Informe Final del Equipo de la Segunda Revisión de Seguridad, Estabilidad y Flexibilidad (SSR2) – Resumen ejecutivo y recomendaciones

Fragmento del Informe Final del Equipo de Revisión SSR2

25/01/2021

ICANN

ÍNDICE

A. Resumen Ejecutivo

En virtud de los Estatutos (Sección 4.6(c)) de la Corporación para la Asignación de Nombres y Números en Internet (ICANN):

"*La Junta Directiva deberá dar lugar a una revisión periódica de la ejecución de los compromisos de la ICANN para mejorar la estabilidad operativa, confiabilidad, flexibilidad, seguridad e interoperabilidad mundial de los sistemas y procesos, tanto internos como externos, que directamente afectan y/o son afectados por el sistema de identificadores únicos de Internet que coordina la ICANN ("Revisión de SSR").*"[1]

Estas revisiones de SSR constituyen una parte fundamental del mandato de la organización de la ICANN[2] de "desempeñarse en la máxima medida posible de manera abierta y transparente, y en concordancia con los procedimientos diseñados para garantizar la equidad". Esta es la segunda revisión de SSR realizada y, conforme a los Estatutos, incluye una revisión del manejo de las recomendaciones de la primera revisión de SSR por parte de la organización de la ICANN, así como nuevas recomendaciones para que la organización de la ICANN las considere.

El Equipo de Revisión SSR2 ofrece 24 grupos de recomendaciones, los cuales dan lugar a 63 recomendaciones específicas, comenzando con la evaluación de la respuesta de la organización de la ICANN a las recomendaciones de la SSR1. Adoptamos el enfoque de dividirlas en recomendaciones muy específicas en respuesta a la falta de especificidad de las recomendaciones de la SSR1. Las recomendaciones luego se estructuran para ofrecer una perspectiva de las operaciones internas de la organización de la ICANN, la participación de la organización de la ICANN (en particular los contratos y la gestión de reclamos) y cómo la organización de la ICANN puede tomar medidas para mejorar sus propias acciones de SSR y para ayudar a otros a entender cómo mejorar las suyas. Las recomendaciones que figuran en todo el documento suelen influirse mutuamente e incluyen dependencias entre ellas. La Junta Directiva y la organización de la ICANN deben tener esto en cuenta al desarrollar los planes de implementación. El equipo de revisión alcanzó un pleno consenso sobre todas las recomendaciones.

Para apoyar evaluaciones más eficientes por parte de futuros equipos de revisión de SSR, el Equipo de Revisión SSR2 intentó formular sus propias recomendaciones de acuerdo con los criterios SMART: *específicas, mensurables, asignables, relevantes y rastreables*. En muchos casos, los detalles necesarios para que cada recomendación sea plenamente "SMART", incluida la asignación de plazos apropiados, requerirá la reflexión y la acción del equipo de implementación y debería incluirse en el plan final de implementación. El equipo de revisión también ofreció varias sugerencias para que se considerara la forma en que se podrían llevar a cabo las revisiones futuras, reconociendo que éstas quedan fuera del mandato directo de la propia revisión de SSR. En el Apéndice C, se incluye información adicional sobre el proceso y la metodología utilizados por el Equipo de Revisión SSR2 para cumplir su mandato: Proceso y metodología.

[1] ICANN, "Estatutos de la Corporación para la Asignación de Nombres y Números en Internet: Sección 4.6(c): Revisiones específicas: Revisión de Seguridad, Estabilidad y Flexibilidad" enmendada el 28 de noviembre de 2019, https://www.icann.org/resources/pages/governance/bylaws-en/#article4.

[2] Estatutos de la ICANN, Sección 3.1: https://www.icann.org/resources/pages/governance/bylaws-en/.

