Iniciativas Propuestas para la Mejora de la Seguridad, Estabilidad y Flexibilidad del Sistema de Nombres de Dominio (DNS)

Presentado por la

Corporación para la Asignación de Números y Nombres en Internet (ICANN)

Para la Recepción de Comentarios Públicos

12 de febrero de 2010

Iniciativas Propuestas para la Mejora de la Seguridad, Estabilidad y Flexibilidad del Sistema de Nombres de Dominio (DNS)

1. Descripción General

Este documento presenta los fundamentos, características clave y proyección de costos de dos iniciativas estratégicas relacionadas con la seguridad, estabilidad y flexibilidad/capacidad de recuperación del Sistema de Nombres de Dominio (DNS), que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) considera necesarias para cumplir con sus obligaciones en virtud de sus estatutos, de la Afirmación de Compromisos 2009 y de su Plan Estratégico 2010-2013. Este documento proporciona una base para que estas iniciativas propuestas, las responsabilidades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en establecer las prestaciones propuestas y la forma en que la comunidad puede proceder en la organización de los esfuerzos para respaldar a tales iniciativas, sean debatidas por las múltiples partes interesadas. Se han identificado personal de alto nivel e implicancias financieras; sin embargo, las alternativas de financiación para estas iniciativas no han sido analizadas.

Nota: Estas iniciativas se proponen como esfuerzos más allá de aquellos señalados en el marco conceptual y de trabajo del Plan Operativo y Presupuesto FY11 de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), publicado en la reunión de Nairobi para su debate.

2. Supuestos

2.1 El Sistema de Nombres de Dominio se ha convertido en un elemento fundamental, en el servicio de empoderamiento que subyace a Internet. El Sistema de Nombres de Dominio (DNS) permite la resolución de nombres para los usuarios de la Web y también mantiene el correo electrónico, la mensajería de texto, los servicios de voz basados en Internet y otros servicios y protocolos clave de Internet. Al mismo tiempo, el Sistema de Nombres de Dominio (DNS) existe en un entorno de crecientes amenazas y riesgos. Las operaciones técnicas del sistema están expuestas a una serie de ataques tales como los Ataques Distribuidos de Denegación de Servicio (DDoS) contra servidores y codificadores (*resolvers*) de nombres a niveles de hasta e incluyendo los servidores de nombres raíz, los ataques de envenenamiento de caché que impactan la integridad de la resolución del Sistema de Nombres de Dominio (DNS) según lo descripto por el investigador de seguridad Dan Kaminsky; y otros métodos como la ingeniería social que permite a los ataques maliciosos desviar o utilizar indebidamente los servicios del Sistema de Nombres de Dominio (DNS). En forma adicional, los malandrines y delincuentes se aprovechan de la dependencia del usuario en el Sistema de Nombres de

Dominio (DNS) y utilizan el sistema de diversas formas para llevar a cabo una amplia gama de actividades maliciosas.

2.2 Actualmente, la comunidad de operadores que ofrece servicios del Sistema de Nombres de Dominio (DNS) colabora activamente con los vendedores, investigadores de seguridad, organismos de orden público y equipos de respuesta, para reaccionar ante amenazas emergentes de un modo ampliamente *ad-hoc*. Dentro de la comunidad del Sistema de Nombres de Dominio (DNS) existen iniciativas para mejorar el intercambio de información, para identificar la actividad maliciosa y para mejorar la colaboración en relación con los Ataques Distribuidos de Denegación de Servicio (DDoS) y con otros ataques integrales. En general, estos esfuerzos de colaboración implican esfuerzos de los miembros de las comunidades del Sistema de Nombres de Dominio (DNS) y de seguridad, para unirse voluntariamente a fin de afrontar nuevas situaciones. El año pasado se realizaron varias convocatorias[1] para tomar acción en el abordaje y mitigación sistémicos de los riesgos del Sistema de Nombres de Dominio (DNS). La frecuencia y la gravedad de estas convocatorias para tomar acción exponen una necesidad creciente de analizar el riesgo del sistema a nivel integral, así como de realizar una planificación de contingencia y una capacidad de respuesta permanentes.

2.3 Los esfuerzos actuales para hacer frente a la gama de amenazas y riesgos para el Sistema de Nombres de Dominio (DNS) no están enfocados en forma sistémica. A nivel operativo, los operadores de seguridad expertos y con buenos recursos dentro del Sistema de Nombres de Dominio (DNS) han desarrollado mecanismos fuertes para entender las amenazas y tomar medidas para mitigar los riesgos para ellos y sus clientes. Sin embargo, la colaboración en esta área no suele extenderse a los operadores del Sistema de Nombres de Dominio (DNS) que cuentan con menos capacidades y menos recursos ni a otras partes interesadas que no son conscientes de las amenazas y riesgos y que por lo tanto carecen de la habilidad para responder adecuadamente al momento de descubrir esas amenazas a la seguridad, estabilidad y flexibilidad. Más aún, los esfuerzos actuales han demostrado que se necesita mantener el enfoque sobre la supervisión, respuesta y solución para enfrentarse a amenazas que no son susceptibles de soluciones técnicas fácilmente localizables. A un nivel superior, el Sistema de Nombres de Dominio (DNS) carece de puntos focales integrales para la rendición de cuentas en relación con las funciones clave en la evaluación de riesgos, la planificación de contingencia y ejercicios, así como con una respuesta dedicada y sostenida. Tales actividades deben mirar al Sistema de Nombres de Dominio (DNS) de manera integral y responder a las necesidades de los distintos componentes y operadores.

2.4 Fundamentalmente, este tipo de funciones no puede recaer enteramente sobre los esfuerzos de voluntarios que actúan sin un apoyo organizacional dedicado, sin enfoques operacionales refinados y sin compromisos de recursos a largo plazo. Los esfuerzos para

[1] Véase http://www.enisa.europa.eu/media/press-releases/improving-resilience-3-tips, y http://www.enisa.europa.eu/media/press-releases/guide-to-mitigate-vulnerabilities-threats-cyber-attacks, y http://www.it-scc.org/documents/itscc/IT-SCC_ITSRA_Release_08_21_09_clean_final2.pdf.

garantizar la estabilidad y flexibilidad/capacidad de recuperación del Sistema de Nombres de Dominio (DNS) debe alcanzar niveles de eficacia y responsabilidad acordes a otros aspectos críticos de la infraestructura de comunicaciones que requieren niveles similares de inversión en apoyo y personal de tiempo completo.

