Marco de Seguridad, Estabilidad y Flexibilidad

La Corporación para la Asignación de Números y Nombres en Internet (ICANN) es una organización global que coordina los sistemas de identificadores únicos de Internet para el beneficio público a nivel mundial, permitiendo una Internet única e interoperable.

Marzo de 2013

Tabla de Contenidos

Listado de Gráficos

Resumen Ejecutivo

La Internet se ha desarrollado como un ecosistema en el cual participan muchas partes interesadas a través de la colaboración, en un entorno abierto y transparente. Internet alienta el intercambio del conocimiento, la creatividad y el comercio de los bienes comunes a nivel mundial. La interoperabilidad de los bienes comunes globales depende del funcionamiento y la coordinación de los sistemas de identificadores únicos de Internet y de una Internet que sea saludable, estable y flexible —con capacidad de recuperación—.[1]

Tanto la ICANN como los operadores de estos sistemas reconocen que el mantener y mejorar la seguridad, estabilidad y flexibilidad de estos sistemas constituye un elemento fundamental de su relación colaborativa.

Desde 2009, la ICANN ha publicado un Marco anual de seguridad, estabilidad y flexibilidad (SSR). El Marco está reconocido en la Afirmación de Compromisos[2], y ha sido analizado favorablemente por el Equipo revisor de la seguridad, estabilidad y flexibilidad [3] como parte del proceso de revisión establecido en la Afirmación de Compromisos.

El Marco de SSR describe el rol y alcance de la ICANN en el apoyo de una Internet global única e interoperable, así como los desafíos para los sistemas de identificadores únicos de Internet. El documento se divide en dos partes. La parte A explica el fundamento del rol de la ICANN en la seguridad, estabilidad y flexibilidad, el ecosistema de Internet y la comunidad de la ICANN. La Parte B describe los objetivos estratégicos de ICANN para las actividades de SSR y las planificadas para el año fiscal 2014 (FY14), que abarca el período entre julio 2013 y junio de 2014.

El cambio más importante entre el Marco de FY13 y de FY14 es la adopción de las recomendaciones del Equipo revisor de SSR —en octubre de 2012— y las reacciones ante los desarrollos del ecosistema de Internet desde que la versión anterior fue publicada en junio de 2012 (véase la Parte B). Las actividades proyectadas en FY14 estarán centradas en apoyar un ecosistema saludable, proporcionar las bases para una Internet más estable, fiable y resistente para la comunidad global.

El Marco FY14 está siendo publicado como un documento único, para facilitar la traducción y el intercambio en la próxima reunión de la ICANN que se celebrará en Beijing, China, del 7 al 11 de abril de 2013.

---

[1] Conforme los Estatutos de la ICANN, dicha Corporación coordina la distribución y asignación de tres conjuntos de identificadores únicos para Internet: los nombres de dominio (conformando un sistema denominado DNS); las direcciones de protocolo de Internet (IP) y los números del sistema autónomo (AS); y los números de protocolo de puertos y parámetros.

[2] Afirmación de Compromisos, firmada por el Departamento de Comercio de los Estados Unidos y la ICANN, http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm.

[3] Informe final del Equipo revisor de la seguridad, estabilidad y flexibilidad, 20 de junio de 2012, http://www.icann.org/en/about/aoc-review/ssr/final-report-20jun12-en.pdf.

Parte A – Fundamento del rol de la ICANN

Misión y Valores centrales de la ICANN

> "La misión de la Corporación de Asignación de Nombres y Números en Internet ("ICANN") 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."
>
> Estatutos de la ICANN, según enmienda del 20 de diciembre de 2012 (http://www.icann.org/en/about/governance/bylaws#I)
>
> Valor central #1 – "Preservar y mejorar la estabilidad operativa, la confiabilidad, la seguridad y la interoperabilidad global de Internet."

En la Afirmación de Compromisos, este valor central es reconocido del siguiente modo: "se requiere de la coordinación técnica de la infraestructura subyacente de Internet – el DNS – a nivel mundial para garantizar la interoperabilidad" y para "preservar la seguridad, estabilidad y flexibilidad del DNS", constituyendo un compromiso clave para el beneficio de los usuarios de Internet a nivel mundial.

Rol y alcance de la ICANN sobre SSR

En virtud del proceso de revisión establecido en la Afirmación de Compromisos, el Equipo revisor de SSR recomendó que la ICANN debe "publicar una declaración única, clara y coherente de su área de alcance de SSR y su misión técnica limitada." (Recomendación 1, 20 de junio de 2012).

En el mes de mayo de 2012 se publicó una declaración preliminar del rol y alcance de la ICANN en la seguridad, estabilidad y flexibilidad de los identificadores únicos de Internet (http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm), la cual fue revisada luego de la recepción de comentarios públicos en las reuniones que la ICANN celebró en Praga (junio de 2012) y en Toronto (octubre de 2012, http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct12-en.pdf).

La siguiente descripción del rol y alcance de la ICANN está destinada a abordar la Recomendación 1:

> Como una organización conformada por múltiples partes interesadas, la ICANN facilita la seguridad, estabilidad y flexibilidad de los sistemas de identificadores únicos de Internet a través de la coordinación y colaboración.
>
> La comunidad espera que la ICANN, como una organización a nivel mundial, realice su labor en forma abierta, responsable y transparente, en forma incluyente de la diversidad de las partes interesadas que conforman el ecosistema de Internet más amplio.

Dentro de su misión técnica, el rol de SSR de la ICANN comprende tres categorías de responsabilidades:

1. Responsabilidades operacionales de la ICANN (gestión organizacional de riesgos para el funcionamiento interno, inclusive la raíz-L, las operaciones del DNS, las operaciones de firma de clave de las DNSSEC, las funciones de la IANA —Autoridad de Números Asignados en Internet—, el funcionamiento de los nuevos TLD —dominios de nivel superior—, la gestión de la base de datos de zonas horarias);
2. La participación de la ICANN como un coordinador, colaborador y facilitador con la comunidad mundial en asuntos técnicos y de políticas relacionados a los identificadores únicos de Internet;
3. El compromiso de la ICANN con otros en el ecosistema de Internet a nivel mundial.

Gráfico 1 – Misión Técnica de la ICANN

Definiciones para este Marco

Seguridad – la capacidad de proteger y prevenir el uso indebido de los identificadores únicos de Internet.

Estabilidad – la capacidad de garantizar que el sistema funcione según lo esperado y que los usuarios de los identificadores únicos confíen en que el sistema funciona conforme lo esperado.

Flexibilidad – la capacidad del sistema de identificadores únicos para resistir/tolerar/sobrevivir eficazmente a los ataques maliciosos y demás eventos perjudiciales sin que el servicio sea perturbado o suspendido.

Nota – Estas definiciones no han sido modificadas desde la publicación del Marco de SSR para FY12, en el año 2011.

Sobre la base del trabajo realizado en el II Simposio de Seguridad del DNS (realizado en Kyoto, Japón en 2010) y en el III Simposio de Seguridad del DNS (realizado en Roma, Italia en 2011), el Marco de SSR para FY14 incluye una definición inicial de **Salud del identificador único**. Este concepto ha sido adaptado a partir de la definición de 'Salud del DNS' establecida en el informe del Simposio de Kyoto como:

> Un estado de funcionamiento general de los identificadores únicos de Internet que está dentro de los límites nominales técnicos en las dimensiones de coherencia, integridad, velocidad, disponibilidad, vulnerabilidad y flexibilidad.

Una definición a partir de la disciplina de la economía ecológica define a la salud del ecosistema como "una medida del desempeño global de un sistema complejo que se construye a partir de la conducta de sus partes."[4]

Las responsabilidades que recaen fuera del rol de la ICANN en relación a SSR, incluyen:

- La ICANN no tiene un rol en la vigilancia ni la lucha contra el comportamiento delictivo;
- La ICANN no tiene un rol en cuanto al uso de Internet para el espionaje informático o guerra informática
- La ICANN no tiene un rol en la determinación de aquello que constituye contenido ilícito en Internet.

Como organización, la ICANN no es una agencia de aplicación de la ley, un tribunal o agencia gubernamental. Las fuerzas públicas y los gobiernos participan como partes interesadas en los procesos y el desarrollo de políticas de la ICANN.

La ICANN desempeña un rol de respaldo respecto a la labor del orden público y las agencias gubernamentales, en cuanto al cumplimiento de medidas legítimas por ellos solicitadas. La ICANN participa con la comunidad operativa de seguridad en el estudio, el análisis y la identificación del uso indebido o el abuso del DNS.

---

[4] Este concepto está adaptado a partir del documento: "¿Qué es un ecosistema saludable?" de Robert Costanza y Michael Mageau, Instituto de Economía Ecológica de la Universidad de Maryland, publicado en 1999, en AquaticEcology, http://geminis.dma.ulpgc.es/profesores/personal/jmpc/Master08%28PrimeraEdici%F3n%29/Homeostasis/Homeo03s.pdf, http://books.google.com/books?id=YTeCxF5gqMQC&dq=ecosystem+and+health. El concepto descripto también ha sido influenciado por el documento: Un marco para analizar la robustez de los sistemas ecológico-sociales desde una perspectiva institucional (2004), http://www.ecologyandsociety.org/vol9/iss1/art18/.

La ICANN no puede suspender o dar de baja nombres de dominio en forma unilateral. Sí puede hacer cumplir sus contratos con terceros, incluyendo los proveedores de registración de nombres de dominio.

La ICANN desempeña el mismo rol que cualquier parte interesada en lo que respecta a los protocolos de Internet; la evolución de los protocolos de Internet y los estándares relacionados no están dentro del ámbito de alcance de la ICANN. La ICANN apoya el desarrollo de estándares abiertos a través de procesos colaborativos de múltiples partes interesadas.

El Desafío

El uso indebido y los ataques contra el DNS y las redes a nivel mundial desafían la seguridad general de los identificadores únicos. Los ataques al DNS apuntan a la amplia gama de usuarios, individuos particulares, empresas, la sociedad civil y los gobiernos.

A medida que aumenta la frecuencia y sofisticación de los eventos perjudiciales y otros comportamientos maliciosos, la ICANN y la comunidad internacional deben seguir colaborando hacia un ecosistema sano, mejorando la capacidad de recuperación de los sistemas de identificadores únicos y el fortalecimiento de sus capacidades.

La actividad en Internet refleja el rango completo de las motivaciones y conductas humanas. En parte, esta actividad refleja la naturaleza abierta de Internet que la ha hecho una innovación exitosa, ha habilitado innovaciones de punta y ha permitido el intercambio de conocimientos, creatividad y comercio para el bien común a nivel mundial.

En el entorno actual de gobernanza colaborativa entre las múltiples partes interesadas de Internet dentro de un ecosistema más grande, la visión tradicional de seguridad informática liderada por un sector —ya sea por los gobiernos o por el sector privado—, no funciona. Ni los gobiernos ni los actores individuales del sector privado tienen la competencia administrativa o jurídica adecuada sobre el conjunto diverso de sistemas y redes interconectadas; y la magnitud de la tarea de operar y proteger estos recursos está más allá del alcance de cualquier emprendimiento que no se uno multisectorial y colaborativo.

Todas las partes interesadas en la seguridad informática deben adoptar una visión más amplia. En el contexto de los identificadores únicos de Internet, la seguridad debe abordarse a través de un ecosistema de Internet saludable. Este enfoque se centra en una Internet que sea sustentable o saludable, estable y flexible. Un sistema que es sustentable para el futuro. Necesitamos concentrarnos en forma colectiva sobre "la capacidad [del ecosistema] de mantener su estructura y función en el tiempo, frente a la tensión externa."[5]

Este año pasado se ha visto una escalada en las amenazas contra los sistemas de identificadores únicos de Internet. En 2012, los ataques contra los operadores de registro de dominios de nivel superior (véase la declaración del Registro de Dominios de Irlanda —IEDR— del mes de noviembre de 2012, https://www.iedr.ie/wp-content/uploads/2012/12/IEDR-Statement-D-issued-8Nov.pdf y el artículo de *Techcrunch*, del mismo mes, sobre el Centro de Información de Redes de Pakistán —PKNIC—, http://ta.gg/5uf), contra los registradores, el sector bancario, los

[5] Costanza & Mageau, et al.

organismos de orden público y las amenazas a los operadores de servidores raíz han aparecido en los medios de comunicación. Véase el Informe sobre la Seguridad de Infraestructura a Nivel Mundial de Arbor Networks, enero de 2013, http://www.arbornetworks.com/research/infrastructure-security-report.