1. Información de referencia

Como se ha señalado en la Sección A.2. Objetivos de la Revisión de SSR, los Estatutos de la ICANN requieren una evaluación periódica de la seguridad, estabilidad y flexibilidad del sistema de nombres de dominio (DNS). La Junta Directiva de la ICANN recibió formalmente el primer informe de revisión de SSR el 13 de septiembre de 2012. Cinco años después, la segunda revisión comenzó con la reunión inicial del Equipo de Revisión SSR2, celebrada el 2 de marzo de 2017. Sin embargo, desde su creación, el Equipo de Revisión SSR2 se encontró con varios retos que prolongaron la duración de la revisión mucho más allá de lo que nadie esperaba. El Equipo de Revisión SSR2 se reunió de forma periódica hasta octubre de 2017, cuando la Junta Directiva detuvo las actividades del equipo.[3] Las reuniones comenzaron de nuevo con la reconstitución de los miembros el 19 de junio de 2018.[4]

El panorama del ecosistema mundial de identificadores únicos siguió evolucionando durante el prolongado período de tiempo del proceso de revisión. A pesar de la interrupción mundial de los negocios y los viajes como consecuencia de la pandemia de COVID-19, que introdujo retrasos adicionales en el proceso de revisión del SSR2, el Equipo de Revisión SSR2 pudo completar la revisión. En el último año del proceso de revisión, el equipo optó por no reiniciar la evaluación de sus recomendaciones originales, sino más bien por preservar sus contribuciones fundacionales e históricas. El equipo de revisión cree que estas recomendaciones siguen siendo en gran medida relevantes para la organización de la ICANN y en apoyo de la seguridad, estabilidad y resiliencia del DNS a escala global.

2. Objetivos de la revisión de SSR

Según los Estatutos de la ICANN (Sección 4.6(c)): "*La Junta Directiva deberá dar lugar a una revisión periódica de la ejecución de los compromisos de la ICANN para mejorar la estabilidad operativa, confiabilidad, flexibilidad, seguridad e interoperabilidad mundial de los sistemas y procesos, tanto internos como externos, que directamente afectan y/o son afectados por el sistema de identificadores únicos de Internet que coordina la ICANN ("Revisión de SSR").*"[5]

En concreto, establece lo siguiente:

"ii. Las cuestiones que el equipo de revisión para la Revisión de SSR ("Equipo de Revisión de SSR") puede evaluar son las siguientes:

1. *cuestiones de seguridad, estabilidad operativa y flexibilidad, tanto físicas como de red, relacionadas con la coordinación del sistema de identificadores únicos de Internet;*
2. *conformidad con el marco adecuado de planificación de contingencias de seguridad para el sistema de identificadores únicos de Internet;*
3. *mantenimiento de procesos de seguridad claros e interoperables a nivel mundial para aquellas partes del sistema de identificadores únicos de Internet que coordina la ICANN.*

[3] Carta al Equipo de Revisión SSR2 del Dr. Stephen D. Crocker, Presidente, Junta Directiva de la ICANN, 28 de octubre de 2017, https://www.icann.org/en/system/files/correspondence/crocker-to-ssr2-28oct17-en.pdf.

[4] ICANN, "Se reinicia la Segunda Revisión de Seguridad, Estabilidad y Flexibilidad del DNS (SSR2)", blog, 7 de junio de 2018, https://www.icann.org/news/announcement-2-2018-06-07-en.

[5] Estatutos de la ICANN, Sección 4.6(c), https://www.icann.org/resources/pages/governance/bylaws-en.

iii. El Equipo de Revisión de SSR también evaluará hasta qué punto la organización de la ICANN ha implementado de manera exitosa los esfuerzos en materia de seguridad, la efectividad de los esfuerzos de seguridad para hacer frente a desafíos y amenazas reales y potenciales a la seguridad y estabilidad del DNS y la medida en que los esfuerzos de seguridad son lo suficientemente sólidos como para hacer frente a los futuros desafíos y amenazas a la seguridad, estabilidad y flexibilidad del DNS, de forma consistente con la Misión de la ICANN.

iv. El Equipo de Revisión de SSR también evaluará en qué medida se implementaron las recomendaciones previas de la Revisión de SSR como también en qué medida la implementación de dichas recomendaciones ha logrado los resultados previstos.

v. La Revisión de SSR se llevará a cabo con una frecuencia de al menos cada cinco años, a contarse desde la fecha de convocatoria del Equipo de Revisión de SSR anterior."

