 7.0 FTE (including related IT and other staff support) Financial – $1.2M to support FTEs; planned capital investments for back-up services; DNSSec, L-root, improvements; backup facilities; professional services and travel

ICANN gTLD Registry/Registrar Services (Services)

Objectives	Deliverables

- Ensure implementation new gTLD/IDNs addresses SSR issues
- Continue maturing data escrow process & gTLD continuity plan
- Conduct RSEP/RSTEP processes
	- Enhanced gTLD implementation process from SSR perspective
	  - Root Scaling complete (in FY 11)
	  - Improved Applicant Guidebook (Nov 10)
	- Data escrow exercises (Aug-Nov 10)
	- HSTLD RFI (Sept-Nov 10)
	- Malicious Conduct provisions

Key Stakeholders - Registries/Registrars - ICANN Services staff - ICANN Security & Continuity staff - GNSO/SSAC	**Resources (FY 11)** Human – 2.75 FTE Financial – TBD new gTLD budget - includes portion of evaluation staff/support for new gTLD/IDN activities to include TAS security; dedicated RSEP/RSTEP funds; support for testing/contingency exercise; staff travel/support

Contractual Compliance (Services)

Objectives	Deliverables
- Improved ICANN compliance process - Improved compliant and WDPRS system - Improved WHOIS data accuracy	- Conduct audits as part of 2009 RAA implementation - Improvements to WDPRS (Aug-Nov 10) - Additional WHOIS studies dependent on GNSO Council recommendation
Key Stakeholders - gTLD registry/registrars - ICANN Compliance staff - ICANN Security/Continuity staff	**Resources (FY 11)** Human – 3 FTE Financial – $1.1M support for FTEs, staff/travel support; professional services to conduct studies and support systems improvements;

TLD Security, Stability & Resiliency Collaboration
(Security)

Objectives	Deliverables (milestones)
- Mature DNS Capacity Building Program - Establish joint ISOC/ICANN tech training program - Conduct TLD exercise planning workshops - Establish program metrics	- Conduct ACRP training sessions remaining in 2010 - Joint technical training with ISOC plan, transition in 2010 - Conduct exercise planning workshops - Prototype metrics from DNS Symposium
Key Stakeholders - ccTLD operators - ccNSO, regional TLD operators - ISOC/NSRC - ICANN staff	**Resources (FY 11)** Human – 1 FTE Financial – $650K for FTE, staff/travel to support; professional services for developing and conducting training programs

DNS Security, Stability & Resiliency Collaboration

(Security)

Objectives	Deliverables (milestones)
- Establish collaborative response mechanisms to DNS abuse - Share key SSR practices - Conduct community-based DNS risks and collaboration - Enhance root server SSR collaboration	- Collaboration construct and on-going responses w/ partners - Conduct & report on symposium (Feb & Mar 2011) - Report on root ops exercise (TBA 2010)
Key Stakeholders - ISOC, DNS-OARC, FIRST - Root Server community - Broader DNS ops community - ICANN staff - RSSAC/SSAC	**Resources (FY 11)** Human – 1.25 FTE Financial – $590K for FTE, professional services for portal and collaboration support, travel to support activities

Corporate Security Program (Security, IT, others across staff)

Objectives	Deliverables
- Improve and implement IT/Facilities/ Personnel Security Programs - Implement Formal Plans - Institute Security Training - Implement Traveler and Meetings Security & Contingency Plans	- Conduct Security Training Programs (embedded part of ICANN on-boarding as of Sep 2009) - Improved IT & Physical Access Control Systems implemented (improved IT authentication on key systems – Fall 09) - Exercise Traveler and Meetings Security (one drill per trimester)
Key Stakeholders - ICANN Security & Resiliency Team - ICANN IT/IANA/DNS Ops - ICANN Human Resources - ICANN Global Meetings Team - Other ICANN Staff	**Resources** Human – 2 FTEs (includes IT support for security) Financial – $1.1 M including FTEs, physical & IT access controls, professional services for conducting training and audits