La intervención del gobierno ha causado que usuarios pierdan conectividad con el mundo externo, por ejemplo en Siria (véase http://www.renesys.com/blog/2012/11/syria-off-the-air.shtml). El huracán Sandy impactó la conectividad de Internet para el Noreste de los EE.UU., mostrando el poder de los desastres naturales sobre las redes globales (véase un Análisis preliminar de los cortes de red durante el huracán Sandy, Informe técnico de USC/ISI: ISI-TR-685b, publicado en noviembre de 2012, ftp://ftp.isi.edu/isi-pubs/tr-685.pdf).

Algunas tendencias inhibidoras para mejorar la salud de los identificadores únicos han incluido la lenta adopción de las DNSSEC (Extensiones de Seguridad para el Sistema de Nombres de Dominio) por parte de los registradores, desarrolladores de navegadores, desarrolladores de aplicaciones y registratarios. Una mayor conciencia del uso delictivo del DNS ha estimulado el interés en el desarrollo de tácticas y herramientas para avanzar al mismo ritmo.

Se han observado otras tendencias como:

- El continuo crecimiento en la adopción de DNSSEC por parte de los operadores de TLD
- La ampliación de las instancias del servidor raíz en todo el mundo
- El lanzamiento de nuevos ccTLDs (Dominio de Nivel Superior con Código de País) —de Nombres de Dominio Internacionalizados (IDN) o no—, en un conjunto creciente de idiomas y alfabetos
- Un mayor progreso en la evaluación de solicitudes del Programa de nuevos gTLD y la introducción de nuevos gTLDs prevista para 2013
- Un mayor interés en el desarrollo de capacidades relacionadas con la seguridad informática, estimulando la oferta de formación en DNS más allá de las comunidades operativas, hacia el orden público y la comunidad jurídica.

El Ecosistema de Internet y la Comunidad de la ICANN

La ICANN funciona en beneficio de la comunidad de Internet en su totalidad. El público es un conjunto diverso de comunidades entretejidas por Internet y funcionando como un ecosistema complejo. Ahora, Internet constituye un facilitador esencial para el intercambio de conocimiento, información, comercio y gobernanza a nivel mundial. Véase la declaración de la UNESCO en Vancouver, septiembre de 2012, (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/unesco_ubc_vancouver_declaration_en.pdf) y WSIS+10 (Cumbre Mundial sobre la Sociedad de la Información), Declaración final Hacia las Sociedades del Conocimiento para la Paz y el Desarrollo, 27 de febrero de 2013 (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_final_statement_en.pdf).

Internet es reconocida como fundamental para el apoyo de la economía y el desarrollo sustentable del mundo (véase Perspectiva Económica de Internet de la OECD —Organización para la Cooperación y el Desarrollo Económicos— 2012, http://www.oecd.org/sti/interneteconomy/ieoutlook.htm).

El término "ecosistema", describe el mundo natural que nos rodea. Se puede definir como la red de interacciones entre los organismos y entre los organismos y su entorno. Los ecosistemas son entidades dinámicas. Internet es un ecosistema; y es una red de organizaciones y comunidades. Estas organizaciones y comunidades trabajan juntas, cada una en su rol. La Internet es exitosa y próspera debido a que su ecosistema es abierto, transparente y colaborativo.

El ecosistema de Internet se compone de una serie de organizaciones y procesos que dan forma a la coordinación y gestión de la Internet global; y que permite su funcionamiento general. Estas organizaciones incluyen: las organizaciones de tecnología e ingeniería, los operadores de red, las organizaciones de gestión de recursos, los usuarios, la sociedad civil, las entidades comerciales y no comerciales, los educadores, legisladores, organismos de orden público y gobiernos.

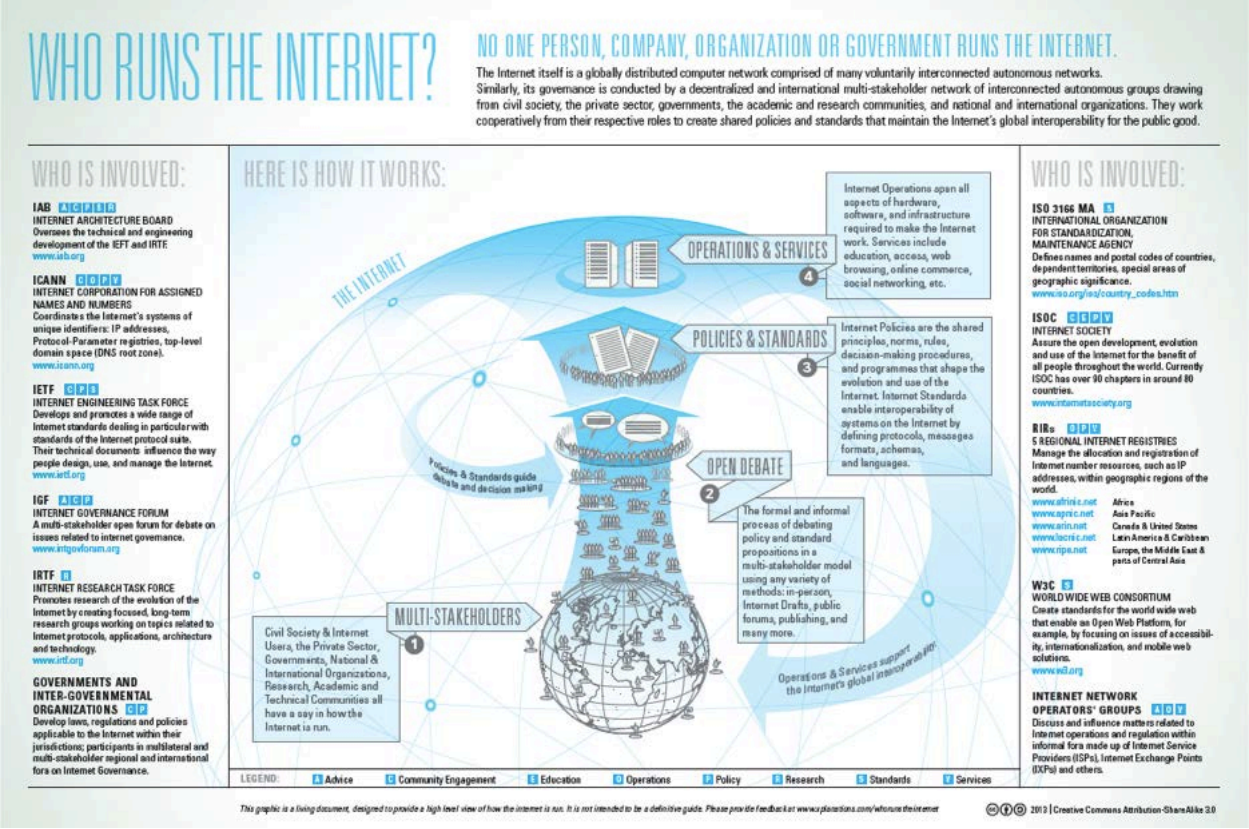


Gráfico 2 – Información gráfica del ecosistema de Internet

Desde una perspectiva de la ICANN, el ecosistema de Internet puede ser visto en tres capas:

- la comunidad global,

- la comunidad de la ICANN,
- y la ICANN como una organización.

La comunidad global contiene a aquellos que confían en un sistema de identificadores únicos que sea saludable, estable y confiable para el intercambio de conocimientos, comercio e innovación, pero que podrían no conocer o participar en la ICANN.

La comunidad de la ICANN contiene a la comunidad más amplia de actores que participan en los programas, procesos y actividades de la ICANN, que impulsan el modelo de desarrollo de políticas de múltiples partes interesadas para el beneficio de los usuarios de Internet a nivel mundial.

La ICANN como organización describe a las estructuras y funciones operativas, al personal de apoyo que respalda a la comunidad más amplia de dicha Corporación y a la coordinación multisectorial de identificadores únicos de Internet.

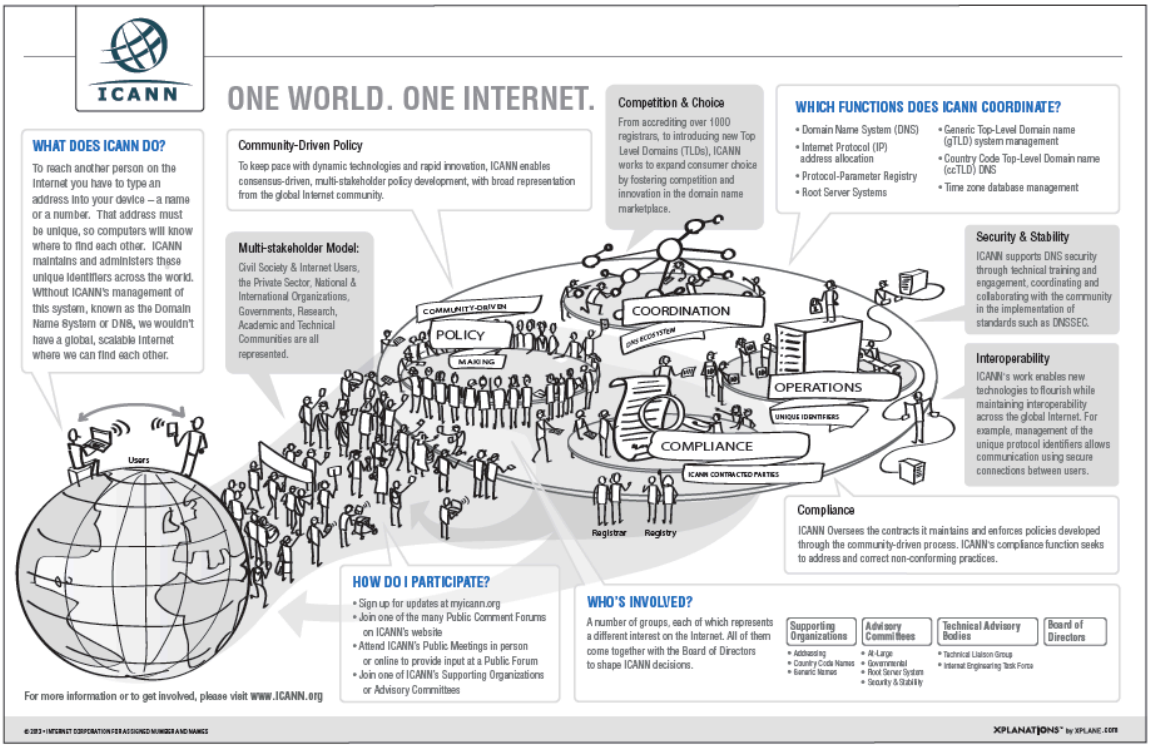


Gráfico 3 – Información gráfica de la ICANN

Una copia completa de 11x17 del gráfico anterior se encuentra disponible en seis idiomas, en https://community.icann.org/display/ISBM/Handouts+for+Speakers+Bureau.
La comunidad participa en la ICANN a través de grupos de partes interesadas, unidades constitutivas, organizaciones de apoyo y comités asesores. La información sobre los comités asesores puede ser encontrada en sus páginas, debajo indicadas:

1. Comité Asesor At Large - http://www.atlarge.icann.org/alac
2. Comité Asesor Gubernamental - https://gacweb.icann.org/

3. Comité Asesor del Sistema de Servidores Raíz- http://www.icann.org/en/groups/rssac
4. Comité Asesor de Seguridad y Estabilidad - http://www.icann.org/en/groups/ssac

Estos comités proporcionan asesoramiento a la Junta Directiva de la ICANN, ofrecen aportes para el proceso de desarrollo de políticas y respaldan la participación de la comunidad.

El desarrollo de políticas se deriva de tres Organizaciones de Apoyo:

1. Organización de Apoyo para Direcciones (ASO) - http://aso.icann.org/ (direcciones IP)
2. Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO) - http://ccnso.icann.org/ (ccTLDs)
3. Organización de Apoyo para Nombres Genéricos – http://gnso.icann.org (gTLDs)

Desde la creación de la ICANN en 1998, hace 15 años, el DNS ha crecido desde cientos de miles de nombres de dominio distribuidos en siete dominios genéricos de nivel superior —y alrededor de 25 mil TLDs con código de país—, a un DNS con más de 250 millones de nombres de dominio, utilizados por 2,5 mil millones de usuarios de Internet, a través de 316 TLDs. Este espacio está destinado a crecer dramáticamente con la introducción de nuevos dominios genéricos de nivel superior en 2013.