3. Influencia de otros equipos de revisión y comités asesores

La organización de la ICANN debe participar con varios equipos de revisión y Comités Asesores (AC), conforme a lo establecido en los Estatutos de la ICANN. Si bien cada uno de esos equipos y comités tiene mandatos específicos, las recomendaciones elaboradas por esos grupos pueden superponerse y se superponen con las áreas de trabajo de otros comités y equipos de revisión. El Equipo de Revisión SSR2 evaluó las recomendaciones de otros equipos de revisión y AC para determinar donde sus recomendaciones publicadas afectaron la SSR de la organización de la ICANN y el DNS a escala global. En varios casos, el Equipo de Revisión SSR2 consideró necesario incorporar y aprovechar esas recomendaciones para desarrollar la guía necesaria relacionada con la SSR para la organización de la ICANN (véase, en particular, la Sección E.1. Medidas de protección no logradas para el Programa de Nuevos gTLD y la Sección E.3. Alternativas al PDP). El Equipo de Revisión SSR2 consideró que estas superposiciones en las recomendaciones eran una corroboración tácita de los méritos de las cuestiones correspondientes y consideró además que los acuerdos entre las recomendaciones del equipo de revisión y las de otros grupos constituían un apoyo empírico a su necesidad. Las recomendaciones del SSR2 tienen como objetivo complementar las recomendaciones de esos otros equipos de revisión.

B. Recomendaciones del SSR2

El Equipo de Revisión SSR2 alcanzó un pleno consenso sobre todas las recomendaciones.

1. Cuadro de resumen

N.°	Recomendación	Encargado	Prioridad
Recomendación 1 del SSR2: Revisión adicional del SSR1			

1.1	La Junta Directiva de la ICANN y la organización de la ICANN deberían realizar una revisión adicional exhaustiva de las Recomendaciones del SSR1 y ejecutar un nuevo plan para completar la implementación de las Recomendaciones del SSR1 (véase el Apéndice D: Conclusiones relacionadas con las Recomendaciones del SSR1).	Junta Directiva de la ICANN y Organización de la ICANN	Baja
Recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos.			
2.1	La organización de la ICANN debería crear un cargo de Director de Seguridad (CSO) o de Director de Seguridad de la Información (CISO) a nivel de alta gerencia ejecutiva de la organización de la ICANN y contratar a una persona debidamente cualificada para dicho cargo y asignar un presupuesto específico suficiente para ejecutar las funciones de este puesto.	Organización de la ICANN	Medio-Alta
2.2	La organización de la ICANN debería incluir, como parte de la descripción de este cargo, que este puesto gestionará la función de seguridad de la organización de la ICANN y supervisará las interacciones del personal en todas las áreas relevantes que afecten a la seguridad. Este puesto debería ser responsable de proporcionar informes periódicos a la Junta Directiva de la ICANN y a la comunidad sobre todas las actividades relacionadas con la SSR dentro de la organización de la ICANN. Las funciones de seguridad existentes deberían reestructurarse y trasladarse organizativamente para estar subordinadas a este nuevo puesto.	Organización de la ICANN	Medio-Alta
2.3	La organización de la ICANN debería incluir, como parte de la descripción de esta función, que este puesto será responsable de la seguridad estratégica y táctica y de la gestión de riesgos. Entre esas esferas de responsabilidad se incluye la de estar a cargo y coordinar estratégicamente una función centralizada de evaluación de riesgos, continuidad de operaciones y planificación de la recuperación ante desastres (véase también la Recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres) en todo el ámbito de la seguridad interna de la organización, incluido el Servidor Raíz Gestionado por la ICANN (IMRS, comúnmente conocido como Raíz L), y coordinar con otras partes interesadas que participan en el sistema de identificación global externo, así como publicar una metodología y un enfoque de evaluación	Organización de la ICANN	Medio-Alta