3. Rol y Responsabilidades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN)

3.1 El Sistema de Nombres de Dominio (DNS) debe operar de forma segura, estable y flexible. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) cuenta con numerosos compromisos que le obligan a realizar esfuerzos para lograr este objetivo. El Artículo I de los Estatutos de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) establece: "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." La Afirmación de Compromisos 2009 (http://icann.org/en/announcements/announcement-30sep09-en.htm) afirma que el Sistema de Nombres de Dominio (DNS) desempeña una función crítica en el entorno de Internet y por lo tanto los riesgos relacionados con el funcionamiento deben ser manejados en forma apropiada. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) se ha comprometido a "preservar la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio (DNS)." En forma adicional, la Afirmación solicita a la Corporación para la Asignación de Números y Nombres en Internet (ICANN) que identifique las amenazas actuales y futuras y que realice la planificación de contingencia apropiada.

3.2 La consecuencia de estos compromisos para la Corporación para la Asignación de Números y Nombres en Internet (ICANN) es clara. La Afirmación de Compromisos requiere que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) emprenda esfuerzos colaborativos para identificar y mitigar los riesgos para la seguridad y flexibilidad a través de un sistema distribuido del Sistema de Nombres de Dominio (DNS), lo cual incluye una amplia gama de partes interesadas que operan y usan los servicios del Sistema de Nombres de Dominio (DNS). [2] Debido a la naturaleza del Sistema de Nombres de Dominio (DNS), las operaciones confiables y flexibles del sistema de servidores raíz y de los dominios de alto nivel deben ser para la Corporación para la Asignación de Números y Nombres en Internet (ICANN) una prioridad de primer nivel. El crecimiento del Sistema de Nombres de Dominio (DNS) a través del incremento natural en el uso y la introducción de nuevas tecnologías y propuestas para establecer

[2] Del modo que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) planea abordar su rol en la gestión de los riesgos para la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio (DNS), no aborda las cuestiones relacionadas con la competencia de seguridad nacional entre estados en el ámbito de la guerra cibernética o de espionaje o control de dirección de los contenidos alojados en el Internet, como se aborda en el Plan para la Mejora de la Seguridad, Estabilidad y Flexibilidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). Véase http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf.

los nuevos Dominios de Alto Nivel (TLD) —incluidos aquellos que utilizan Nombres de Dominio Internacionalizados—, exigen además que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) entienda e intente reducir los riesgos para el sistema. Es importante señalar que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha buscado mejorar la seguridad, estabilidad y flexibilidad/capacidad de recuperación del Sistema de Nombres de Dominio (DNS), desde su creación. El Plan para la Mejora de la Seguridad, Estabilidad y Flexibilidad de Internet de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) (http://www.icann.org/en/announcements/announcement-2-21may09-en.htm) aborda la amplia gama de programas y actividades existentes. Las iniciativas descriptas en este documento abordan esfuerzos adicionales que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) debe asumir para cumplir con estos compromisos.

3.3 Los imperativos para mejorar la comprensión y mitigación del riesgo sistémico para el Sistema de Nombres de Dominio (DNS) y hacer frente a sus compromisos, requerirán que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) colabore con la comunidad del Sistema de Nombres de Dominio (DNS) para iniciar un trabajo adicional que se base tanto en los esfuerzos realizados en el pasado como en la colaboración actual. A tal fin, el Plan Estratégico 2010-2013 de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) establece la mejora de la estabilidad, seguridad y flexibilidad del Sistema de Nombres de Dominio (DNS) como una de las cuatro áreas de enfoque de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) durante este período. Específicamente, el Plan Estratégico se refiere al requisito para que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) establezca un enfoque hacia un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT), así como hacia la planificación de contingencias y ejercicios para el Sistema de Nombres de Dominio (DNS). La Corporación para la Asignación de Números y Nombres en Internet (ICANN) busca avanzar para garantizar el establecimiento de enfoques integrales para la evaluación de riesgos, la planificación y ejercicios de contingencia frente a amenazas potenciales, así como para orquestar una capacidad de respuesta colaborativa ante emergencias a fin de mejorar la seguridad, estabilidad y flexibilidad/capacidad de recuperación del Sistema de Nombres de Dominio (DNS). La Corporación para la Asignación de Números y Nombres en Internet (ICANN) también tiene previsto iniciar esfuerzos para mejorar el sistema de medición del sistema en forma integral, de modo que la comunidad del Sistema de Nombres de Dominio (DNS) pueda obtener una comprensión más clara de la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio (DNS) a fin de anticipar los desafíos y poder responder con eficacia.

3.4 La posible utilidad y éxito operacional de las iniciativas debajo descriptas requerirán del apoyo y del compromiso de la comunidad. La revisión, retroalimentación y planificación de la comunidad relativas a la implementación de estas iniciativas serán integradas a la

planificación operacional y al proceso de presupuestación de la Corporación para la Asignación de Números y Nombres en Internet (ICANN).

4. Riesgos para el Funcionamiento del Sistema de Nombres de Dominio (DNS)

4.1 Al comenzar el año 2010, el ecosistema de Internet continúa siendo vibrante. Cada vez más, la actividad en Internet refleja el rango completo de motivaciones y conductas humanas. 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. El ecosistema también está amenazado por los crecientes niveles de actividad maliciosa llevados a cabo por una serie de actores diversos, con fuertes indicios de que la participación de organizaciones delictivas está creciendo rápidamente. El panorama de amenazas incluye el fraude, la extorsión y otras actividades ilícitas en línea —las cuales socavan la confianza del usuario en los servicios basados en Internet—, así como ataques de Denegación de Servicio (DoS) y otras actividades perturbadoras que desestabilizan la infraestructura de Internet. En particular, la capacidad de los agentes maliciosos para realizar ataques contra el funcionamiento del Sistema de Nombres de Dominio (DNS) en sí mismo —y la facilidad y frecuencia con la que estos actores utilizan tanto la resolución de nombres y los servicios de registración para permitir una serie de actividades maliciosas o delictivas—, presenta crecientes riesgos para el buen funcionamiento de Internet y llama a poner en duda la integridad y fiabilidad de Internet como una plataforma mundial de comunicaciones.