A partir de marzo de 2013, hay 316 TLDs delegados en la zona raíz. El gráfico siguiente explica cómo se clasifican estos dominios de nivel superior.

Gráfico 4 - TLDs en la Zona Raíz (crédito de la imagen: Kim Davies, IANA)

Relaciones de SSR

La ICANN mantiene relaciones con partes contratadas (registros y registradores de nombres de dominio, proveedores de depósitos y demás), así como asociaciones, memorandos de entendimiento, marcos de responsabilidad e intercambio de cartas. Las relaciones entre la ICANN y otras organizaciones o partes interesadas internacionales del ecosistema, podrían ser menos formales o poco estructuradas. https://www.icann.org/en/about/agreements.

Las partes en el proceso de registración de nombres de dominio deben trabajar juntas para asegurar que las decisiones tomadas en relación con la coordinación técnica global de los identificadores únicos de Internet sean tomadas en el interés público, de manera responsable y transparente.

La imagen de abajo muestra la naturaleza de las relaciones en el proceso de registración de dominios https://www.icann.org/en/about/agreements.

Como parte de las recomendaciones 4 y 5 del Equipo revisor de SSR, la ICANN está en proceso de documentar y definir la naturaleza de sus relaciones de SSR dentro de la comunidad de la ICANN. Esto ayudará a proporcionar un único punto focal para la comprensión de las interdependencias entre las diversas organizaciones y entidades —dentro de sus respectivas funciones—, y permitirá a la ICANN mantener acuerdos de trabajo eficaces en apoyo a los objetivos de SSR y objetivos estratégicos de la ICANN.

Parte B – Módulo de SSR para FY14

Esta sección del Marco de seguridad, estabilidad y flexibilidad se enfoca en las actividades e iniciativas previstas de SSR para el año fiscal 2014, abarcando el período desde el 1 de julio de 2013 al 30 de junio de 2014.

Seguridad en el Plan Estratégico de la ICANN

El Plan estratégico de la ICANN identifica la estabilidad y seguridad del DNS como una de las cuatro áreas clave de enfoque estratégico para la organización. Esto está alineado con la gran importancia dada a la SSR en la Afirmación de Compromisos. El Plan estratégico separa la amplia gama de responsabilidades de la ICANN en cuanto a la seguridad, estabilidad y flexibilidad en objetivos estratégicos, trabajos de la comunidad, proyectos estratégicos y la labor del personal.

El Plan estratégico de la ICANN para 2012-2015 no cambiará durante 2013 (véase https://www.icann.org/en/news/announcements/announcement-28jan13-en.htm). Este es el mismo Plan estratégico publicado con antelación al Marco de SSR para FY13 (junio de 2012). El mismo ha sido reorganizado a partir de la retroalimentación recibida en el ciclo de planificación de 2013 respecto a la existencia de una constante demanda de actividades de formación y desarrollo de capacidades por parte de la comunidad. Esto demuestra el apoyo a la participación técnica ofrecido por el Equipo de seguridad de la ICANN.

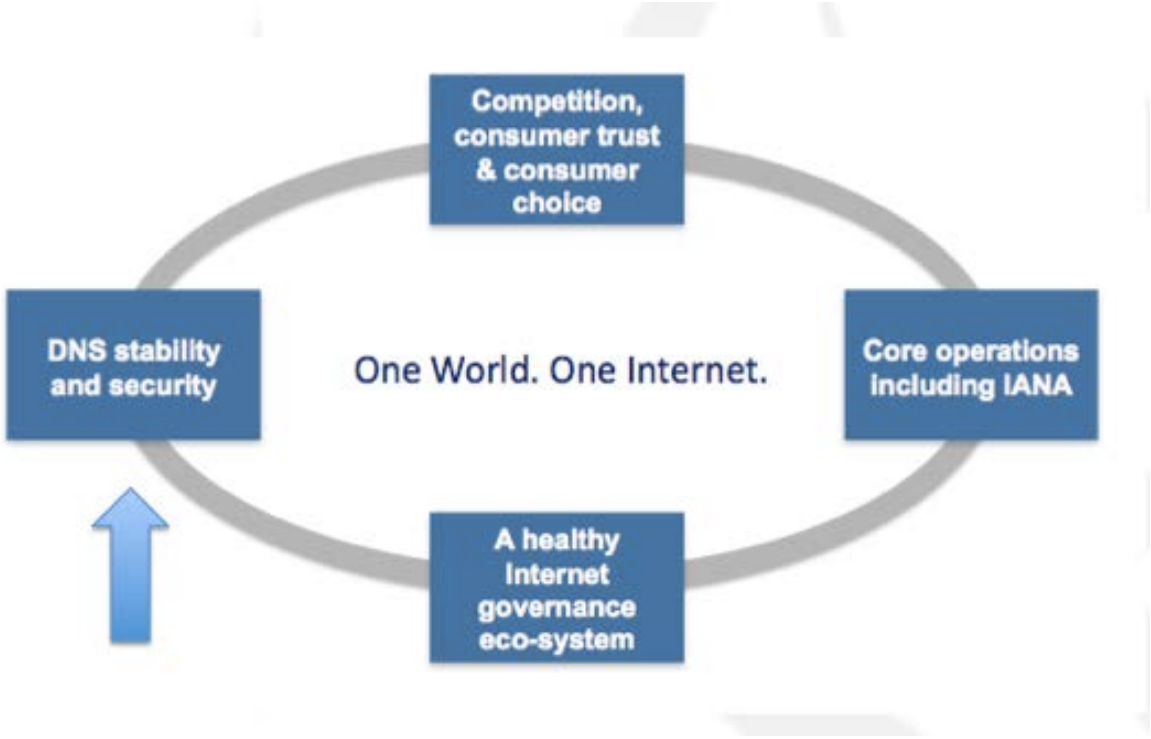


Gráfico 5 – Plan estratégico de la ICANN

El Plan estratégico 2012-2015 describió 5 objetivos estratégicos para la seguridad y estabilidad del DNS:

1. Mantener y manejar la disponibilidad del DNS
2. Mejorar la gestión de riesgos y la flexibilidad del DNS, las direcciones IP y parámetros
3. Promover la amplia adopción de las DNSSEC
4. Mejorar la cooperación internacional sobre el DNS
5. Mejorar las respuestas a incidentes de seguridad del DNS

ICANN comenzará un proceso de Planificación estratégica para enfocarse en un plan a largo plazo para los próximos cinco años, a partir de junio de 2013. Mayor información sobre este nuevo enfoque estará disponible. Dado que la seguridad es fundamental para la organización, la seguridad, estabilidad y flexibilidad del sistema de identificadores únicos continuará siendo una de las principales áreas estratégicas para la ICANN.

Revisión de la Afirmación de Compromisos

La Afirmación de Compromisos firmada por la ICANN y el Departamento de Comercio de los EE.UU. el 30 de septiembre de 2009 (http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm) reconoció que un compromiso clave incluye preservar la seguridad, estabilidad y flexibilidad del DNS (Sección 3b). La Afirmación también ha "institucionalizado y formalizado la coordinación técnica del sistema de nombres de dominio y direccionamiento de Internet (DNS) a nivel mundial, por parte de una organización conducida por el sector privado".

En la Sección 9.2, la Afirmación de Compromisos reconoce que la ICANN ha adoptado un Plan de Seguridad, Estabilidad y Flexibilidad (SSR), el cual será regularmente actualizado para reflejar las nuevas amenazas al DNS (incluidos los identificadores únicos). Este Plan será revisado al menos cada tres años.

La primera revisión de SSR concluyó en junio de 2012 "la búsqueda de áreas en las que la ICANN está trabajando bien, áreas en las que existe margen de mejora y otras áreas donde los elementos clave de SSR deben ser definidos e implementados." Informe final del Equipo revisor de SSR, junio de 2012.

La Junta Directiva de la ICANN aprobó el informe final y las recomendaciones en el mes de octubre de 2012.[6] Desde la reunión que la ICANN celebró en Toronto, dicha Corporación ha avanzado hacia la implementación de las recomendaciones del Equipo revisor de SSR.

El 19 de diciembre de 2012 se publicó una actualización del progreso de implementación llevado a cabo por la ICANN (http://blog.icann.org/2012/12/tracking-the-ssr-review-implementation/). Ya se han implementado dos recomendaciones (recomendaciones 18 y 24). Para el período que queda de FY13 hasta FY15 y el inicio del nuevo proceso de revisión de SSR,

[6] http://www.icann.org/en/groups/board/documents/resolutions-18oct12-en.htm#1.e

la ICANN realizará el seguimiento de las implementaciones conjuntamente con otras revisiones de la Afirmación de Compromisos. (http://www.icann.org/en/news/in-focus/accountability).

Las veintiocho recomendaciones se han alineado con la estructura de Entregas de gestión de la ICANN, revelada en la reunión que la ICANN celebró en Toronto. Estas son:

- Afirmación de Propósito [recomendaciones 1, 2, 18, 24]
- Excelencia Operativa [recomendaciones 7, 8, 17, 20, 21, 9, 10, 11, 22, 25, 26, 27, 15, 28]
- Internacionalización [recomendaciones 3, 4, 5, 14, 16]
- Evolución del modelo de múltiples partes interesadas [recomendaciones 6, 12, 13, 19, 23]

En el Apéndice A se pueden encontrar mayores detalles sobre la implementación de recomendaciones particulares. Los Planes y Marcos de SSR previos de la ICANN, que abarcaron los años fiscales 2010, 2011, 2012 y 2013, están disponibles en https://www.icann.org/en/about/staff/security/archive.

Una Nueva Temporada – Hacia una Organización Matriz

En el mes de octubre de 2012, en la reunión que la ICANN celebró en Toronto, el Director Ejecutivo (CEO) de la ICANN, Fadi Chehade, dio a conocer la nueva estructura de Entregas de gestión de la ICANN. Esto aplica una organización matriz a las funciones de la ICANN. La seguridad es parte de las funciones técnicas dentro de la ICANN, a la par con la IANA y los equipos de IT (Tecnología de la Información) y Operaciones de dicha Corporación.

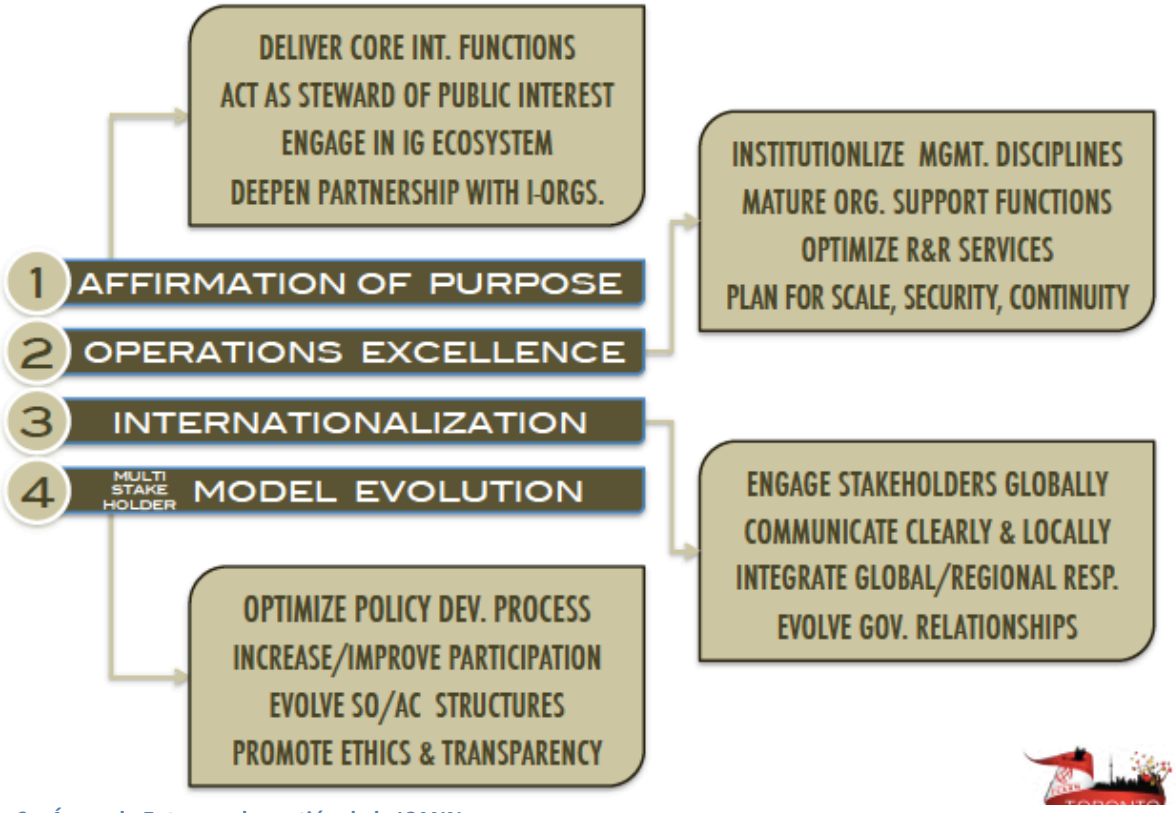


Gráfico 6 – Áreas de Entregas de gestión de la ICANN

Las actividades del Equipo de seguridad se entrecruzan en toda la organización, respaldando a cada una de las 4 áreas de entregas de gestión. Esto incluye el apoyo a la Excelencia operativa y al Equipo multisectorial de participación mundial (GSE) en la internacionalización, la evolución del modelo de múltiples partes interesadas y las contribuciones a los debates más extensos de gobernanza con la comunidad más amplia de Internet.