	de riesgos.		
2.4	La organización de la ICANN debería incluir, como parte de la descripción de esta función, que esta función será responsable de todas las partidas presupuestarias y responsabilidades relevantes para la seguridad y participará en todas las negociaciones contractuales relevantes para la seguridad (por ejemplo, acuerdos de registro y registrador, cadenas de suministro para hardware y software y acuerdos de nivel de servicio asociados) que emprendió la organización de la ICANN, refrendando todos los términos contractuales relacionados con la seguridad.	Organización de la ICANN	Medio-Alta
Recomendación 3 del SSR2: Mejorar la transparencia presupuestaria relacionada con la SSR			
3.1	El Director Ejecutivo de Seguridad a nivel de alta gerencia (véase la Recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos) debe informar a la comunidad en nombre de la organización de la ICANN sobre la estrategia, los proyectos y el presupuesto de la ICANN en materia de SSR dos veces al año y debe actualizar y publicar resúmenes presupuestarios anualmente.	Organización de la ICANN	Alta
3.2	La Junta Directiva de la ICANN y la organización de la ICANN deberían garantizar que las partidas presupuestarias específicas relacionadas con el desempeño de la organización de la ICANN de las funciones relacionadas con la SSR estén vinculadas a las metas y objetivos específicos del plan estratégico de la ICANN. La organización de la ICANN debería implementar esos mecanismos a través de un proceso anual de presupuestación y presentación de informes consistente y detallado.	Junta Directiva de la ICANN y Organización de la ICANN	Alta
3.3	La Junta Directiva de la ICANN y la organización de la ICANN deberían crear, publicar y solicitar comentarios públicos sobre los informes detallados relativos a los costos y el presupuesto relacionado con la SSR como parte del ciclo de planificación estratégica.	Junta Directiva de la ICANN y Organización de la ICANN	Alta
Recomendación 4 del SSR2: Mejorar los procesos y procedimientos de gestión de riesgos			
4.1	La organización de la ICANN debería seguir centralizando su gestión de riesgos y debería articular	Organización de la	Alta

	claramente su marco de gestión de riesgos para la seguridad y asegurarse de que se ajuste estratégicamente a los requisitos y objetivos de la organización. La organización de la ICANN debería describir las medidas relevantes de éxito y cómo evaluarlas.	ICANN	
4.2	La organización de la ICANN debería adoptar e implementar la norma ISO 31000 "Gestión de riesgos" y validar su implementación con auditorías independientes apropiadas. La organización de la ICANN debería poner a disposición de la comunidad los informes de auditorías, potencialmente en una versión censurada. Las iniciativas de gestión de riesgos deberían incorporarse a los planes y procedimientos de continuidad de operaciones y recuperación ante desastres (véase la Recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres).	Organización de la ICANN	Alta
4.3	La organización de la ICANN debería nombrar o designar a una persona responsable y dedicada a la gestión de riesgos de seguridad que esté subordinada al cargo de seguridad de alta gerencia (véase la Recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos). Esta función debería actualizar periódicamente y proporcionar informes sobre un registro de riesgos de seguridad y guiar las actividades de la organización de la ICANN. Las conclusiones deberían incorporarse a los planes y procedimientos de continuidad de operaciones y recuperación ante desastres (véase la Recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres) y el Sistema de Gestión de Seguridad de la Información (ISMS) (véase la Recomendación 6 del SSR2: Cumplir con los sistemas de gestión de seguridad de la información apropiados y las certificaciones de seguridad).	Organización de la ICANN	Alta
Recomendación 5 del SSR2: Cumplir con los sistemas de gestión de seguridad de la información apropiados y las certificaciones de seguridad.			
5.1	La organización de la ICANN debería implementar un ISMS y ser auditada y certificada por un tercero según las normas de seguridad de la industria (por ejemplo, ITIL, familia ISO 27000, SSAE-18) por sus responsabilidades operativas. El plan debería incluir	Organización de la ICANN	Alta

	una hoja de ruta y fechas de hitos para obtener certificaciones y señalar las áreas que serán objeto de mejoras continuas.		
5.2	En base al ISMS, la organización de la ICANN debería elaborar un plan de certificaciones y requisitos de capacitación para los cargos en la organización, realizar un seguimiento de los índices de finalización, proporcionar un fundamento para sus decisiones y documentar cómo las certificaciones se ajustan a las estrategias de gestión de la seguridad y los riesgos de la organización de la ICANN.	Organización de la ICANN	Alta
5.3	La organización de la ICANN debería exigir a las partes externas que prestan servicios a la organización de la ICANN que cumplan las normas de seguridad pertinentes y documenten su verificación de antecedentes respecto de los proveedores y prestadores de servicios.	Organización de la ICANN	Alta
5.4	La organización de la ICANN debería contactar a la comunidad y otras partes con informes claros que demuestren lo que está haciendo la organización de la ICANN y lo que está logrando en materia de seguridad. Estos informes serían más beneficiosos si proporcionaran información que describiera cómo la organización de la ICANN sigue las mejores prácticas y procesos maduros y en constante mejora para gestionar los riesgos, la seguridad y las vulnerabilidades.	Organización de la ICANN	Alta
Recomendación 6 del SSR2: Divulgación y transparencia sobre vulnerabilidades de SSR			
6.1	La organización de la ICANN debería promover de forma proactiva la adopción voluntaria de las mejores prácticas de SSR y los objetivos de divulgación de las vulnerabilidades por las partes contratadas. Si las medidas voluntarias resultan insuficientes para lograr la adopción de dichas mejores prácticas y objetivos, la organización de la ICANN debería implementar las mejores prácticas y objetivos en los contratos, acuerdos y memorandos de entendimiento.	Organización de la ICANN	Alta
6.2	La organización de la ICANN debería implementar el proceso para el informe de la divulgación coordinada de vulnerabilidades. Las divulgaciones y la información sobre cuestiones relacionadas con la SSR, como las infracciones en cualquier parte contratada y en los casos de vulnerabilidades críticas descubiertas y	Organización de la ICANN	Alta