4.2 Existen tres categorías principales de riesgos para la seguridad, estabilidad y flexibilidad/capacidad de respuesta: actividades maliciosas/dolosas (ataques contra el Sistema de Nombres de Dominio —DNS— o ataques que explotan/se aprovechan de la resolución de nombres o los sistemas de registración), los riesgos técnicos para la estabilidad del Sistema de Nombres de Dominio (DNS) y los riesgos organizacionales relacionados con el Sistema de Nombres de Dominio (DNS).

4.2.1 Riegos de Actividad Maliciosa

4.2.1.1 Fundamentalmente, el riesgo principal de preocupación para la Corporación para la Asignación de Números y Nombres en Internet (ICANN) es la disponibilidad del Sistema de Nombres de Dominio (DNS) para resolver nombres y facilitar una amplia variedad de transacciones a través de Internet. Una amenaza importante para la disponibilidad puede provenir en forma de ataques de Denegación de Servicio (Dos) contra quienes operan los servicios del Sistema de Nombres de Dominio (DNS) en los distintos niveles de los sistemas. El impacto de los ataques de Denegación de Servicio (DoS) depende tanto de los tipos de servicios a los que se apunta como de la complejidad y el volumen de tráfico del ataque. Durante la última década, las operaciones de los servidores raíz —así como de los dominios de alto nivel (TLDs)—, han sido atacados en forma directa. Se destacan cuatro casos: 1) el 21 de octubre 2002, el primer caso documentado de un

ataque coordinado que se llevó a cabo contra los trece servidores raíz del Sistema de Nombres de Dominio (DNS) (http://d.root-servers.org/october21.txt); 2) en febrero de 2006 se llevaron a cabo ataques contra los servidores de nombre operados por un proveedor clave de servicios de nombre de Dominios de Alto Nivel (TLD) (http://www.icann.org/en/committees/security/dns-ddos-advisory-31mar06.pdf); 3) en febrero de 2007 se realizó un ataque contra de seis de los trece servidores raíz del Sistema de Nombres de Dominio (DNS) (http://www.icann.org/en/announcements/factsheet-dns-attack-08mar07.pdf); 4), más recientemente, en diciembre de 2009, nuevamente los titulares fueron dedicados a ataques de Denegación de Servicio (DoS) contra proveedores del Sistema de Nombres de Dominio (DNS), al realizarse un ataque contra el servicio UltraDNS de NeuStar, afectado a muchos sitios de comercio electrónico (http://www.cnn.com/2009/TECH/12/24/cnet.ddos.attack/index.html). Este historial de ataques demuestra el constante incremento de los recursos disponibles para aquellos que realizan atentados, así como el aumento de la sofisticación de los perpetradores.

4.2.1.2 En forma continua se están realizando importantes esfuerzos para mitigar estos riesgos, en términos de proporcionar aprovisionamiento de ancho de banda para hacer frente a los Ataques Distribuidos de Denegación de Servicio (DDoS) y el establecimiento y despliegue de tecnologías y metodologías —tales como *anycasting*—, por las cuales los datos son transportados al destino mejor o más cercano. Como ejemplo de implementación de soluciones *anycast* el sistema de servidores raíz del Sistema de Nombres de Dominio (DNS) ha crecido de una presencia en trece localidades (sistemas) a una presencia en más de dos centenares de localidades (ver detalles en http://www.root-servers-org). También existen incrementos en los niveles de planificación y colaboración entre los operadores del Sistema de Nombres de Dominio (DNS) mediante la creación de organizaciones como el Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio (DNS-OARC) (http://www.dns-oarc.org), el Grupo de Seguridad de Registros de Internet (RISG) (http://registrysafety.org/website/) y los esfuerzos para entender los riesgos asociados con el Sistema de Nombres de Dominio (DNS) tales como el Simposio Mundial sobre Seguridad, Estabilidad y Flexibilidad del Sistema de Nombres de Dominio (http://www.gtisc.gatech.edu/pdf/DNS_SSR_Symposium_Summary_Report.pdf). Sin embargo, las amenazas también están aumentando a medida que redes de robots cada vez más grandes bajo el control de actores delictivos y maliciosos plantean el riesgo de ataques muy significativos, tanto en términos de complejidad como de escala. La planificación de esas perturbaciones debe también abordar la posibilidad de que los servicios del Sistema de Nombres de Dominio (DNS) sean interrumpidos como resultado de ataques malintencionados contra los sistemas sobre los cuales recae el Sistema de Nombres de Dominio (DNS), los cuales van desde la energía eléctrica hasta el enrutamiento de Internet.

4.2.1.3 El carácter abierto y distribuido de la operación del Sistema de Nombres de Dominio (DNS) junto con la administración ampliamente distribuida de los servidores de nombres

y codificadores (*resolvers*), expone a los usuarios a una serie de riesgos adicionales. El protocolo del Sistema de Nombres de Dominio (DNS) (sin el uso de extensiones de seguridad) es vulnerable a los ataques que emplean el desvío de consultas. Específicamente, el ataque devuelve información falsa en respuesta a una consulta del Sistema de Nombres de Dominio (DNS) (envenenamiento —*poisoning*— o desvío —*pharming*—) o devuelve información que es diferente a aquello intencionado por una autoridad de nombres de dominio (redirección o modificación de respuesta). Este tipo de ataques engañan a los usuarios del Sistema de Nombres de Dominio (DNS) en una gran variedad de formas: direccionando a los usuarios acceder a sitios web con contenido fraudulento o código malicioso, haciendo que los correos electrónicos parezcan provenir de fuentes falsificadas y demás. Las técnicas utilizadas para ejecutar los ataques que permitirían el envenenamiento sistemático de los cachés del Sistema de Nombres de Dominio (DNS) y por lo tanto, el desvío del tráfico de Internet ofrece la oportunidad de realizar actividades maliciosas que pueden plantear riesgos para la integridad del Sistema de Nombres de Dominio (DNS) en su conjunto.

4.2.1.4 Los servicios de registración de nombres de dominio son otro vector de ataque para los delincuentes. Los atacantes explotarán las debilidades técnicas (vulnerabilidades del sitio web) u operacionales de un registrador o registrante (personal que puede contar con ingeniería social) para obtener el control no autorizado a una cuenta de registración de nombres de dominio (para más detalles, véase el documento SAC040 http://www.icann.org/en/committees/security/sac040.pdf). Una vez en control de la cuenta de registración secuestrada, el atacante modifica la configuración del Sistema de Nombres de Dominio (DNS) de, potencialmente, todos los dominios en una cuenta secuestrada para que apunten a un servidor de nombre controlado por el atacante, dando al atacante el control de la resolución de nombres de dominio de Internet para el sitio web, correo electrónico y demás aplicaciones de Internet del dominio comprometido. Dichos ataques de secuestro de nombres de dominio o cuenta son utilizados para alterar sitios web, interrumpir los servicios de correo electrónico u otros servicios ofrecidos por el registrante, o para la captura de información confidencial o personal.