Corporate Continuity Program (Security, IT, others across staff)

Objectives	Deliverables

- Improve Business Continuity program
  - Establish formal plan
  - Establish secure data center
  - Establish formal drill/exercise programs
	- Internal ICANN Business Continuity plan (Oct 10)
	- Improve data center resiliency
	- Exercise Business Continuity/Crisis Management (Oct 10-Mar 11)

Key Stakeholders - ICANN Security Team - ICANN IT/IANA/DNS Ops - ICANN Human Resources - ICANN Global Meetings Team - ICANN Staff	**Resources** Human – 5 FTEs (includes planning and IT for data center) Financial – $1.7M including FTEs, capital support for data center, professional services for conducting training and audits

Global Security, Stability and Security Engagement
(Global Partnerships & Security)

Objectives	Deliverables
- Sustain partnerships with key organizations (ISOC; IISI; IMPACT; EC/ENISA; CSIS; Atlantic Council) - Continue participation in IGO sponsored cyber security dialogues OECD, IGF, others) - Collaborate with others on global cyber security response	- Conduct joint activities with partner organizations (One per trimester) - Engagement in forums across all major regions (On-going) - Membership in Forum of Incident Response and Security Teams (FIRST)
Key Stakeholders - Global/international organizations - ISOC; IETF; ITU; IGF - Cyber security forums - Governments/Commercial Stakeholders - ICANN Global Partnerships Team & Security Staff	**Resources (FY 11)** Human – 1.5 FTE Financial – $530K for FTEs; staff/travel support; support to ICANN-led or supported forums; professional services support for metrics development

Policy Support for SSR-related efforts (Policy)

Objectives	Deliverables
Set by supported SO/ACs conducting SSR activity - GNSO; ccNSO - GAC - RSSAC; ALAC	- Derive from FY 11 work plans as they are established
Key Stakeholders - Named SO/ACs - ICANN policy staff - ICANN security staff	**Resources (FY 11)** Human – 2 FTE Financial – $550K for FTEs and limited additional funding support for SSR-related activities

Security and Stability Advisory Committee (SSAC)

Objectives	Deliverables
- Foster DNSSEC Deployment - Ensure Root Zone stability with growth and complexity - Protection of domain registration - Reduction in domain name abuse - Address system stability	- Reports, Advisories, Comments - Root Scaling Studies - Domain name protection study - Registration data study: display, access, accuracy
Key Stakeholders - External Internet security community - IANA and Root Server community - GNSO and CCNSO - ALAC - ASO - ICANN staff - GAC and Board	**Resources (FY 11)** Human – 1.5 FTE Financial – $650K for FTEs and limited additional funding support for related travel and publications; support for completing root scaling studies

Appendix B – Glossary of SSR Plan Terms and Acronyms

ACRP – Attack Contingency Response Planning

Add Grace Period – a five-day option period at the beginning of the registration of an ICANN-regulated second-level domain. Registrants may opt to cancel their registration during this five day time period, when registration fees must be fully refunded by the domain name registry.

APWG – Anti Phishing Working Group

ASN – Autonomous System Numbers: within the Internet, an Autonomous System (AS) is a collection of connected IP routing prefixes that presents a common, clearly defined routing policy to the Internet. Internet Service Providers (ISPs) must have an Autonomous System Number (ASN) officially registered through IANA.

ccNSO - Country Code Names Supporting Organization of ICANN is the policy development body for a narrow range of global country code Top Level Domain issues within the ICANN structure.

ccTLD – country code Top Level Domain

CENTR – Council of European National Top Level Domain Registries is an association of Internet country code Top Level Domain Registries such as .uk in the United Kingdom and .es in Spain. Full Membership is open to organizations, corporate entities or individuals that operate a country code Top Level Domain registry.

CSIS - Center for Strategic and International Studies provides strategic insights and policy solutions to decision makers in government, international institutions, the private sector, and civil society.