	comunicadas a la organización de la ICANN, deberían ser comunicadas rápidamente a las partes de confianza y pertinentes (por ejemplo, los afectados o requeridos para resolver el asunto en cuestión). La organización de la ICANN debería informar de forma periódica sobre las vulnerabilidades (al menos una vez al año) e incluir métricas anónimas y emplear la divulgación responsable.		
Recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres			
7.1	La organización de la ICANN debería establecer un Plan de Continuidad de Operaciones para todos los sistemas que sean de propiedad o estén bajo el ámbito de competencia de la organización de la ICANN, basado en la norma ISO 22301 "Gestión de Continuidad de Operaciones", en el que se identifiquen los plazos aceptables de continuidad de operaciones y recuperación ante desastres.	Organización de la ICANN	Medio-Alta
7.2	La organización de la ICANN debería asegurarse de que el plan de recuperación ante desastres para las operaciones de los Identificadores Técnicos Públicos (PTI) (es decir, las funciones de la IANA) incluya todos los sistemas relevantes que contribuyan a la seguridad y estabilidad del DNS y también incluya la Gestión de la Zona Raíz y esté en consonancia con la norma ISO 27031. La organización de la ICANN debería desarrollar este plan en estrecha colaboración con el Comité Asesor del Sistema de Servidores Raíz (RSSAC) y los Operadores de Servidores Raíz (RSO).	Organización de la ICANN	Medio-Alta
7.3	La organización de la ICANN también debería establecer un plan de recuperación ante desastres para todos los sistemas que son propiedad o se encuentran dentro del ámbito de competencia de la organización de la ICANN, nuevamente en consonancia con la norma ISO 27031.	Organización de la ICANN	Medio-Alta
7.4	La organización de la ICANN debería establecer un nuevo sitio para la recuperación ante desastres para todos los sistemas que son propiedad o se encuentran dentro del ámbito de competencia de la organización de la ICANN con el objetivo de reemplazar los sitios de Los Ángeles o Culpeper o agregar un tercer sitio permanente. La organización de la ICANN debería localizar este sitio fuera de la región de América del Norte y de cualquier territorio de los Estados Unidos. Si la organización de la ICANN decide reemplazar uno de	Organización de la ICANN	Medio-Alta

	los sitios existentes, el sitio al que la organización de la ICANN reemplace no debería cerrarse hasta que la organización haya verificado que el nuevo sitio esté plenamente operativo y sea capaz de gestionar la recuperación ante desastres de estos sistemas para la organización de la ICANN.		
7.5	La organización de la ICANN debería publicar un resumen de sus planes y procedimientos generales de continuidad de operaciones y recuperación ante desastres. De esta manera, mejoraría la transparencia y la confianza además de abordar las metas y objetivos estratégicos de la organización de la ICANN. La organización de la ICANN debería contratar a un auditor externo para verificar el cumplimiento de estos planes de continuidad de operaciones y recuperación ante desastres.	Organización de la ICANN	Medio-Alta
Recomendación 8 del SSR2: Habilitar y demostrar la representación del interés público en las negociaciones con las partes contratantes			
8.1	La organización de la ICANN debería encargar a un equipo de negociación que incluya expertos en uso indebido y seguridad no afiliados o pagados por las partes contratadas que representen los intereses de las entidades no contratadas y que trabajen con la organización de la ICANN para renegociar los contratos de las partes contratadas de buena fe, con transparencia pública y con el objetivo de mejorar la SSR del DNS para los usuarios finales, las empresas y los gobiernos.	Organización de la ICANN	Media
Recomendación 9 del SSR2: Supervisar y exigir el cumplimiento			
9.1	La Junta Directiva de la ICANN debería ordenar al equipo de cumplimiento que supervise y exija el cumplimiento estricto de las partes contratantes de las obligaciones actuales y futuras en materia de SSR y de uso indebido en los contratos, los acuerdos de base, las especificaciones temporarias y las políticas de la comunidad.	Junta Directiva de la ICANN	Alta
9.2	La organización de la ICANN debería supervisar y exigir de forma proactiva el cumplimiento de las obligaciones contractuales del registro y del registrador para mejorar la exactitud de los datos de registración. Esta supervisión y control del cumplimiento deberían incluir la validación de los campos de dirección y la realización de auditorías periódicas sobre la exactitud	Organización de la ICANN	Alta