4.2.1.5 Mientras que el Sistema de Nombres de Dominio (DNS) está destinado a servir a los usuarios de Internet, lamentablemente también es explotado por inescrupulosos para facilitar una amplia gama de conductas delictivas y abusos. Esta consecuencia no intencionada se ejemplifica mejor de la manera en que el Sistema de Nombres de Dominio (DNS) es explotado para facilitar una actividad maliciosa comúnmente conocida como "*phishing*". Los creadores de la suplantación de identidad (*phishing*) registran nombres de dominio específicamente para apoyar los ataques lanzados desde las redes de ordenadores comprometidos o computadoras en red (*botted*), llamadas redes de robots (*botnets*). El atacante a menudo utiliza algunos de estos nombres de dominio maliciosos para operar un Sistema de Nombres de Dominio (DNS) delictivo, una colección de codificadores (*resolvers*) del Sistema de Nombres de Dominio (DNS) que están específicamente programados y desplegados para resolver consultas al Sistema de

Nombres de Dominio (DNS) realizadas por las víctimas de esa suplantación de identidad (*phishing*). Otros nombres de dominio maliciosos se utilizan para alojar sitios web de suplantación de identidad (*impersonation*). Las respuestas a la consulta del Sistema de Nombres de Dominio (DNS) de una víctima que solicita un nombre de dominio aparentemente legítimo de una institución financiera, comercio electrónico, caridad, agencia gubernamental o alguna entidad similar, y que en forma desprevenida dirige a los usuarios a un sitio web engañoso o de suplantación de identidad. La víctima interactúa inocentemente con este sitio engañoso como normalmente lo haría con los sitios legítimos de instituciones financieras, comercio electrónico, caridad o agencia gubernamental. Sin embargo, estos sitios maliciosos están diseñados para robar información sobre identidad, cuenta bancaria y tarjeta de crédito del usuario, para vender productos falsos o en forma ilegal o hacer un fraude a una organización de caridad, entre otras. [3]

4.2.1.6 Cada vez más, el Sistema de Nombres de Dominio (DNS) también está desempeñando un papel destacado en permitir las redes de robots en alquiler (*botnets for hire*), redes de ataque que se ofrecen para prestar servicios en una próspera economía clandestina. Las redes de robots están compuestas por cientos de miles o incluso millones de ordenadores comprometidos (robots) que son controlados a distancia para llevar a cabo muchos tipos de ataques maliciosos (por ejemplo, Ataques Distribuidos de Denegación de Servicio —DDoS—) o para respaldar actividades delictivas (tráfico de seres humanos, distribución de productos farmacéuticos ilegales, envío de correo no solicitado —*spam*—, etc.). Para controlar los robots de manera eficiente y con una considerable resistencia contra las contramedidas adoptadas por los profesionales de seguridad y agentes de orden público, los atacantes programan los robots para utilizar el Sistema de Nombres de Dominio (DNS) para identificar la dirección del mando-y-control o puntos de encuentro (*rendezvous points*) que emiten órdenes a los robots. Recientemente, algunos software maliciosos —como las variantes del programa informático dañino Conficker—, han utilizado enfoques que buscan poder contar con grupos de nombres de dominio predeterminados como un aspecto clave del control de los robots.

4.2.2 Riesgos Técnicos

4.2.2.1 El funcionamiento o la integridad del Sistema de Nombres de Dominio (DNS) puede ser adversamente afectado mediante el uso generalizado de prácticas operacionales cuestionables que resultan en una interrupción del servicio, o en caso que un cambio técnico resulte en una vulnerabilidad no prevista que sea explotada por malandrines o delincuentes para facilitar las actividades maliciosas. Las instancias de este último tipo de problema y la manera en gran medida reactiva en la cual estos problemas son actualmente abordados, ocurrieron en 2008. El experto en seguridad Daniel Kaminsky descubrió una grave vulnerabilidad en el protocolo del Sistema de Nombres de Dominio

[3] Departamento de Seguridad de la Patria de los EE.UU., Consejo Gubernamental de Coordinación de Tecnología de la Información. 2009. Evaluación Referencial de Riesgo del Sector de Tecnología de la Información. Washington, DC: Oficina de Publicación del Gobierno, pp 32–33.

(DNS) y posteriormente demostró públicamente que una práctica conocida como modificación de respuesta del Sistema de Nombres de Dominio (DNS) podría ser explotada por atacantes para secuestrar los sitios web de las principales empresas utilizando servicios de alojamiento web totalmente fuera del alcance de la administración de esas organizaciones. Luego, el Comité Asesor de Seguridad y Estabilidad (SSAC) publicó una alerta de asesoramiento sobre las potenciales amenazas que la modificación de respuesta del Sistema de Nombres de Dominio (DNS) representa para la comunidad (http://www.icann.org/en/committees/security/ sac032.pdf). Se establecieron sistemas *ad hoc* para que los operadores del Sistema de Nombres de Dominio (DNS) y los usuarios pudiesen poner a prueba sus sistemas en relación a su vulnerabilidad y pudiesen tomar medidas preventivas o reparadoras. La comunidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha comenzado y continúa llevando a cabo varias iniciativas que pueden contribuir a una divulgación más coordinada y a una respuesta más organizada ante las amenazas de este tipo para el Sistema de Nombres de Dominio (DNS). Esto incluye la labor de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) con socios para llevar a cabo simposios anuales a fin de traer a expertos para estudiar el panorama de amenazas, para evaluar el riesgo en forma colectiva y para elaborar recomendaciones sobre cómo abordar el riesgo. El primer simposio fue realizado en el mes de febrero de 2009, conjuntamente con el Centro de Seguridad de Información Tecnológica de Georgia (GTISC).