El modelo matriz se implementará mediante la distribución del trabajo de la ICANN entre tres centros principales: Los Ángeles, Singapur y Estambul. La ICANN también mantendrá las oficinas participativas en Bruselas, Washington DC y otros lugares, para acercarse a sus grupos de partes interesadas.

Una Visualización de la Seguridad de la ICANN

Como parte de la explicación del rol y el alcance de la ICANN, el siguiente gráfico preliminar proporciona una visualización de las funciones de seguridad, estabilidad y flexibilidad de la ICANN.

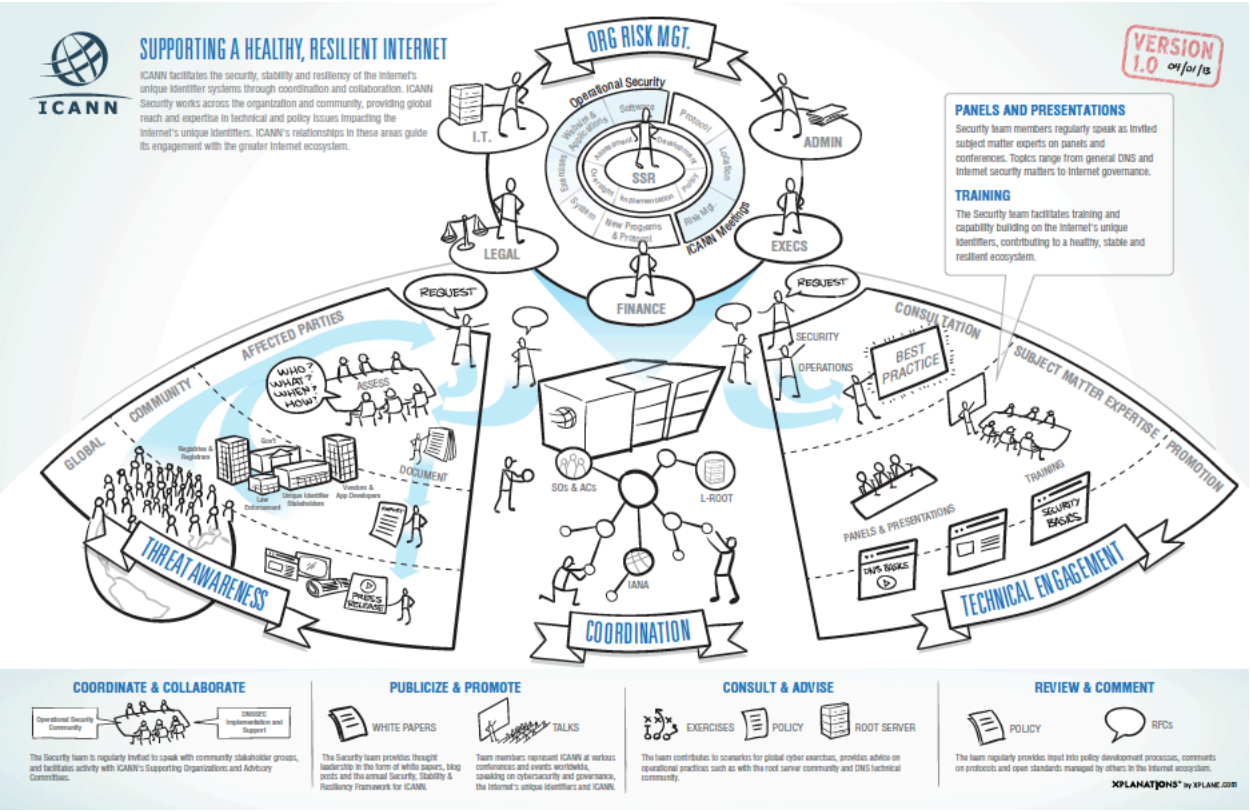


Gráfico 7 – Información gráfica de seguridad de la ICANN

Este gráfico muestra las principales funciones de seguridad de ICANN, en el apoyo a la gestión de riesgos de la organización, en facilitar el conocimiento de las amenaza a los identificadores únicos de Internet, en la colaboración y la coordinación con los socios de la comunidad de Internet, y en ofrecer pericia en el tema de la participación técnica —incluyendo capacitación—, liderazgo y consultas sobre asuntos técnicos y de política. (Nota: este es un trabajo en progreso y será revisado antes de la reunión que la ICANN celebrará en Beijing).

Cómo cabe la seguridad, estabilidad y flexibilidad en las áreas funcionales de la ICANN

La seguridad en la ICANN puede ser vista como:

- Un valor central para la ICANN, en la Afirmación de Compromisos
- Una de las cuatro áreas de enfoque del Plan estratégico
- Un área temática general entrecruzada a través de toda la organización
- Un departamento dentro de la ICANN
- Un elemento esencial en los proyectos y actividades

El Equipo de seguridad de la ICANN está distribuido, contando con un alcance a nivel mundial y con pericia en cuestiones técnicas y de políticas que afectan a los identificadores únicos de Internet. El equipo de Seguridad tiene un rol interno y uno externo, trabajando a través de toda la organización y la comunidad para apoyar la misión de la ICANN de preservar y mejorar la estabilidad operacional, la confiabilidad e interoperabilidad de Internet a nivel mundial. Este trabajo no siempre es visible o público, pero sí juega un rol importante para la ICANN y sus compromisos. El equipo se desempeña como un puente entre los operadores del DNS, la comunidad técnica, los organismos de orden público, la comunidad de seguridad operativa y los grupos de partes interesadas.

Miembros del equipo de seguridad de la ICANN

Al momento de publicar el presente documento, el equipo de Seguridad incluye a:

- Jeff Moss – Vicepresidente y Ejecutivo Jefe de Seguridad (Conductor del equipo y miembro del Equipo Ejecutivo de la ICANN; Participación técnica y orador frecuente sobre cuestiones de seguridad e Internet)
- Geoff Bickers – Director de Seguridad (Programas de seguridad corporativos, Seguridad de reuniones, Seguridad física y del Personal de la ICANN, coordinador con el Departamento de IT de la ICANN)
- John Crain – Director Principal de Seguridad, Estabilidad y Flexibilidad (Participación técnica, Conducción en conocimiento y monitoreo de amenazas, Representante del servidor raíz en el Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio —DNS-OARC— de la Junta)
- Patrick Jones – Director Principal, Seguridad (Coordinación del equipo, miembro del Equipo Ejecutivo de la ICANN, implementación del Equipo revisor de SSR, coordinador con el Equipo multisectorial de participación mundial —GSE— y participación en la gobernanza de Internet)
- Richard Lamb – Gerente Principal de Programa, DNSSEC (Participación técnica en la adopción y capacitación sobre DNSSEC; colaboración con la comunidad sobre DNSSEC; Gestión de políticas y Prácticas para el despliegue de las DNSSEC)

- Dave Piscitello – Tecnólogo Principal de Seguridad (Participación técnica, capacitación y liderazgo innovador; Dirigente dentro de la comunidad de orden público y seguridad operativa; miembro del Grupo de gestión ejecutiva de la Iniciativa contra delitos informáticos de la Commonwealth)
- Sean Powell – Ingeniero de Seguridad de la Información (Seguridad organizacional; Seguridad de información y de redes; colaboración con el Departamento de IT y apoyo al Director de Seguridad de la ICANN)

Foto 1- Jeff Moss en el Foro de Gobernanza de Internet (IGF) de Rusia

Foto 2 - John Crain, Rick Lamb (ICANN) y Revil Wooding (PCH) en CaribNOG 3

Foto 3 - Patrick Jones en el Diálogo sobre seguridad informática de la Organización de Estados Americanos (OAS), diciembre de 2012

Foto 4 - Dave Piscitello hablando en la Red de Derecho Penal Internacional (ICLN), La Haya, diciembre de 2012

Criterios de Participación

En febrero de 2012, el Equipo de seguridad formalizó sus criterios para la difusión y participación. Los criterios han tenido una gran influencia en otras partes de la ICANN y está destinado a ofrecer orientación al Equipo de seguridad de la ICANN y la Dirección ejecutiva respecto a los tipos de actividades de colaboración y de la comunidad que están respaldados por el Equipo de seguridad.

Tabla 1 – Criterios de seguridad para la difusión y participación

Tipos de Eventos	Ejemplos
Reuniones públicas de la ICANN	ICANN Beijing, Durban, Buenos Aires
Reuniones internas de la ICANN	Reunión ejecutiva, Equipo de seguridad, Talleres, Capacitación del personal, Presupuesto, otras
Reuniones relevantes para aspectos operativos de ICANN/IANA/raíz-L/DNSSEC, etc.	IETF, DNS-OARC, RIPE NCC, NOGs, SSAC, RSSAC, otras
Reuniones donde la ICANN colabora sobre amenazas y su mitigación a nivel mundial	APWG, MAAWG, Interpol Underground Economy, ejercicios informáticos, OAS
Participación técnica – Capacitación y Desarrollo de capacidades	Entrenamiento sobre Plan de Respuesta a Ataques y Contingencia (ACRP), Operaciones seguras de registros, DNSSEC, Orden público y gobiernos, Iniciativa contra el delito informático de la Commonwealth
Simposios, Conferencias de SME como invitados, educación continua	SATIN, Simposio de SSR, Security Confab, RSA, BlackHat, FIRST, ICLN
Participación en el ecosistema, modelo de múltiples partes interesadas	Foro de Gobernanza de Internet (IGF) y IGFs regionales, RANS, OECD, Foro de WSIS, Seguridad informática del panarabismo, CTU

Criterios de Participación		✓
¿Apoya el evento un objetivo estratégico de la ICANN?	1. Mantener, Conducción de la disponibilidad del DNS 2. Mejorar la Gestión de riesgos y la flexibilidad del DNS 3. Promover la amplia adopción de las DNSSEC 4. Mejorar la cooperación internacional para el DNS 5. Mejorar las respuestas a incidentes de seguridad del DNS	
¿Se adecua el evento a una de las siguientes áreas?	1. Operativo/Organizacional 2. Colaboración 3. Participación técnica	
¿Respalda una asociación, Memorando de Entendimiento o relación multisectorial?		
¿Respalda o suma a la reputación organizacional		

de la ICANN?	
¿Qué tan frecuentemente ocurre el evento?	
¿Pueden otras partes interesadas reunirse cerca?	¿Quién más asiste?
¿En qué lugar del presupuesto se adecua?	¿Es para respaldar a otro equipo?