	de los datos de registración. La organización de la ICANN debería centrar sus esfuerzos para garantizar el cumplimiento en aquellos registradores y registros que hayan sido objeto de más de 50 reclamos o denuncias por año ante la organización de la ICANN en relación con su inclusión de datos inexactos.		
9.3	La organización de la ICANN debería asegurarse de que las actividades de cumplimiento sean auditadas externamente por lo menos una vez al año y publicar los informes de auditoría y la respuesta de la organización de la ICANN a las recomendaciones de la auditoría, incluidos los planes de implementación.	Organización de la ICANN	Alta
9.4	La organización de la ICANN debería encargar la función de cumplimiento con la publicación de informes periódicos que enumeren las herramientas que les faltan y que les ayudarían a apoyar a la organización de la ICANN en su conjunto a utilizar eficazmente los mecanismos contractuales para hacer frente a las amenazas a la seguridad del DNS, incluidas las medidas que requerirían cambios en los contratos.	Organización de la ICANN	Alta
Recomendación 10 del SSR2: Aclarar las definiciones de los términos relacionados con el uso indebido			
10.1	La organización de la ICANN debería publicar una página web que incluya su definición de trabajo sobre el uso indebido del DNS, es decir, lo que utiliza para proyectos, documentos y contratos. La definición debería señalar explícitamente qué tipos de amenazas a la seguridad considera actualmente la organización de la ICANN dentro de su ámbito de competencia para hacer frente a través de mecanismos contractuales y de cumplimiento, así como los que la organización de la ICANN entiende que están fuera de su ámbito de competencia. Si la organización de la ICANN utiliza otra terminología similar (por ejemplo, amenaza a la seguridad, conducta maliciosa, etc.), la organización de la ICANN debería incluir tanto su definición de trabajo de esos términos como la forma precisa en que la organización de la ICANN los distingue del uso indebido del DNS. Esta página debería incluir enlaces a fragmentos de todas las obligaciones actuales relacionadas con el uso indebido en los contratos con las partes contratadas, incluidos los procedimientos y protocolos para responder ante el uso indebido. La organización de la ICANN debería actualizar esta página anualmente, fechar la última versión y enlazar con versiones anteriores con fechas de publicación	Organización de la ICANN	Alta

	asociadas.		
10.2	Establecer un grupo de trabajo intercomunitario (CCWG), apoyado por el personal, para establecer un proceso de evolución de las definiciones de uso indebido del DNS prohibido, al menos una vez cada dos años, en un calendario previsible (por ejemplo, cada dos años en enero), que no tardará más de 30 días hábiles en completarse. En este grupo, deberían participar las partes interesadas relacionadas con la protección del consumidor, la ciberseguridad operacional, la investigación académica o independiente sobre ciberseguridad, los organismos encargados de exigir el cumplimiento de la ley y el comercio electrónico.	Organización de la ICANN	Alta
10.3	Tanto la Junta Directiva de la ICANN como la organización de la ICANN deberían utilizar las definiciones consensuadas de forma coherente en los documentos públicos, contratos, planes de implementación de equipos de revisión y otras actividades, y que dichos usos hagan referencia a esta página web.	Organización de la ICANN	Alta
Recomendación 11 del SSR2: Resolver los problemas de acceso a los datos del CZDS			
11.1	La comunidad de la ICANN y la organización de la ICANN deberían tomar medidas para garantizar que el acceso a los datos del Servicio de Datos de Zona Centralizado (CZDS) esté disponible, de manera oportuna y sin obstáculos innecesarios para los solicitantes, por ejemplo, la falta de renovación automática de las credenciales de acceso.	Comunidad de la ICANN y Organización de la ICANN	Media
Recomendación 12 del SSR2: Revisar el análisis del uso indebido del DNS y las iniciativas de presentación de informes para permitir la transparencia y la revisión independiente			
12.1	La organización de la ICANN debería crear un equipo asesor de análisis de uso indebido del DNS compuesto por expertos independientes (es decir, expertos sin conflictos de intereses financieros) para recomendar una revisión de la actividad de notificación de uso indebido del DNS con datos procesables, validación, transparencia y reproducibilidad independiente de los análisis como sus máximas prioridades.	Organización de la ICANN	Media
12.2	La organización de la ICANN debería estructurar sus acuerdos con los proveedores de datos para permitir	Organización de la	Media