4.2.2.2 El funcionamiento del Sistema de Nombres de Dominio (DNS) también puede verse adversamente afectado si los cambios técnicos al Sistema de Nombres de Dominio (DNS) alteran el comportamiento del sistema o resultan en cargas de tráfico que requieren cambios substanciales en el funcionamiento actual o previsto. Para reducir la posibilidad de la adopción de prácticas operativas que puedan perturbar la seguridad y estabilidad del Sistema de Nombres de Dominio (DNS) a nivel de los Dominios de Alto Nivel (TLD), en 2009 la Junta Directiva de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) implementó medidas para prohibir el uso de la redirección en base a los riesgos que esta práctica supone para la estabilidad del Sistema de Nombres de Dominio (DNS), identificados por el Comité Asesor de Seguridad y Estabilidad (documento SAC041 http://www.icann.org/en/committees/security/sac041.pdf). [4] En 2010, la comunidad del Sistema de Nombres de Dominio (DNS) continuará realizando una revisión exhaustiva de los posibles impactos que podrían resultar a partir de una serie de cambios propuestos en el nivel raíz del Sistema de Nombres de Dominio (DNS): la implementación de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC), la implementación de IPv6 y la necesidad de registros de pegado (*glue records*) IPv6 que se añadirán al archivo de zona raíz, la introducción del proceso de avance acelerado para

[4] Departamento de Seguridad de la Patria de los EE.UU., Consejo Gubernamental de Coordinación de Tecnología de la Información. 2009. Evaluación Referencial de Riesgo del Sector de Tecnología de la Información. Washington, DC: Oficina de Publicación del Gobierno, pp 32–33.

permitir el uso de etiquetas de Nombres de Dominio Internacionalizados (IDN) a nivel superior del Sistema de Nombres de Dominio (DNS) y la introducción de los nuevos Dominios de Alto Nivel (TLDs).

4.2.3 Fracasos Organizacionales

4.2.3.1 El posible fracaso de las organizaciones que desempeñan roles clave en el funcionamiento del Sistema de Nombres de Dominio (DNS) para operar con eficacia, también constituye una categoría de riesgo significativo. En el núcleo del Sistema de Nombres de Dominio (DNS), la capacidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), de los operadores de servidores raíz, de los registros y registradores de Dominios de Alto Nivel (TLD) para prestar servicios sin interrupción, resulta esencial para la seguridad y estabilidad general del Sistema de Nombres de Dominio (DNS). Cada una de estas entidades es individualmente responsable por su propia viabilidad financiera, continuidad de negocios y gestión del riesgo; sin embargo, a nivel del sistema (integral) debe existir una provisión tanto para las contingencias ante la eventualidad de que una organización no pueda desempeñar su función, según proceda, como para la manera en que los servicios serán restaurados, perpetuados o reconstituidos para garantizar el funcionamiento continuado y efectivo del Sistema de Nombres de Dominio (DNS) y para proteger a los registrantes.

4.2.4. Medición del Riego y de la Seguridad, Estabilidad y Flexibilidad

4.2.4.1 Actualmente, existe poco consenso respecto a las medidas correctas y a los niveles de desempeño/rendimiento aceptables para el sistema como un todo en relación al riesgo, a la seguridad, estabilidad y flexibilidad/capacidad de recuperación. Los operadores individuales e investigadores independientes han medido los diversos aspectos del Sistema de Nombres de Dominio (DNS), pero hasta la fecha se ha avanzado poco en la definición e implementación de métricas estándar integrales o niveles de servicio aceptables. Los esfuerzos para mejorar la gestión de riesgos relacionados con la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio (DNS) deben ser guiados por una mayor habilidad/capacidad para medir estas características y evaluar la utilidad de los programas e inversiones de recursos.

4.2.4.2 Un elemento clave para mejorar esta situación será garantizar que las partes que componen las operaciones del Sistema de Nombres de Dominio (DNS) estén correctamente instrumentadas y medidas. El Informe del Equipo de Estudio del Servidor Raíz 2009 (RSST) sobre el escalamiento de la raíz (http://www.enisa.europa.eu/events/ee/ EWNI2010) hace una llamada al "establecimiento de mecanismos eficaces para detectar y mitigar los riesgos a medida que se hacen visibles" en relación al sistema de servidores raíz. El establecimiento de indicadores (métrica) e instrumentación plantea algunos desafíos interesantes. Específicamente, la naturaleza distribuida del Sistema de Nombres de Dominio (DNS) requiere de un modelo de medición cooperativa, el cual necesita de la participación de múltiples actores y organizaciones. El tema de Sistemas de Alerta Temprana de Internet está siendo estudiado por distintos frentes, como la Agencia Europea de Seguridad de Redes e Información (ENISA), quien en el mes de marzo de 2010 celebrará su primer

taller sobre Alerta Temprana e Inteligencia de Red de Internet (http://www.enisa.europa.eu/events/ee/ EWNI2010). En el mes de febrero de 2010, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) celebró en colaboración con la Universidad de Kyoto el segundo simposio mundial sobre Seguridad, Estabilidad y Flexibilidad del Sistema de Nombres de Dominio (DNS), con un enfoque específico sobre la medición. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) planea alentar y participar en actividades que mejoren el estado de entendimiento/comprensión sobre la forma de medir los riesgos del Sistema de Nombres de Dominio (DNS), así como la salud, seguridad, estabilidad y flexibilidad del sistema como un factor fundamental en el establecimiento de la evaluación de riesgos, planificación/ejercicios de contingencia y capacidad de respuesta.

5. Iniciativas Estratégicas

5.1 Las dos iniciativas presentadas aquí responden a necesidades críticas en el establecimiento de las prestaciones necesarias para que la Corporación para la Asignación de Números y Nombres en Internet (ICANN) cumpla con los compromisos de seguridad, estabilidad y flexibilidad anteriormente identificados. Tal como se indica al principio, este documento está destinado a proporcionar una base para que estas iniciativas propuestas, las responsabilidades de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en establecer las prestaciones propuestas y la forma en que la comunidad puede proceder en la organización de esfuerzos para respaldar a tales iniciativas, sean debatidas por las múltiples partes interesadas. Se han identificado personal de alto nivel e implicancias financieras; sin embargo, las alternativas de financiación para estas iniciativas no han sido analizadas.

5.2 La Iniciativa 2 relacionada con la necesidad de establecer un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) se presenta con mayor detalle en el caso de negocios del Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT), el cual acompaña a este documento.