FIRST – Forum of Incident Response and Security Teams

gTLD – generic Top Level Domain

IANA – Internet Assigned Numbers Authority

IDN – Internationalized Domain Name

IETF - Internet Engineering Task Force

IP – Internet Protocol specifies the format of packets and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which

establishes a virtual connection between a destination and a source. By itself IP is something like the postal system. It allows you to address a package and send it using the system, but there's no direct link between your packet and the recipient. TCP/IP creates the connection between two hosts so that they can send messages back and forth.

IPv4 - Internet Protocol version 4 is the fourth revision in the development of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet, and is still by far the most widely deployed Internet Layer protocol.

IPv6 - Internet Protocol version 6 is the next-generation Internet Layer protocol for packet-switched internetworks and the Internet. In December 1998, the Internet Engineering Task Force (IETF) designated IPv6 as the successor to version 4 by the publication of a Standards Track specification, RFC 2460.

ISOC – Internet Society

IT – Information Technology

Botnets – most commonly created by duping ordinary users into opening an attachment on their computer that appears to do nothing but actually installs hidden software to be used later for an attack. The now compromised computers, or "bots," are combined to form networks which can then be directed as desired, most often for malicious attacks.

Cache Poisoning – exploiting a flaw in the DNS software to make it accept incorrect information which then causes the server to cache the false entry thereby sending all subsequent server requests to the new, falsely verified domain.

Denial of Service attack (DoS) – malicious code which causes a flood of incoming messages, essentially forcing the targeted system to shut down, thereby denying use by legitimate users.

Distributed Denial-of-Service attack (DDoS) – a type of denial of service attack in which an attacker uses malicious code installed on multiple systems in order to attack a single target. This method has a greater effect on the target than is possible with just a single attacking machine. On the Internet, a distributed denial-of-service attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. DDoS attacks are most effective

when launched via a large number of open recursive servers: distribution increases the traffic and decreases the focus on the sources of the attack. The impact on the misused open recursive servers is generally low, but the effect on the target is high. The amplification factor is estimated at 1:73. Attacks based on this method have exceeded 7 Gigabits per second.

DNS – Domain Name System which translates domain names (alpha) into IP addresses (numeric). Because they're easier to remember domain names are alphabetic. The Internet, however, is based on numeric IP addresses (e.g. 198.123.456.0). When you use a domain name (www.examplir.gratis.com), a DNS service translates the alphabetic name into the corresponding numeric IP address.

DNSSEC – Domain Name System Security Extensions provide a way for software to validate that Domain Name System (DNS) data have not been modified during Internet transit. This is done by incorporating public-private signature key pairs into the DNS hierarchy to form a chain of trust originating at the root zone. Importantly, DNSSEC is not a form of encryption. It is backward compatible with existing DNS, leaving records as they are—unencrypted. DNSSEC ensures record integrity through the use of digital signatures that attest to their authenticity.

At the core of DNSSEC is the concept of a chain of trust. ICANN's proposal to sign the root zone file with DNSSEC (of October 2008) builds on that notion and, based on security advice, recommends that the entity responsible for making changes, additions and deletions to the root zone file and confirming those changes are valid, should generate and digitally sign the resulting root zone file update. This signed file should then be passed to another organization (presently VeriSign Corporation) for distribution. In other words, the organization responsible for the initial basis of trust—validating root zone changes with top level domain operators—should also authenticate the validity of the final product before it is distributed.

Domain Name Front Running – the questionable practice employed by some domain name registrars of using insider information to register domain names in advance with the intent to sell the name, at a premium, to registrants who would logically benefit from having the name for their own use

Domain tasting – the practice of a domain name registrant using the five-day Add Grace Period at the beginning of the registration of an ICANN-regulated second-level domain to test the marketability of a domain name. During this period a cost-benefit analysis is conducted by the registrant on the viability of deriving

income from advertisements being placed on the domain's website.