	un mayor intercambio de datos para uso no comercial, específicamente para la validación o la investigación científica con revisión de pares. Esta licencia especial de uso de datos sin costo y sin fines comerciales puede conllevar un retraso para no interferir con las oportunidades de ingresos comerciales del proveedor de los datos. La organización de la ICANN debería publicar todos los términos del contrato de intercambio de datos en el sitio web de la ICANN. La organización de la ICANN debería rescindir todo contrato que no permita la verificación independiente de la metodología detrás de las listas de bloqueo.	ICANN	
12.3	La organización de la ICANN debería publicar informes que identifiquen los registros y registradores cuyos dominios más contribuyan al uso indebido. La organización de la ICANN debería incluir formatos legibles por computadoras de los datos, además de los datos gráficos de los informes actuales.	Organización de la ICANN	Media
12.4	La organización de la ICANN debería cotejar y publicar informes de las medidas que los registros y registradores han adoptado, tanto de forma voluntaria como en respuesta a obligaciones legales, para responder a los reclamos de conductas ilegales y/o maliciosas en base a las leyes aplicables en relación con el uso del DNS.	Organización de la ICANN	Media
Recomendación 13 del SSR2: Aumentar la transparencia y la responsabilidad en la presentación de reclamos por uso indebido			
13.1	La organización de la ICANN debería establecer y mantener un portal central de reclamos por uso indebido del DNS que dirija automáticamente todas las denuncias de uso indebido a las partes pertinentes. El sistema actuaría puramente como un flujo de entrada, en el cual la organización de la ICANN recopilaría y procesaría solo el resumen y los metadatos, incluidas las marcas de tiempo y los tipos de reclamos (categóricos). El uso del sistema debería ser obligatorio para todos los dominios genéricos de alto nivel (gTLD); la participación de cada dominio de alto nivel con código de país (ccTLD) sería voluntaria. Además, la organización de la ICANN debería compartir los informes de uso indebido (por ejemplo, por correo electrónico) con todos los ccTLD.	Organización de la ICANN	Alta
13.2	La organización de la ICANN debería publicar la cantidad de reclamos presentados en un formulario que permita a terceros independientes analizar los	Organización de la ICANN	Alta

	tipos de reclamos en el DNS.		
Recomendación 14 del SSR2: Crear una especificación temporaria para las mejoras de seguridad basadas en pruebas			
14.1	La organización de la ICANN debería crear una especificación temporaria que exija a todas las partes contratadas mantener el porcentaje de dominios identificados por la actividad de notificación de uso indebido del DNS revisada (véase la Recomendación 13.1 del SSR2) como abusivos por debajo de un umbral razonable y publicado.	Organización de la ICANN	Alta
14.2	Para permitir la adopción de medidas contra el uso indebido, la organización de la ICANN debería proporcionar a las partes contratantes listas de dominios de sus carteras identificados como abusivos, de conformidad con la Recomendación 12.2 del SSR2 relativa a la revisión independiente de los datos y métodos para el bloqueo de dominios.	Organización de la ICANN	Alta
14.3	En caso de que la cantidad de dominios vinculados a actividades abusivas alcance el umbral publicado descrito en la Recomendación 14.1 del SSR2, la organización de la ICANN debería investigar para confirmar la veracidad de los datos y el análisis, y luego emitir una notificación a la parte pertinente.	Organización de la ICANN	Alta
14.4	La organización de la ICANN debería conceder a las partes contratadas 30 días para reducir la fracción de dominios abusivos por debajo del umbral o para demostrar que las conclusiones o los datos de la organización de la ICANN son erróneos. Si una parte contratada no rectifica durante 60 días, el departamento de Cumplimiento Contractual de la ICANN debería pasar al proceso de desacreditación.	Organización de la ICANN	Alta
14.5	La organización de la ICANN debería considerar la posibilidad de ofrecer incentivos financieros: las partes contratadas con carteras con menos de un porcentaje específico de nombres de dominio abusivos deberían recibir una reducción de las tarifas sobre las transacciones cobrables hasta un umbral apropiado.	Organización de la ICANN	Alta
Recomendación 15 del SSR2: Iniciar un EPDP para las mejoras de seguridad basadas en pruebas			
15.1	Después de crear la especificación temporaria (véase la Recomendación 14 del SSR2: Crear una especificación temporaria para las mejoras de	Organización de la ICANN	Alta