5.1 Iniciativa 1 – Análisis de Riesgo, Planificación de Contingencia y Ejercicios en el Sistema de Nombres de Dominio (DNS) en su conjunto

5.1.1 La Corporación para la Asignación de Números y Nombres en Internet (ICANN) colabora con la comunidad del Sistema de Nombres de Dominio (DNS) para comprender de forma proactiva los riesgos clave para el Sistema de Nombres de Dominio (DNS), incluyendo el análisis de nuevas amenazas y riesgos, conforme a los requisitos de la Afirmación de Compromisos. Una vez que estos riesgos se hayan analizado, la comunidad del Sistema de Nombres de Dominio (DNS) debe identificar las contingencias de mayor preocupación para la seguridad, estabilidad y flexibilidad/capacidad de recuperación integrales del Sistema de Nombres de Dominio (DNS) y asegurar que se establezcan los esfuerzos de planificación para mitigar los riesgos identificados. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) considera que tiene un rol importante en posibilitar la planificación y ejercicios de contingencia integrales del Sistema de Nombres de Dominio (DNS), como parte de sus

responsabilidades en virtud de la Afirmación de Compromisos. Este programa proactivo complementará las capacidades de respuesta que puedan ser ofrecidas por un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT), además de mejorar la organización como un centro natural para respaldar la contingencia y planificación de ejercicios.

5.1.2 El primer aspecto de esta iniciativa sería la de constituir un enfoque basado en la comunidad para el análisis de riesgos, que incluya un marco aceptado de riesgo del Sistema de Nombres de Dominio (DNS) y que defina los enfoques para refinar la medición de riegos. Este esfuerzo incluirá el establecimiento de un enfoque para la realización de evaluaciones de riesgo periódicas del Sistema de Nombres de Dominio (DNS) y propuestas de mitigación. Este esfuerzo se basará en la labor del Simposio 2010 sobre Seguridad, Estabilidad y Flexibilidad del Sistema de Nombres de Dominio (DNS), así como en los esfuerzos realizados por el Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio (DNS-OARC), la Agencia Europea de Seguridad de Redes e Información (ENISA) y otros.

5.1.3 Otro aspecto de esta iniciativa es mejorar la colaboración de toda la comunidad en la planificación de contingencia y usar eso como una base para dirigir los esfuerzos para establecer capacidades de respuesta. La base para la planificación de contingencia debe comenzar a partir de un consenso en torno a un marco de riesgo integral del Sistema de Nombres de Dominio (DNS) que identifique los riesgos principales para el Sistema de Nombres de Dominio (DNS) y los escenarios clave. Este esfuerzo se basará en los esfuerzos existentes, tales como los realizados a través de asociaciones público-privadas relacionadas con la protección de infraestructuras críticas, como el Consejo de Coordinación de los EE.UU. para el Sector de Tecnología de la Información y la Agencia Europea de Seguridad de Redes e Información (ENISA), así como aquellos realizados como parte de la comunidad operacional del Sistema de Nombres de Dominio (DNS) tales como los llevados a cabo por el Centro de Investigación y Análisis de Operaciones para el Sistema de Nombres de Dominio (DNS OARC) y NL Net Labs. Esta iniciativa propuesta también prevé una estrecha coordinación con un mecanismo emergente para intercambiar información del sistema de servidor raíz y con los operadores de registro de Dominios de Alto Nivel (TLD). El análisis de riesgos y las contingencias clave se utilizarán para evaluar la adecuación de los actuales mecanismos de respuesta, para identificar las carencias que requieren de una acción y para elaborar planes de contingencia para riesgos identificados. El esfuerzo debe ser avalado por un grupo de trabajo/asesoría experto y prestigioso, abarcador de la comunidad. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) asumiría la responsabilidad de respaldar al grupo y de elaborar un plan de acción para la revisión para revisión de la comunidad, el cual constituiría un aporte al ciclo anual de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) tanto para su seguridad, estabilidad y flexibilidad como para la presupuestación de la planificación operacional.

5.1.4 Una vez que la planificación de contingencia esté establecida, se necesita un programa de ejercicio integral del Sistema de Nombres de Dominio (DNS) para garantizar que la

capacidad de respuesta sea evaluada y que las carencias sean identificadas[5]. Al igual que con el Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) y los esfuerzos de planificación de contingencia, la elaboración de un programa de ejercicio debe estar basado en las actividades existentes y deben incorporar esfuerzos tales como los esfuerzos existentes de ejercicios de contingencia de los Dominios de Alto Nivel (TLD) como sub-elementos de un programa más amplio. El objetivo debe ser poner en marcha un programa de actividades que culmine en un ejercicio semestral integral del Sistema de Nombres de Dominio (DNS), centrado en la respuesta a las contingencias clave. En forma adicional, el programa debe incluir la integración con otros programas de ejercicio, tales como una serie de ejercicios multinacionales de *cyber storm* (ejercicios intencionados para probar las defensas nacionales contra el espionaje digital) y otros ejercicios internacionales de las múltiples partes interesadas. Conforme a lo identificado en la Afirmación de Compromisos, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) tiene la responsabilidad de apoyar un planteamiento abarcador de la comunidad para tal programa, facilitando subelementos de un programa, según el caso, y coordinar el ejercicio semestral integral del Sistema de Nombres de Dominio (DNS).

5.1.1 Pasos Específicos Propuestos

5.1.1.1 Establecer un grupo asesor experto en Evaluación de Riesgos del Sistema de Nombres de Dominio (DNS) y Planificación de Contingencias. Este grupo estará integrado por expertos de las comunidades de operaciones del Sistema de Nombres de Dominio (DNS) y de ciber-seguridad. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) brindará apoyo al grupo con personal. El enfoque inicial del grupo será establecer un marco aceptado por la comunidad para los riesgos sistémicos del Sistema de Nombres de Dominio (DNS) e identificar los principales riesgos existentes para el 3er trimestre de 2010. En forma adicional, el grupo se basará en el trabajo del Simposio 2010 sobre Seguridad, Estabilidad y Flexibilidad relacionado con las métricas/parámetros para establecer un marco aceptado por la comunidad para la medición de la salud, la seguridad, la estabilidad y la flexibilidad del Sistema de Nombres de Dominio (DNS) para comienzos de 2011. El grupo también será responsable de establecer escenarios de planificación de contingencia de referencia, para el 2do trimestre de 2011. El grupo realizará un informe anual de riesgos del Sistema de Nombres de Dominio (DNS) y su mitigación, entregando el primer informe en el 3er trimestre de 2011.