Domain tasting should not be confused with **domain kiting**, which is the process of deleting a domain name during the five-day add grace period and immediately re-registering it for another five-day period. This process is repeated any number of times with the end result of having the domain registered without ever actually paying for it.

Double flux – Of particular concern to ICANN is a variant of fast flux called double flux where the attacker not only changes addresses that point to illegal web sites, but the addresses of the DNS name servers that the attacker uses for the "user friendly" names he embeds in phish emails. In both cases, the changes occur very quickly, on the order of 3 minutes, leaving virtually no time for investigators to respond. ICANN's SSAC is working closely with the brand defenders and law enforcement as well as registries and registrars to identify countermeasures, especially ones that take DNS out of the fast flux equation.

Fast flux – an evasion technique used by phishers, identity thieves and other e-criminals to frustrate incident response team and law enforcement agency efforts to track down and take down illegal web sites. The fast flux technique closely resembles a three-card Monte shell game, where a "tosser" lays three folded playing cards on a table and a victim is lured into betting on his ability to "follow the red queen" (the British call this scam "Find the Lady"). The tosser moves all three cards at blinding speed while simultaneously distracting the victim with conversation, clever quips, and sleights of hand. Fast flux, however, is a high stakes trick, and has become a worrisome and omnipresent attack technique. In fast flux hosting, the tosser rapidly changes the addresses that point to illegal web sites.

Malware – an amalgamation of the words "malicious" and "software" often used as a catchall phrase to include computer viruses, worms, trojans , rootkits, spyware, adware, crimeware and any other unwanted software introduced to a user's computer with or without their consent. Malware is deemed to be such based on the perceived intent of the creator rather than any particular features of the software.

NOC – a Network Operations Center is a physical location from which a typically large network is managed, monitored and supervised. NOCs also provide network accessibility to users connecting to the network from outside of the physical space.

NOG – Network Operations Group

NRO – Number Resource Organization

Patches – programs designed to fix software flaws, often installed automatically to reduce need for end-user participation and increase ease of use.

Phishing – a form of Internet fraud that aims to steal valuable information such as credit cards, social security numbers, user IDs and passwords by creating a website similar to that of a legitimate organization, then directing email traffic to the fraudulent site to harvest what should be private information for financial or political gain.

RAA – Registrar Accreditation Agreements

Registry – an organization that manages the registration of top-level Internet domain names

Registrar - a company authorized to register Internet domain names

RIR – Regional Internet Registry

RPKI – Resource Public Key Infrastructure

RSEP – Registry Services Evaluation Process

RSTEP – Registry Services Technical Evaluation Panel

Spam – any unsolicited email. Usually considered a costly nuisance, spam now often contains malware. Malware is a class of malicious software—viruses, worms, trojans, and spyware—that is designed to infect computers and systems and steal critical information, delete applications, drives and files, or convert computers into an asset for an outsider or attacker.

Spoofing – an attack situation where one person or program masquerades as another by falsifying data. The falsified data is in turn trusted as valid by the individual system attempting to connect with the legitimate system or program.

TLD – Top Level domain

Trojan - a class of malicious software (malware) that appears to perform a desirable function but instead performs undisclosed malicious functions allowing unauthorized access to the host machine, giving Trojan users the ability to save their files onto the unwitting computer user's machine or even watch the user's screen and control the computer.

Virus –a program or string of code that is loaded onto a computer without the user's knowledge and runs malicious software (malware). Even a simple virus can replicate itself, making it more damaging because it will quickly use all available memory on an infected computer system.

Worm – similar to a virus by design a Worm is considered to be a variant of a virus, but is more dangerous due to its ability to transmit itself across networks. Worms spread from computer to computer, but unlike viruses, have the ability to travel without any human action intentional or unintentional. A worm takes advantage of file or information transport features on a computer system, which is what allows it to travel unaided. For example, a worm can send a copy of itself using an unknowing user's email address book. It would then replicate on the newly infected computers and propagate yet again through the newly compromised systems' email address books and continue on eventually consuming so much memory and bandwidth that it causes entire networks to come to a halt.