Con la creación de la nueva estructura matriz, el Equipo de seguridad proporciona apoyo al Equipo multisectorial de participación mundial (GSE) de la ICANN y a otros equipos de la organización. Los siguientes son ejemplos de los tipos de eventos y actividades apoyadas por el Equipo de seguridad de ICANN:

- Reuniones de la IETF (Fuerza de Trabajo en Ingeniería de Internet) en Vancouver y Atlanta
- Reuniones de X-Con, CNNIC y CONAC en China
- BlackHat y DefCon en Las Vegas, Abu Dhabi y Ámsterdam
- Grupo de expertos en nombres geográficos de las Naciones Unidas (UN)/Conferencia de la UN sobre la Normalización de los nombres geográficos en Nueva York
- Interpol Underground Economy en Lyon, France
- Reunión de los registros CIS en Budva, Montenegro
- Capacitación en DNS con la Agencia contra el Gran Crimen Organizado y el Departamento de protección al consumidor en Londres, Reino Unido
- Capacitación sobre DNSSEC en Colombia con .CO; en Perú con .PE y el Centro de Recursos para Redes en Formación en Hong Kong
- Capacitación sobre el desarrollo de capacidades sobre el DNS, con LACTLD en St. Maarten y Paraguay
- Comunidad de Telecomunicaciones de Asia-Pacífico en Macau
- MENOG en Jordania
- LACNIC/LACNOG en Uruguay
- Capacitación sobre DNS con Europol
- MAAWG, APWG, RIPE NCC y DNS-OARC
- Lanzamiento de laboratorio informático de OAS CICTE para ejercicios
- APNIC 34
- ION Bombay e Interop
- Suministro de conversaciones a través de presentaciones a distancia, tal como en IGF del Caribe en St. Lucia, en agosto de 2012 y la Conferencia nepalesa de ICT, en febrero de 2013

Una parte clave de la participación técnica suministrada por el Equipo de seguridad es en la capacitación sobre el DNS en respuesta a las peticiones de la comunidad. El equipo ha elaborado un plan de estudios, que incluye módulos sobre:

- Conceptos básicos sobre el DNS (incluyendo generalidades de la participación en la ICANN)
- Programa de respuesta a ataques y contingencia para los operadores de TLD
- Capacitación sobre el DNS para las fuerzas de orden público y la comunidad de seguridad operacional
- Capacitación sobre las DNSSEC
- Curso de operaciones de seguridad de los registros

A menudo la ICANN colabora con el Centro de Recursos para Redes en Formación (http://nsrc.org/), con sede en la Universidad de Oregon, suministrando participación técnica con las organizaciones regionales de TLD, universidades y operadores de todo el mundo. Para esta capacitación, la ICANN también se asocia con AfTLD (Organización de Dominios de Nivel Superior de África), APTLD (Asociación de Dominios de Nivel Superior de Asia-Pacífico) y LACTLD (Asociación de Dominios de Nivel Superior de América Latina y el Caribe).

Desarrollos Internacionales

En FY13 ha habido una actividad significativa en el ámbito global. La ICANN firmó los Principios para la Flexibilidad informática del Foro Mundial de Economía, http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf, y participó en los eventos del Foro Mundial de Economía en Davos, Suiza y en Washington DC, en 2012 y 2013.

La ICANN fue anfitriona de la Iniciativa contra Delitos Informáticos de la Commonwealth (CCI) en la reunión de Praga, República Checa, en junio de 2012. En el mes de noviembre de 2012, Dave Piscitello del Equipo de seguridad de la ICANN fue designado para el Grupo de gestión ejecutiva de la Iniciativa contra delitos informáticos de la Commonwealth (http://blog.icann.org/2012/11/icann-security-team-members-appointed-to-lead-roles-in-global-community-initiatives/).

La ICANN apoyó la capacitación sobre las DNSSEC en América Latina y el Caribe (Trinidad, Colombia, Chile, Perú y Paraguay).

En el mes de julio, el Departamento de Comercio de los EE.UU. anunció la asignación del contrato de funciones de la IANA para la ICANN, http://www.ntia.doc.gov/press-release/2012/commerce-department-awards-contract-management-key-internet-functions-icann. El día 9 de julio de 2012, la ICANN publicó una versión redactada de su propuesta para el contrato de funciones de la IANA: https://www.icann.org/en/news/announcements/announcement-2-09jul12-en.htm. El período de desempeño es desde el día 1 de octubre de 2012 al día 30 de septiembre de 2015, con dos períodos opcionales para un período contractual total de siete años.

En el mes de julio de 2012, la ICANN participó en la Reunión de seguridad informática hemisférica de OAS en Uruguay y en el Diálogo sobre seguridad informática de OAS en Washington DC, el 13 de diciembre de 2012, http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-465/12.

En agosto de 2012, el IAB (Comité de Arquitectura de Internet), el IEEE-SA (Instituto de Ingenieros Eléctricos y Electrónicos), la IETF, la Sociedad de Internet y el W3C (Consorcio Mundial de Internet) lanzaron una Normativa Abierta (http://open-stand.org/) como un modelo abierto para el desarrollo colaborativo y ascendente de normativas para la innovación e interoperabilidad. Esta iniciativa está en consonancia con los principios de la ICANN para la colaboración multisectorial, de abajo hacia arriba, basada en el consenso.

La ICANN contribuyó con el III Consejo de seguridad, flexibilidad e interoperabilidad de la Comisión de Comunicaciones Federales de los EE.UU. (US FCC - CSRIC III). En septiembre de 2012, el Grupo de trabajo 4 publicó su informe sobre las Mejores prácticas recomendadas para la seguridad de redes (http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG4-FINAL-Report-DNS-Best-Practices.pdf). También se suministraron contribuciones al Grupo de trabajo 3, a las DNSSEC, al Grupo de trabajo 7 y al Código de conducta anti robots para los ISPs (Proveedores de Servicios de Internet).

En el mes de octubre de 2012, la ICANN participó en la Conferencia de Budapest sobre el Espacio informático (http://www.cyberbudapest2012.hu/), el evento de seguimiento de la Conferencia de Londres celebrada en 2011 (https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement).

La ICANN fue coanfitriona de su 4to Simposio Mundial sobre SSR del DNS, junto con el Grupo de trabajo sobre Suplantación de Identidad (APWG) en su evento eCOS realizado en Las Croabas, Puerto Rico, en el mes de octubre de 2012 (http://docs.apwg.org/events/2012_ecrime.html).

En octubre de 2012, la OECD (Organización para la Cooperación y el Desarrollo Económicos) publicó en varios documentos nacionales de estrategia, un análisis de las estrategias nacionales de seguridad informática, describiendo el respaldo al diálogo multisectorial sobre la seguridad informática. La cita de este documento es OECD (2012), "*Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*" [Desarrollo de Políticas sobre Seguridad Informática en un Punto de Inflexión: Analizando una Nueva Generación de Estrategias Nacionales para la Seguridad Informática de la Economía de Internet], *OECD Digital Economy Papers* [Documentos Digitales de Economía de la OECD], No. 211, OECD Publishing. http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

La ICANN estuvo bien representada en el 7mo Foro de Gobernanza de Internet (IGF) celebrado en Bakú, Azerbaiyán, en el mes de noviembre de 2012 (http://blog.icann.org/2012/10/icann-at-internet-governance-forum-2012-2/), durante el cual la seguridad de Internet fue uno de los principales temas de debate (http://www.intgovforum.org/cms/component/content/article/114-preparatory-process/927-igf-2012). La ICANN también asistió a los eventos regionales del IGF en América Latina y el Caribe, en Rusia, Emiratos Árabes Unidos y los Estados Unidos de América.

En diciembre de 2012, el CEO de la ICANN, Fadi Chehade, habló sobre la apertura de la Conferencia Mundial sobre Telecomunicaciones Internacionales en Dubai (http://www.itu.int/en/wcit-12/Pages/speech-chehade.aspx). En febrero de 2013, la ICANN participó en la preparación del Grupo informal de expertos para el próximo Foro Mundial de Políticas sobre Telecomunicaciones, a celebrarse en Ginebra durante el mes de mayo de 2013.

En el mes de diciembre de 2012, la ICANN participó en el Observatorio de Seguridad Informática del Panarabismo en Túnez, República Tunecina, compartiendo información con los participantes respecto al rol y alcance de la ICAN en cuanto a las actividades de seguridad, estabilidad y flexibilidad. En diciembre la ICANN también participó en la conferencia de la Red de Derecho Penal Internacional (ICLN) celebrada en La Haya, Países Bajos, y se comprometió con Europol para suministrar capacitación sobre el DNS junto al lanzamiento del nuevo Centro Europeo para la Delincuencia Informática (EC3).

En enero de 2013, el Equipo de seguridad de la ICANN publicó un documento de reflexión titulado El Valor de Evaluar el Daño Colateral Antes de Solicitar la Captura de un Dominio, http://blog.icann.org/2013/01/the-value-of-assessing-collateral-damage-before-requesting-a-domain-seizure/. Este es un seguimiento del documento de reflexión de marzo de 2012 sobre Capturas y Bajas de Dominios, http://blog.icann.org/2012/03/thought-paper-on-domain-seizures-and-takedowns/. Esto está relacionado con el documento SAC056, Asesoramiento del SSAC (Comité Asesor de Seguridad y Estabilidad) sobre los Impactos en el Bloqueo de Contenido a través del Sistema de Nombres de Dominio, http://www.icann.org/en/groups/ssac/documents/sac-056-en.pdf, publicado en el mes de octubre de 2012.

La ICANN ha seguido la elaboración de la Estrategia de Seguridad Informática de la Unión Europea (EU) (enero de 2013), http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security y la Orden Ejecutiva sobre Seguridad Informática de los EE.UU. (febrero de 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0. Ambos documentos representan el creciente interés en el establecimiento de mecanismos para el intercambio y la colaboración, en respuesta a amenazas para la seguridad informática.

Los eventos clave de Internet a nivel mundial, antes de la publicación del presente documento, incluyeron:

- APRICOT 2013 (Conferencia Regional de Asia Pacífico sobre las Tecnologías Operativas de Internet) en Singapur, del 19 de febrero al 1 de marzo de 2013, http://www.apricot2013.net/.
- WSIS+10, Hacia el Conocimiento de las Sociedades para la Paz y Desarrollo Sustentable (auspiciado por la UNESCO), en París del 25 al 27 de febrero de 2013, http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/wsis-10-review-event-25-27-february-2013/.
- Evento de Gobernanza de Internet de múltiples partes interesadas árabes, evento celebrado en Dubai, Emiratos Árabes Unidos (UAE) y evento de Gobernanza de Internet de múltiples partes interesadas africanas, celebrado en Addis Ababa,

Etiopía, http://www.icann.org/en/news/announcements/announcement-07feb13-en.htm.

- IETF 86, celebrada en Orlando, Florida, del 10 al 15 de marzo de 2013, http://www.ietf.org/meeting/86/index.html.

Actividades para FY14

Para FY14, las actividades de la ICANN en respaldo a un ecosistema saludable, estable y flexible, tendrán los siguientes enfoques:

- Apoyo a la Excelencia Operativa en las actividades dirigidas por la IANA, IT y operaciones del DNS
- Proporcionar la participación técnica (a través de expertos en la materia y de liderazgo innovador, la participación de la comunidad, la realización de actividades de capacitación sobre el DNS y actividades de desarrollo de capacidades solicitadas entre los asociados)
- Fomentar la adopción y el conocimiento de las DNSSEC por parte de las empresas, los usuarios y operadores
- Implementación de las recomendaciones del Equipo revisor de SSR
- Apoyo adicional para la capacidad de la raíz-L, la publicación de los datos y medidas por parte del Equipo de operaciones del DNS de la ICANN
- Entrega de un Marco para la gestión de riesgos del DNS y la finalización de un ciclo de evaluación
- Incrementar la experiencia de la ICANN en la gestión de riesgos empresariales a fin de respaldar mejor al Comité de Riesgos de la Junta y las necesidades de gestión de riesgos organizacionales cambiantes de la ICANN
- Apoyar el establecimiento de nuevas oficinas de ICANN en Singapur y Estambul; y la ampliación de las capacidades del Equipo de seguridad en esos lugares para servir mejor a la comunidad
- Servir como un recurso para el Equipo multisectorial de participación mundial, en las discusiones sobre seguridad informática y gobernanza de Internet, representando a la ICANN en conferencias y reuniones
- Facilitar y promover una participación más amplia en la ICANN por parte de las agencias de orden público y la comunidad de seguridad operacional
- Participar con la Sociedad civil sobre cuestiones de privacidad y libre expresión en relación a la seguridad de los identificadores únicos y a un ecosistema saludable de Internet (ampliar la difusión y el compromiso sobre cuestiones de SSR por parte de los participantes del ecosistema)
- Fortalecer las redes internas de la ICANN, los procesos de IT y la seguridad de la información

- Colaborar con la comunidad técnica, los operadores de servidores raíz y los desarrolladores de aplicaciones y buscadores sobre problemas del DNS
- Apoyo a los equipos de Políticas y Relaciones multisectoriales de la ICANN, cuando sea necesario (SSAC, RSSAC–Comité Asesor del Sistema de Servidores Raíz– y cuestiones de SSR cuando sean debatidas en las SOs –Organizaciones de Apoyo– y ACs –Comités Asesores–)
- Apoyo para reuniones exitosas de la ICANN en Durban, Buenos Aires, Singapur y Londres

Con el fin de cumplir con estas iniciativas, la ICANN necesita ampliar su Equipo de seguridad en FY14, contando con conocimientos y habilidades adicionales. Esto es necesario para satisfacer las necesidades de la comunidad y la estructura matriz que está siendo implementada este año fiscal. En el próximo plan operativo y presupuestario FY14 se ofrecerá una explicación en apoyo a las actividades de SSR proyectadas para FY14, la cual se publicará después de la reunión que la ICANN celebrará en Beijing. Esto seguirá las directrices de las Recomendaciones 20 y 21 de SSR, en cuanto a que la ICANN aumente la transparencia de la información sobre la organización y el presupuesto relacionado con el Marco de SSR y que suministre un proceso más estructurado para mostrar de qué manera se relacionan las decisiones organizacionales y presupuestarias con el Marco de SSR.