5.1.1.2 Establecer un mecanismo para intercambiar información del sistema de servidor raíz y con los operadores de registro de Dominios de Alto Nivel (TLD) que resulte del esfuerzo colaborativo conjunto de la comunidad de operadores del servidor raíz y otros involucrados en la comunidad del servidor raíz, en base a las recomendaciones del Estudio de Escalamiento de la Raíz de 2009. Se conformará un grupo de trabajo apoyado

[5] El requisito de un programa de este tipo para el Sistema de Nombres de Dominio (DNS) está específicamente identificado en la Evaluación de Riesgos del Sector de Tecnología de la Información (IT) del Departamento de Seguridad de la Patria (DHS) de los EE.UU.

por el personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) para identificar los requisitos funcionales y de supervisión del desempeño/rendimiento. Entre las prestaciones clave se incluyen: la maduración del modelado del sistema raíz del Sistema de Nombres de Dominio (DNS), el mejoramiento del intercambio de información entre las organizaciones que participan en el sistema raíz, el posible despliegue de los sensores necesarios y el apoyo analítico dedicado a evaluar la salud actual del sistema raíz del Sistema de Nombres de Dominio (DNS) y de advertir los problemas emergentes. Se llevarán a cabo esfuerzos para trabajar con la comunidad para implementar e instalar sensores y para medir los parámetros que permitan brindar una visión general del servidor raíz y del sistema de Dominios de Alto Nivel (TLD) y cómo se comporta. Este esfuerzo requerirá de la colaboración de los operadores de Dominios de Alto Nivel (TLD), los operadores de servidor raíz, la Administración Nacional de Telecomunicaciones e Información (NTIA), la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y otros involucrados en el funcionamiento y la gestión de la infraestructura principal del Sistema de Nombres de Dominio (DNS). Prevemos que este sistema se establecerá en forma de apoyo mutuo conjuntamente con el desarrollo del Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT).

5.1.1.3 Apoyo continuo de la planificación de contingencia y ejercicios de los operadores del servidor raíz. Tras el éxito de los ejercicios de comunicaciones y de un ejercicio inicial realizado para el segundo semestre de 2010, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) planificará el trabajo con los operadores para establecer un enfoque programático para la planificación de contingencia y ejercicios basados en distintos escenarios. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) desplegará capacidades de comunicación que se complementen con —y que mejoren— los sistemas existentes, utilizados en las operaciones de su propio servidor de raíz.

5.1.1.4 Maduración continua de la planificación y ejercicios de continuidad de Dominios de Alto Nivel (TLD). Durante 2010 y parte de 2011, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y los operadores de registro de Dominios de Alto Nivel (TLD) llevarán a cabo pruebas de custodia de datos basadas en el desarrollo de especificaciones sobre la custodia de datos para el proceso de los nuevos Dominios Genéricos de Alto Nivel (gTLD). Se planean ejercicios adicionales, enfocados sobre las comunicaciones y elementos de respuesta a la crisis entre la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y los operadores de registro de Dominios de Alto Nivel (TLD).

5.1.1.5 Iniciar el desarrollo de un ejercicio integral del Sistema de Nombres de Dominio (DNS) y de un programa de evaluación. Este programa incluirá aprovechar los esfuerzos ya existentes y requiere de la participación de una amplia gama de partes interesadas, incluyendo a aquellos involucrados en las comunidades de operaciones del Sistema de Nombres de Dominio (DNS), de vendedores/proveedores del Sistema de Nombres de Dominio (DNS) y de usuarios, así como la comunidad más amplia en ciber-seguridad.

Este programa también implicaría la comprensión y el aprovechamiento de la intersección con otros ejercicios de ciber-seguridad, con ejercicios asociados y con programas de evaluación. A fines de 2010, este esfuerzo evaluará la naturaleza y la adecuación de los esfuerzos existentes e identificará las principales carencias. Para mediados de 2011, se elaborará un documento conteniendo una propuesta conceptual del programa de ejercicio del Sistema de Nombres de Dominio (DNS) para ser evaluado por la comunidad. En forma adicional, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) patrocinará un ejercicio limitado e integral del sistema en la segunda mitad de 2011, como un prototipo, con la participación voluntaria de toda la gama de partes interesadas y destinado a establecer una planificación a largo plazo y procesos de ejecución. La planificación de este ejercicio prototipo comenzará en 2010. El personal de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y otros miembros de la comunidad del Sistema de Nombres de Dominio (DNS) participarán en el ejercicio multilateral *Cyber Storm III* y también pueden participar en otras actividades internacionales.

5.1.2 Proyección de Recursos

5.1.2.1 Proyectar la necesidad para cinco puestos de personal de tiempo completo:

- Coordinador Principal, Evaluación de Riesgo, Planificación de Contingencia y Programa de Ejercicios
- Coordinador de Planificación de Contingencia
- Coordinador de Programa de Evaluación y Ejercicios
- Planificador de Ejercicios
- Analista de Sistemas/Experto de modelado, Sistema de Intercambio de Información del Sistema

5.1.2.2 Los requisitos de apoyo/respaldo incluyen: la definición de los requisitos para el intercambio de información del sistema de servidores raíz; el apoyo para el análisis de riesgos y esfuerzos de intercambio de información del servidor raíz; infraestructura y costos asociados a fin de incluir la concesión de licencias y soporte de software/hardware para el modelado, un sistema para el intercambio de información del sistema de servidor raíz, sistemas de comunicaciones y sistema prototipo para la implementación de sensores; gastos de viajes y reuniones para los grupos de trabajo y el personal; e instalaciones físicas y apoyo informático para el personal adicional.

5.1.2.3 Anticipamos que los gastos para apoyar este esfuerzo desde julio 2010 a junio de 2011 son de aproximadamente 1,25 millones dólares estadounidenses para el personal y de 850 mil dólares estadounidenses para el apoyo. El costo total anual proyectado para el primer año de esta iniciativa sería de 2,1 millones de dólares estadounidenses.

5.1.2.4 **Supuestos:** El análisis de riesgo utilizaría la información sobre amenazas y el análisis del Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT). El sistema de intercambio de información del servidor raíz

utilizaría el portal Web 2.0 desarrollado para el Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS CERT) para apoyar el intercambio de información.