Apéndices

Apéndice A- Seguimiento de las recomendaciones del Equipo revisor de SSR

Esta sección proporciona detalles sobre los enfoques de implementación para las 28 recomendaciones realizadas por el Equipo revisor de SSR, según su alineación con las 4 áreas de entrega de gestión.

Afirmación de Propósito – Alcance y Misión de la ICANN

Recomendación del Equipo Revisor de SSR	Implementación y Estatus
#1 - La ICANN debe publicar una declaración única, clara y coherente de su área de alcance de SSR y su misión técnica limitada.	Entre los meses de mayo a septiembre de 2012 se recibieron comentarios públicos sobre la declaración [enlace: http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm]. La declaración preliminar fue revisada el día 4 de octubre de 2012 [http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct2012-en.pdf]. En el Marco de SSR para FY14 aparece una versión actualizada.
#2 - La definición de la ICANN y la implementación de su área de alcance de SSR y misión técnica limitada deben ser revisadas con el fin de mantener el consenso y obtener retroalimentación por parte de la comunidad.	El rol y declaración de alcance actualizados serán examinados con el próximo Equipo revisor de SSR en 2015.
#24 - La ICANN debe definir claramente el estatuto, los roles y responsabilidades del equipo del Oficial jefe de seguridad (CSO).	**Implementado** con la página actualizada del Equipo de seguridad [enlace: https://www.icann.org/security] el día 4 de octubre de 2012 y la publicación del Marco de SSR para FY13. En 2012, los roles y responsabilidades serán refinados más detalladamente con la implementación de la estructura de Entregas de gestión.
#18 - La ICANN debe efectuar una revisión operacional anual de su progreso en la implementación del Marco de SSR e incluir esta evaluación como un componente del Marco de SSR del año siguiente.	**Implementado** como parte del Marco de SSR para FY13 y se repetirá en forma anual. El seguimiento del progreso realizado será agregado a la nueva página de Panel de Gestión de la página del Equipo de seguridad del sitio web de la ICANN.

Excelencia Operativa – Objetivos

Recomendación del Equipo Revisor de SSR	Implementación y Estatus
#7 - La ICANN debe ampliar su marco actual de SSR mediante el establecimiento de un conjunto claro de objetivos y priorizando sus iniciativas y actividades de	La nueva estructura de Entregas de gestión se utilizará para alinear los objetivos e iniciativas de la ICANN con el Marco anual de SSR, y apoyar el desarrollo del presupuesto, el plan operativo y el próximo Plan estratégico de ICANN para FY14. La ICANN está trabajando para alinear sus objetivos y actividades con esta

acuerdo con estos objetivos.	estructura.
#8 - La ICANN debe continuar refinando sus objetivos del Plan estratégico; en particular, el objetivo de mantener e impulsar la disponibilidad del DNS. Clara consonancia entre el Marco y el Plan estratégico.	Esto está relacionado con el próximo Plan Estratégico. Se necesita de un alineamiento de los objetivos y las actividades del Plan Estratégico con el Marco anual de SSR y las recomendaciones del Equipo revisor de SSR.

Excelencia en las Operaciones – Transparencia

Recomendación del Equipo de SSR	Implementación y Estatus
#17 - La ICANN debe establecer un proceso interno más estructurado para mostrar cómo se relacionan las actividades e iniciativas con metas y objetivos estratégicos y con las prioridades dentro del Marco de SSR.	La estructura de Entregas de gestión ha sido muy útil para abordar esta recomendación, creando un mecanismo para un proceso interno que mostrará cómo las actividades e iniciativas de SSR de la ICANN están relacionadas con las metas, objetivos y prioridades. Más información sobre este proceso se pondrá a disposición de la comunidad a través de MyICANN y en el sitio web de la ICANN entre las reuniones que dicha Corporación celebrará en Beijing y Durban.
#20 - La ICANN debe aumentar la transparencia de la información sobre la organización y el presupuesto relacionado con la implementación del Marco de SSR y la realización de funciones relacionadas con SSR.	Esto se implementará a través del Marco de SSR para FY14 y el Plan operativo y presupuesto para FY14. La nueva página de Panel de gestión del Equipo de seguridad también se utilizará para abordar esta recomendación.

Excelencia en las Operaciones – Estructura

Recomendación del Equipo revisor de SSR	Implementación y Estatus
#21 - La ICANN debe establecer un proceso interno más estructurado para mostrar la manera en que las decisiones de la organización y presupuesto se relacionan con el Marco de SSR, inclusive el análisis fundamental de costo-beneficio.	La ICANN utilizará la labor de Entregas de gestión como el proceso estructurado para la identificación de las decisiones organizacionales y presupuestarias y en forma alineada con las actividades de SSR del Marco anual. Esto será implementado en el Plan operativo y Presupuesto FY14.

Excelencia en las Operaciones – Normalización y Cumplimiento

Recomendación del Equipo de SSR	Implementación y Estatus
#9 –Para sus responsabilidades operacionales, la ICANN debe	La implementación de las DNSSEC en la raíz, por parte de la ICANN, ha logrado la certificación SysTrust

evaluar las opciones de certificación con estándares internacionales comúnmente aceptados (por ejemplo, ITIL, ISO y SAS-70). La ICANN debe publicar un claro plan de acción hacia la certificación.	[enlace: https://www.iana.org/dnssec/systrust y https://cert.webtrust.org/icann.html]. El Equipo de funciones de la IANA así como los equipos de IT y Operaciones del DNS de la ICANN está conduciendo otros procesos de certificación, con el apoyo del Equipo de seguridad.
#10 - La ICANN debe continuar sus esfuerzos para incrementar la ejecución del cumplimiento contractual y proporcionar los recursos adecuados para esta función. La ICANN también debe desarrollar e implementar un proceso más estructurado para el seguimiento de las cuestiones e investigaciones de cumplimiento.	Esta recomendación está siendo conducida por el Equipo de cumplimiento de la ICANN y mediante la implementación de las recomendaciones del Equipo revisor de WHOIS.

Excelencia en las Operaciones – nTLDs

Recomendación del Equipo revisor de SSR	Implementación y Estatus
#11 - La ICANN debe finalizar e implementar medidas de éxito para los nuevos gTLDs y avance acelerado de IDN, que expresamente se relacionen con sus objetivos del programa en lo que respecta a SSR, incluyendo medidas para la efectividad de los mecanismos de mitigación del abuso de nombres de dominio.	El personal está explorando todas las implicaciones de esta Recomendación. El Equipo de seguridad espera que esto involucre la colaboración de la comunidad y el personal para una implementación completa. Como esto se relaciona con la Revisión y métricas de competencia, la confianza del consumidor y la elección del consumidor, tanto para los nuevos gTLDs e IDN ccTLDs (Dominios de Nivel Superior con Código de País de Nombres de Dominio Internacionalizados) delegados a través del proceso de Avance acelerado de IDN ccTLD, habrá un compromiso con los grupos de interés de toda la comunidad. El objetivo de esta recomendación es establecer mecanismos relacionados con la mitigación del abuso de nombres de dominio. El personal está apoyando la labor sobre indicadores de abuso, realizada por parte de los comités asesores y la comunidad.
#22 - La ICANN debe publicar, monitorear y actualizar la documentación sobre recursos de la organización y presupuestos necesarios para gestionar las cuestiones de SSR, conjuntamente con la introducción de nuevos gTLDs.	Esto está relacionado con la Recomendación 21 (las decisiones presupuestarias y organizacionales), así como con desarrollar un monitoreo con la introducción de nuevos gTLDs.

Excelencia en las Operaciones – Gestión de riesgos y Mitigación de Amenazas

Recomendación del Equipo Revisor de SSR	Implementación y Estatus
#25 – La ICANN debe establecer mecanismos para la identificación de riesgos y factores estratégicos —tanto a corto como a largo plazo—, en su Marco para la gestión de riesgos.	Esta recomendación está en marcha y vinculada con el marco de Gestión de Riesgos de la Recomendación 26.
#26 –La ICANN debe priorizar la oportuna compleción de un Marco para la gestión de riesgos.	Esta recomendación está en marcha. La ICANN ha conservado la Gobernanza Westlake para ayudar con su proyecto de Marco para la Gestión de Riesgos del DNS. Westlake realizó una sesión abierta en Toronto, y ofrecerá en un futuro próximo una versión preliminar del marco, así como también suministrará una sesión informativa sobre el concepto del marco, en la reunión que la ICANN celebrará en Beijing.
#27 –El Marco para la gestión de riesgos de la ICANN debe ser integral, dentro del área de alcance y misiones limitadas de SSR.	El Marco para la Gestión de Riesgos estará alineado con las actividades de la ICANN en apoyo a su misión técnica y a la comunidad. Esto será integral en ese ámbito, y se cumplirá con la entrega del Marco indicado en la Recomendación 26.
#15 –La ICANN debe actuar como facilitador en la divulgación y diseminación de las amenazas a la seguridad del DNS y las técnicas de mitigación.	El Equipo de seguridad de la ICANN está elaborando una versión preliminar del documento de Divulgación Coordinada. El personal colabora con los operadores y entidades de confianza de la comunidad sobre las amenazas a la seguridad del DNS y las técnicas de mitigación. Esto está relacionado con la Recomendación 28.
#28 –La ICANN debe continuar comprometiéndose activamente en la detección, mitigación y participación en los esfuerzos de distribución de información sobre amenazas e incidentes.	Esta recomendación respalda una continuación de los esfuerzos de la ICANN, incluyendo el monitoreo de la zona raíz, la detección y mitigación de amenazas relacionadas con las operaciones del DNS de la ICANN y las amenazas e incidentes generales del DNS.

Internacionalización – Terminología y Relaciones

Recomendación del Equipo revisor de SSR	Implementación y Estatus
#3 - Una vez que la ICANN publique una declaración basada en el consenso de su área de alcance de SSR y su misión técnica limitada, dicha Corporación debe utilizar en todos los materiales una terminología y descripciones coherentes con esta declaración.	El Equipo de seguridad trabajará a través de la organización para utilizar una terminología coherente y descripciones relacionadas con el rol y el alcance de SSR de la ICANN, en todos los materiales de dicha Corporación. Un primer paso es llevar a cabo la capacitación con el personal de la ICANN, luego ofrecer un seminario para la participación de la comunidad. También utilizaremos esta terminología y descripción en las presentaciones y participaciones de la ICANN.

#4 - La ICANN debe documentar y definir claramente la naturaleza de las relaciones de SSR que tiene dentro de su comunidad, a fin de proporcionar un único punto focal para la comprensión de las interdependencias entre las organizaciones.	El trabajo ha comenzado para documentar y definir estas relaciones. La visualización de las funciones de seguridad de la ICANN se utilizará para asignar relaciones con la coordinación y funciones de colaboración, conocimiento de amenazas y áreas técnicas de participación.
#5 - La ICANN debe utilizar la definición de sus relaciones de SSR para mantener acuerdos de trabajo eficaces y para demostrar la manera en que estas relaciones son utilizadas para el logro de cada objetivo de SSR.	El Equipo de seguridad trabajará con el Equipo multisectorial de participación mundial de la ICANN para mantener y mejorar la eficacia de los acuerdos y relaciones de trabajo. El Equipo de seguridad ha establecido relaciones con los organismos de orden público y comunidad de seguridad operacional en todo el mundo, y ha proporcionado entrenamiento pasado en la República Checa, Francia, Países Bajos, Reino Unido, EE.UU., entre otros.

Internacionalización – Difusión y Participación

Recomendación del Equipo revisor de SSR	Implementación y Estatus
#14 –La ICANN debe garantizar que sus actividades de divulgación relacionadas con SSR evolucionen continuamente para permanecer relevantes, oportunas y adecuadas.	Las actividades de divulgación se han ampliado y serán revisadas en forma anual. El Equipo de seguridad ofrece una función de servicio al Equipo multisectorial de participación mundial de la ICANN, en calidad de expertos en la materia, y una función de servicio a la comunidad en la difusión, participación y compromiso en materia de SSR.
#16 –La ICANN debe continuar sus esfuerzos de divulgación para ampliar la participación y aportes de la comunidad al proceso de desarrollo del Marco de SSR. La ICANN también debe establecer un procedimiento para obtener aportes más sistemáticos por parte de otros participantes del ecosistema.	Las actividades y procesos de difusión se han ampliado y serán examinadas en forma anual. La labor continua del Equipo de seguridad con las comunidades de seguridad tal como APWG, MAAWG (Grupo de Trabajo contra el Abuso de Mensajería) ha dado lugar a la participación de los miembros de esas comunidades en el SSAC. A través del compromiso con ICLN y CCI, el Equipo de seguridad hace hincapié en el valor de los enfoques multisectoriales en los problemas de seguridad informática. Esto se relaciona con las Recomendaciones de 4, 5 y 14. El Equipo de seguridad respalda a una variedad de iniciativas de desarrollo de capacidades a petición de las partes interesadas, tal como la formación en DNSSEC, la capacitación de respuesta a ataques y contingencias de ccTLD, la capacitación a los organismos de orden pública, la promoción en las reuniones del Grupo de operadores de red, tal como CaribNOG o MENOG, entre otros.

Evolución del Modelo de Múltiples Partes Interesadas

Recomendación del Equipo revisor de SSR	Implementación y Estatus

#6 - La ICANN debe publicar un documento que establezca claramente los roles y responsabilidades, tanto para el SSAC como para el RSSAC, a fin de delinear claramente las actividades de ambos.	Esta recomendación requerirá de la colaboración del personal y de la comunidad. Para realizar un seguimiento de esto, se lo ha dividido en 6A [SSAC] y 6B [RSSAC]. 6A – Los roles y responsabilidades del SSACC están definidos en los Procedimientos operativos de dicho Comité. El SSAC está examinando sus procedimientos operativos para el año 2013 y también está interesado en adaptar estos roles y responsabilidades del RSSAC. 6B – Los roles y responsabilidades del RSSAC están siendo elaborados, luego de finalizar el período de comentarios públicos sobre las enmiendas propuestas a los Estatutos de la ICANN respecto al propósito de dicho Comité. Véase http://www.icann.org/en/news/public-comment/bylaws-03jan13-en.htm.
#12 –La ICANN debe trabajar con la comunidad para identificar las mejores prácticas recomendadas en relación a SSR, así como respaldar la implementación de tales prácticas a través de contratos, acuerdos y MoUs (memorandos de entendimiento) u otros mecanismos.	La implementación de la Recomendación 12 involucrará la colaboración del personal y de la comunidad. Un mayor debate tomará lugar a este respecto, en la reunión que la ICANN celebrará en Beijing, en un Panel de Expertos en Seguridad del DNS y con el Grupo de Trabajo Técnico de la ccNSO, sobre las mejores prácticas no contractuales. El Equipo de seguridad ha trabajado con el Comité de Políticas de Internet del APWG para publicar recomendaciones para la protección de aplicaciones web, ha participado en la elaboración de recursos para la toma de consciencia respecto a la seguridad (a través de las actividades de SANS Securethehuman.org y con Stop.Think.Connect NCA). El actual período de comentarios públicos sobre la versión revisada del acuerdo de registro de nuevos gTLD (véase http://www.icann.org/en/news/public-comment/base-agreement-05feb13-en.htm) contiene un texto adicional sobre las mejores prácticas recomendadas.
#13 –La ICANN debe alentar a todas las Organizaciones de apoyo a desarrollar y publicar las mejores prácticas relacionadas con SSR para sus miembros.	Esta recomendación involucrará la colaboración del personal y de la comunidad a través de la ASO, la ccNSO y la GNSO sobre la idoneidad de las mejores prácticas recomendadas en relación a los identificadores únicos en sus respectivos roles.
#19 - La ICANN debe establecer un proceso que permita a la comunidad realizar un seguimiento de la implementación del Marco de SSR. La información debe ser proporcionada con la claridad suficiente como para que la comunidad pueda realizar un	El Equipo de seguridad pronto lanzará un Panel de gestión en su página, el cual mostrará el seguimiento del estatus tanto del Marco de SSR como de las iniciativas de SSR de la ICANN.

seguimiento de la ejecución de las responsabilidades de SSR de la ICANN, sin dañar la capacidad de la ICANN para operar eficientemente.	
#23 - La ICANN debe proporcionar los recursos adecuados para los grupos de trabajo y comités asesores relacionados con SSR, en consonancia con las demandas establecidas sobre ellos. La ICANN también debe garantizar que las decisiones adoptadas por los grupos de trabajo y comités asesores se alcancen de manera objetiva, libre de presiones externas o internas.	El personal está llevando a cabo un inventario [23A] de la actividad en los grupos de trabajo y comités asesores existentes relacionados con SSR (SSAC y RSSAC). Esto será seguido por una descripción o documentación del proceso presupuestario para aportes de las SOs y ACs [23B]. 23C se describirá un proceso operativo estándar para demostrar que las decisiones de las SOs/ACs/grupos de trabajo sean alcanzadas de manera objetiva.

SSR RT Recommendations Tracking – February 2013

Recommendation	FY 13 T1	T2	T3	FY 14 T1	T2	T3	FY 15 T1	T2	T3
Rec 1 – Clear statement of ICANN's SSR role and remit	Published	Revise	Update						
Rec 2 – Role & remit review in 2015								Review	Publish
Rec 3 – Use consistent terminology	Develop	Ongoing							
Rec 4 – Document & define SSR relationships		Develop	Publish						
Rec 5 – Use SSR relationships for effective working	Ongoing	Ongoing	Ongoing						
Rec 6 – Roles for SSAC (6A) & RSSAC (6B)		Publish							
Rec 7 – Build from SSR Framework, clear objectives & priorities	Develop	Publish	Expected Complete	Reporting					
Rec 8 - Strategic Plan & SSR Framework alignment		Publish	Refine						
Rec 9 – Assess certification options, publish roadmap		Develop	Publish						
Rec 10 – Process for monitoring compliance & investigations (see Whois RT Implementation)		Whois RT Recs							
Rec 11 – Measures for success in nTLD & IDN FT re SSR			Develop	Publish			AoC CCR		
Rec 12 – w/Community, SSR-related best practices	Engage	Discuss							
Rec 13 – Encourage SOs/SGs to develop & publish SSR-related best practices			Expected Complete						
Rec 14 – Evolving SSR outreach		Publish	ongoing	ongoing	review	publish	ongoing	ongoing	
Rec 15 – Facilitate responsible disclosure of threats		Draft	Ongoing	X					
Rec 16 – Outreach w community; process for input		Publish	ongoing	ongoing	review	publish	ongoing	ongoing	
Rec 17 – Mapping activities to SSR Framework		Publish	X	Reporting					
Rec 18 (Implemented w FY 13 SSR Framework) – Annual review of SSR Framework	Complete								
Rec 19 – Dashboard for SSR Framework			Publish	Reporting					
Rec 20 – Transparency on SSR budget			Publish	ongoing					
Rec 21 – Show how budget & op decisions relate to SSR			Publish						
Rec 22 – Documenting mgmt. of SSR issues with operational readiness from introduction of nTLDs		Develop	Publish						
Rec 23 – Appropriate resources for SSR-related WGs & ACs		FY 14 Budget	Budget approx						
Rec 24 (Implemented w FY 13 SSR Framework) – Define Security team roles	Complete								
Rec 25 – DNS Risk Management Framework	Consultant	Draft	Publish	Assess	work	work	Review		
Rec 26 – Prioritizing completion of DNS RMF		Publish	Approx						
Rec 27 – DNS RMF covers IANA, L-root, other functions				Assess	work	work	Review		
Rec 28 – Active engagement in threat detection & mitigation	Underway	X							

Gráfico 8 – Seguimiento de las Recomendaciones del Equipo Revisor de SSR

Apéndice B – Informe de Estatus de FY13

Área General	Programa/Iniciativa	Estatus
Participación de Seguridad a nivel mundial	Compromiso con la comunidad más amplia, empresas, comunidad académica, comunidad técnica y organismos de orden público sobre temas de Seguridad del DNS	Se realizó el 4to Simposio Mundial de SSR del DNS, conjuntamente con el APWG en eCOS, Puerto Rico, octubre de 2012
		Talleres sobre iniciativas contra la delincuencia informática del Commonwealth en las reuniones de la ICANN en Costa Rica y Praga, Grupo directivo CCI y reuniones de EMG
		BlackHat/Defcon en julio de 2012
		Foro de Gobernanza de Internet y eventos regionales de IGF
		Discurso a Unidad Constitutiva Empresarial en Washington DC y contribución al Boletín Informativo de dicha Unidad para la reunión que la ICANN celebró en Toronto
Colaboración	Mayor respaldo para las herramientas de medición e indicadores del DNS, tal como RIPE NCC's ATLAS	Contribución a RIPE NCC para un mayor desarrollo de los nodos ATLAS y análisis de datos. https://atlas.ripe.net/
	Automatización de la zona raíz	El sistema de Gestión de la Zona Raíz (RZM) utilizado por la IANA con la NTIA (Administración Nacional de Telecomunicaciones e Información) y Verisign cumplió un año en agosto de 2012 (véase http://blog.icann.org/2012/08/rzm-is-one-year-old/). El Equipo de la IANA está trabajando en procesos de seguridad adicionales, tales como un sistema de Notificación segura. Véase http://www.icann.org/en/news/public-comment/iana-secure-notification-12dec12-en.htm.
	Capacitación técnica con los organismos de orden público y la comunidad de seguridad operacional	El Equipo de seguridad facilitó el orden público en las reuniones que la ICANN celebró en Praga y en Toronto, a la vez que proveyó una formación sobre DNS para Europol, en los Países Bajos, y para SOCA, OFT y la Policía Metropolitana del Reino Unido.
	Comité Asesor de Seguridad y Estabilidad	Colaboración con el SSAC en los talleres sobre DNSSEC realizados en las reuniones de la ICANN; equipos de trabajo, asesoramientos e informes del SSAC. En FY13, la labor del SSAC ha sido considerable.
	Apoyo al Grupo de trabajo para el Análisis de la seguridad y estabilidad del DNS (DSSA)	En agosto de 2012, el DSSA completó su Informe de la Fase 1. http://www.icann.org/en/news/public-comment/dssa-phase-1-report-14aug12-en.htm. El DSSA se volverá a reunir durante la reunión que la ICANN celebrará en Beijing. La ICANN también participó en la Gobernanza Westlake, con actividades del Marco para la gestión de riesgos del DNS.
	Evolución Técnica de	En febrero de 2013, la ICANN anunció a un grupo de expertos en