5.2 Iniciativa 2 – Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT)

5.2.1 Además de la evaluación proactiva de riesgos, la planificación de contingencia y el ejercicio, la comunidad del Sistema de Nombres de Dominio (DNS) necesita contar con una capacidad de respuesta eficaz, operativa e integral del sistema para abordar adecuadamente los desafíos para la seguridad, estabilidad y flexibilidad. Un ataque coordinado a gran escala contra el Sistema de Nombres de Dominio (DNS) podría resultar en significativas pérdidas económicas y políticas; sin embargo, no existe un punto central de contacto para la gestión de incidentes técnicos y para la coordinación de las políticas relacionadas con la identificación y coordinación de respuesta a incidentes en el Sistema de Nombres de Dominio (DNS). En 2009, el Simposio Mundial sobre Seguridad, Estabilidad y Flexibilidad del Sistema de Nombres de Dominio (DNS) señaló específicamente la brecha de respuesta a la seguridad en el Sistema de Nombres de Dominio (DNS) y recomendó la toma de acciones para hacer frente a este déficit. Además, muchos operadores del Sistema de Nombres de Dominio (DNS) no cuentan con los recursos suficientes y como resultado tienen limitaciones en el desarrollo de esfuerzos de seguridad y flexibilidad robustos. Estas organizaciones podrían no saber adónde recurrir en búsqueda de ayuda o podrían enfrentarse a barreras geográficas o idiomáticas que les impidan obtener asistencia. Tales organizaciones tienden a ser vulnerables o a conformar puntos de explotación dentro del Sistema de Nombres de Dominio (DNS) como un todo. La Corporación para la Asignación de Números y Nombres en Internet (ICANN) considera que un punto central de contacto, un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT), es necesario para brindar apoyo técnico y coordinación de políticas del Sistema de Nombres de Dominio (DNS) y para trabajar con la comunidad del Sistema de Nombres de Dominio (DNS) a fin de identificar y coordinar las respuestas a incidentes del Sistema de Nombres de Dominio (DNS) a nivel mundial.

5.2.2 Un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) coordinaría los esfuerzos existentes con la comunidad del Sistema de Nombres de Dominio (DNS) para mantener la conciencia de la situación, de modo que la comunidad en general pueda llegar a obtener el asesoramiento adecuado en cualquier momento. Las partes interesadas clave de tal esfuerzo serían los operadores y usuarios del Sistema de Nombres de Dominio (DNS), los vendedores/proveedores, investigadores de seguridad y encargados de respuesta de incidentes. Un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) permitiría utilizar una serie de iniciativas existentes que intentan identificar las amenazas, compartir información y facilitar una respuesta de todo el Sistema de Nombres de Dominio (DNS). Las actividades del Equipo de Respuesta ante Emergencias

del Sistema-Computadora de Nombres de Dominio (DNS-CERT) pueden ayudar en la colaboración y coordinación de estos esfuerzos y pueden brindar servicios en áreas que actualmente no están cubiertas o con partes interesadas que no participan en estos esfuerzos. Un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) podría ser lanzado con el apoyo de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), pero la estructura organizacional específica y el modelo de asignación de recursos se determinarán mediante el diálogo con la comunidad. En este sentido, la supervisión del Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) sería realizada por una Junta basada en patrocinadores, que garantice la responsabilidad/rendición de cuentas a la unidad constitutiva del Equipo de Respuesta ante Emergencias (CERT) y que evalúe las actividades del Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) sobre la base de las necesidades de las partes interesadas a quienes sirve la organización. Las operaciones del Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) estaría supervisadas por un equipo central conformado con personal administrativo y técnico, el cual sería asistido por un equipo ampliado compuesto por individuos que aumenten la experiencia virtual, prestando apoyo tangible al Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) y operando en forma geográficamente dispersa.

5.2.3 Un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) proporcionará a su unidad constitutiva servicios tanto proactivos —es decir: análisis de amenazas, salud y monitoreo de seguridad del Sistema de Nombres de Dominio (DNS), toma de consciencia sobre cada situación e intercambio de información—, como servicios reactivos —es decir: punto de contacto 365 x 24 x 7, coordinación de gestión de incidentes, respaldo de gestión ante vulnerabilidad y servicios de asesoría sobre seguridad—. Este enfoque es importante por dos razones: (1) porque el contar con información acerca del panorama de amenazas en forma proactiva puede ayudar a la comunidad del Sistema de Nombres de Dominio (DNS) a contar con planes en caso de amenazas, a través de la capacitación y ejercicios; y (2) porque los servicios reactivos de gestión de incidentes pueden ayudar a las unidades constitutivas con una significativa limitación de recursos, tales como los registradores de regiones del mundo menos desarrolladas. La información y el análisis de amenazas también servirían como aporte para el establecimiento proyectado de la identificación de riesgos y capacidades de análisis sistémicas del Sistema de Nombres de Dominio (DNS) descriptas en la Iniciativa 1. La definición de los requisitos funcionales para las prestaciones centrales que ofrecerá un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) ocurrirá a través de un análisis basado en la comunidad que cuente con la participación de las partes interesadas y posibles colaboradores para un Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT).

5.2.2 Proyección de Recursos

5.2.2.1 En base a la evaluación de Equipos de Respuesta ante Emergencias (CERT) nacionales de tamaño y nivel de responsabilidad similares, creemos que el Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) puede funcionar inicialmente con un presupuesto anual de una plana de personal de aproximadamente 15 personas, la cual incluye a un director, dos gerentes/directivos principales, un equipo de gestión de incidentes de diez personas y personal de apoyo administrativo/jurídico. La proyección de los costos de personal es de 2,6 millones de dólares estadounidenses. Los gastos de apoyo para los viajes del personal, las herramientas de comunicaciones y análisis, las instalaciones físicas y el apoyo informático se estiman en 1,6 millones de dólares estadounidenses. El costo total estimado para el primer año de esta iniciativa es de 4.2 millones de dólares estadounidenses. En el Caso de Negocios del Equipo de Respuesta ante Emergencias del Sistema-Computadora de Nombres de Dominio (DNS-CERT) que acompaña a este documento se pueden encontrar más detalles.

6. Conclusión

Los desafíos de seguridad, estabilidad y flexibilidad/capacidad de respuesta que enfrenta el Sistema de Nombres de Dominio (DNS) están aumentando. En virtud de sus estatutos y de la Afirmación de Compromisos la Corporación para la Asignación de Números y Nombres en Internet (ICANN) tiene responsabilidades importantes para trabajar con la comunidad del Sistema de Nombres de Dominio (DNS) para abordar esos desafíos. Específicamente, se requiere el establecimiento de una planificación de contingencias integral del Sistema de Nombres de Dominio (DNS), de ejercicios y capacidades de respuesta colaborativas. Este documento conceptual proporciona una base para un análisis/debate de las partes interesadas respecto a estas iniciativas propuestas para abordar tales requisitos/necesidades.