	WHOIS	Servicios de directorio de gTLD (https://www.icann.org/en/news/announcements/announcement-14feb13-en.htm). En octubre de 2012, la ICANN anunció que se había comprometido con el CNNIC (Centro de Información de la Red de Internet de China) para implementar un servidor de WHOIS RESTful de fuente abierta, http://blog.icann.org/2012/10/cnnic-selected-to-implement-an-open-source-restful-whois-server/.
	Desarrollo de políticas – Abuso de registración; Acuerdo de acreditación de registradores	La ICANN tiene abierto un período de comentarios públicos sobre un informe preliminar sobre la Uniformidad en la Presentación de Informes, https://www.icann.org/en/news/public-comment/uofr-20feb13-en.htm. Este informe siguió a la acción del Consejo de la GNSO en respuesta al Grupo de trabajo sobre abuso de registración. En el Acuerdo de Acreditación de Registradores, las negociaciones continúan. El día 7 de febrero de 2013, el CEO Fadi Chehade, ofreció una actualización http://blog.icann.org/2013/02/registrar-accreditation-agreement-negotiation-session/.
	DNSSEC – grupo de trabajo para el despliegue de claves en el SSAC	El grupo de trabajo del SSAC para el despliegue de claves continúa sus actividades en 2013. En la reunión que la ICANN celebrará en Beijing se brindará información adicional. En Culpeper, Virginia y en El Segundo, California se realizaron ceremonias exitosas de claves.
	DNSSEC – Auditoría de SysTrust	La certificación de las DNSSEC por parte de SysTrust está disponible en https://www.iana.org/dnssec/systrust.
	Capacitación sobre DNSSEC con la comunidad	La ICANN respaldó la capacitación sobre DNSSEC en Colombia, Perú, Paraguay, Hong Kong, Chile y cuenta con formaciones programadas para el Líbano (marzo de 2013) y la República Tunecina (abril de 2013).
	Flexibilidad de la raíz-L	La ICANN ha apoyado el crecimiento y la distribución de las instancias de la raíz-L a nivel mundial. En particular, se han anunciado asociaciones para ofrecer instancias de la raíz-L en África con AfriNIC (Centro Africano de Información de Redes), en América Latina y el Caribe con LACNIC (Registro de Direcciones de Internet de América Latina y el Caribe), en Brasil con CGI.Br, en Corea con KISA, así como en otros lugares.
Programas de Seguridad Corporativa	Mejorar los procesos y seguridad de redes internas de la ICANN	El Equipo de seguridad ha estado trabajando con el Departamento de IT de la ICANN para fortalecer las redes internas de dicha Corporación. El Equipo ha apoyado la capacitación de SANS para el personal de IT y ha ofrecido formaciones básicas de seguridad para el personal de la ICANN en Los Ángeles and Bruselas.
	Mejorar la continuidad de negocios y realizar ejercicios internos	Se ha apoyado la seguridad con ejercicios de flexibilidad de la raíz y de los procesos de comunicación interna.
	Seguridad de reuniones – evaluación de riesgos, seguridad del viajero	Realizó evaluaciones en los emplazamientos de la ICANN; proporcionó salud y servicios de emergencia en el lugar, durante las reuniones celebradas por la ICANN (ISOS)
Interorganizacional	Apoyo a operaciones de los nuevos gTLD	Proporcionó apoyo para el equipo de nuevos gTLD con el establecimiento de prioridades y procesos de revisión
		Asistencia con el sistema de revisión previa a la delegación, con .SE, http://www.icann.org/en/news/announcements/announcement-

		21dec12-en.htm.
	Contractual Cumplimiento	El Equipo de cumplimiento ha continuado creciendo en FY13, publicando su plan de auditoría (véase http://www.icann.org/en/resources/compliance/audits)
	Programa de IDN	Participación en reuniones de UNGEGN/UNCSGN en Nueva York, en los meses de julio y agosto de 2012 en la Sede Central de las Naciones Unidas, apoyando la continua labor en el Programa de variantes de IDN
	Iniciativas de Gestión de riesgos	La ICANN ha participado en la Gobernanza Westlake sobre la iniciativa del Marco para la gestión de riesgos del DNS. Durante la reunión que la ICANN celebrará en Beijing se ofrecerá un mayor desarrollo sobre el progreso de Westlake.

El trabajo en el compromiso técnico realizado por el Equipo de seguridad de la ICANN es colaborativo. Hacemos esto para el beneficio de la comunidad más amplia. Es agradable recibir cartas de apoyo para nuestro trabajo, aunque no es algo que buscamos con el fin de sólo recolectar declaraciones de felicitación. Las siguientes cartas son una muestra del respaldo que la ICANN ha recibido en FY13, por su compromiso de seguridad en la comunidad.

COMNET
Foundation for ICT Development

www.comnet.org.mt

ICANN Security Team

12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

2nd July 2012

Re: Commonwealth Cybercrime Initiative

Dear ICANN Security Team,

We would like to express our gratitude and thanks for providing the Commonwealth Cybercrime Initiative the opportunity to host another workshop at the ICANN Meeting in Prague. The Event in Costa Rica was a big success and to follow with another space in Prague was excellent as it provided continuity. We sincerely appreciate the time and resources that ICANN has invested to provide a platform for the Initiative to raise its profile amongst the ICANN community.

Our Prague workshop resulted in two expressions of interest in the CCI from two governments in Africa and we also had excellent additions to our expert resource repository. We are already working on translating these expressions of interest into meaningful activity on the ground.

We are especially grateful of Mr Dave Piscitello's contributions in his capacity as ICANN representative on the CCI Steering Group. Mr Piscitello's involvement, in a very short time resulted in very tangible achievements for the Initiative.

ICANN's support of the Commonwealth Cybercrime Initiative has proven invaluable and we look forward to the opportunity to present the CCI at the next ICANN meeting in Canada if scheduling allows.

Thank you once again, and we look forward to our continued collaboration.

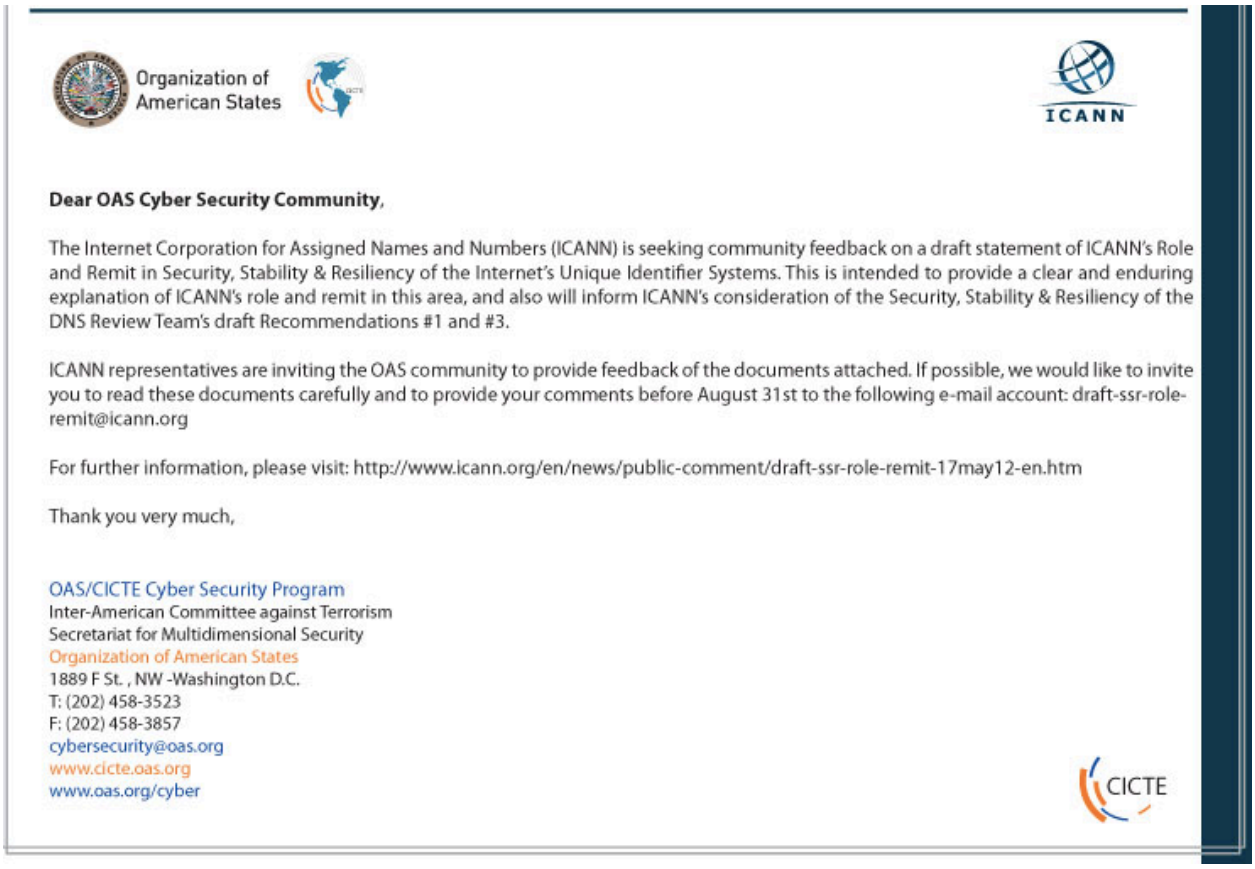
Yours,

Joseph V. Tabone

Chairman CCI Secretariat

Alfir, Reggie Miller Street, Gzira, GZR 1541, Malta | t: (356) 2132 3393 | f: (356) 2132 3390 | e: info@comnet.org.mt

Apéndice C – Carta de COMNET a la ICANN



Organization of American States

ICANN

Dear OAS Cyber Security Community,

The Internet Corporation for Assigned Names and Numbers (ICANN) is seeking community feedback on a draft statement of ICANN's Role and Remit in Security, Stability & Resiliency of the Internet's Unique Identifier Systems. This is intended to provide a clear and enduring explanation of ICANN's role and remit in this area, and also will inform ICANN's consideration of the Security, Stability & Resiliency of the DNS Review Team's draft Recommendations #1 and #3.

ICANN representatives are inviting the OAS community to provide feedback of the documents attached. If possible, we would like to invite you to read these documents carefully and to provide your comments before August 31st to the following e-mail account: draft-ssr-role-remit@icann.org

For further information, please visit: http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm

Thank you very much,

OAS/CICTE Cyber Security Program
Inter-American Committee against Terrorism
Secretariat for Multidimensional Security
Organization of American States
1889 F St. , NW -Washington D.C.
T: (202) 458-3523
F: (202) 458-3857
cybersecurity@oas.org
www.cicte.oas.org
www.oas.org/cyber

CICTE

Apéndice D – Solicitud de Comentarios Públicos a la Comunidad OAS

CARIBBEAN TELECOMMUNICATIONS UNION
3rd Floor, Victoria Park Suites, 14-17 Victoria Square, Port of Spain, Trinidad & Tobago, W.I.
Tel: (868)627 0281/0347 Fax: (868) 623 1623 E-Mail: ctunion@ctu.int Website: www.ctu.int

7th September, 2012

Mr. Patrick Jones
Senior Manager, Security
Internet Corporation for Assigned Names and Numbers (ICANN)
1101 New York Ave
New York Avenue
Washington DC 20005
USA

Dear Mr. Jones,

Expression of Appreciation

On behalf of the Caribbean Telecommunications Union (CTU), I would like to express our sincere appreciation to you for participating in the CTU's 8th Caribbean Internet Governance Forum, which took place from the 29th to 30th August, 2012 at the Bay Gardens Hotel, Castries, St. Lucia.

Thank you for your presentation on "DNSSEC, Collaboration and Training" which was well received by the audience.

I take this opportunity to re-affirm the CTU's commitment to Caribbean ICT development and look forward to an ongoing partnership with ICANN in supporting Caribbean countries as they seek to leverage the power of ICT for social and economic development.

Sincerely,

Bernadette Lewis
SECRETARY GENERAL

Apéndice E – Carta de la Unión de Telecomunicaciones del Caribe a la ICANN

The Hague, 3 January 2013

Ref: 647233

Dr Stephen D. Crocker
Internet Corporation for Assigned Names and Numbers (ICANN)
12025 Waterfront Drive, Suite 300
Los Angeles CA 90094-2536
USA

Dear Dr Crocker, Dear Steve!

Dave Piscitello of ICANN visited us in The Hague on 12 December. The purpose of this meeting was for Dave to be informed on the development of the new European Cybercrime Centre (EC3), ourselves to be aware of ICANN cooperation with law enforcement and all of us to see how this could specifically work between ICANN and the EC3.

We were all pleased by the constructive dialogue and positive outcomes of the meeting. There appear clear opportunities for the EC3 to play the role of facilitator with ICANN for MS law enforcement, both with respect to their views on internet governance and in training to improve investigative capabilities. We will be in contact with Dave over the specifics concerning this in the coming weeks.

The EC3 is very appreciative of this initiative between our two organisations and hope that you can lend your full support to it. Thank you very much.

Yours sincerely,

Troels Oerting
Assistant Director
Head of European Cybercrime Centre (EC3)

EDOC#647233

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

P.O. Box 908 50
2509 LW The Hague
The Netherlands

Phone: +31(0)70 302 50 00
Fax: +31(0)70 345 58 96
www.europol.europa.eu

Apéndice F – Carta de EC3 a la ICANN