	seguridad basadas en pruebas), la organización de la ICANN debería establecer un Proceso Expeditivo de Desarrollo de Políticas (EPDP) apoyado por el personal para crear una política contra el uso indebido. Los voluntarios del EPDP deberían representar a la comunidad de la ICANN, utilizando como plantilla los números y la distribución de la Especificación Temporaria para los Datos de Registración de los gTLD de la carta orgánica del equipo responsable del EPDP.		
15.2	El EPDP debería basarse en la definición de los fundamentos del CCWG propuesta en la Recomendación 10.2 del SSR2. Este marco normativo debería definir las contramedidas y medidas correctivas apropiadas para los diferentes tipos de uso indebido, los plazos para las acciones de las partes contratadas, como los plazos para la presentación de informes de uso indebido / informes de respuesta, y las medidas coercitivas del departamento de Cumplimiento Contractual de la ICANN en caso de infracciones a las políticas. La organización de la ICANN debería insistir en la facultad de rescindir los contratos en caso de que exista en cualquier parte contratada un patrón y práctica de albergar usos indebidos. El resultado debería incluir un mecanismo para actualizar los puntos de referencia y las obligaciones contractuales relacionadas con el uso indebido cada dos años, utilizando un proceso que no requiera más de 45 días hábiles.	Organización de la ICANN	Alta
Recomendación 16 del SSR2: Requisitos de privacidad y RDS			
16.1	La organización de la ICANN debería proporcionar referencias cruzadas coherentes en todo su sitio web para ofrecer información cohesiva y fácil de encontrar sobre todas las acciones (pasadas, presentes y previstas) realizadas sobre el tema de la privacidad y la custodia de datos, con especial atención a la información sobre el Servicio de Directorio de Registración (RDS).	Organización de la ICANN	Media
16.2	La organización de la ICANN debería crear grupos especializados dentro de la función de Cumplimiento Contractual que comprendan los requisitos y principios de privacidad (como la limitación de la recopilación, la calificación de los datos, la especificación de los fines y las medidas de seguridad para la divulgación) y que puedan facilitar las necesidades de aplicación de la ley en el marco del RDS a medida que ese marco sea	Organización de la ICANN	Media

	enmendado y adoptado por la comunidad (véase también la Recomendación 11 del SSR2: Resolver los problemas de acceso a los datos del CZDS).		
16.3	La organización de la ICANN debería realizar auditorías periódicas de la adhesión a las políticas de privacidad implementadas por los registradores para garantizar que cuentan con procedimientos para abordar las infracciones a la privacidad.	Organización de la ICANN	Media
Recomendación 17 del SSR2: Medición de colisiones de nombres			
17.1	La organización de la ICANN debería crear un marco para caracterizar la naturaleza y la frecuencia de las colisiones de nombres y las preocupaciones que generan. Este marco debería incluir métricas y mecanismos para medir el grado de éxito de la interrupción controlada en la identificación y eliminación de colisiones de nombres. Esto podría apoyarse en un mecanismo que permita la divulgación protegida de los casos de colisión de nombres. Este marco debería permitir el manejo adecuado de datos sensibles y amenazas a la seguridad.	Organización de la ICANN	Media
17.2	La comunidad de ICANN debería desarrollar una política clara para evitar y manejar las nuevas colisiones de nombres en relación con los gTLD e implementar esta política antes de la próxima ronda de gTLD. La organización de la ICANN debería asegurarse de que la evaluación de esta política sea llevada a cabo por las partes que no tengan ningún interés financiero en la expansión de los gTLD.	Comunidad de la ICANN y Organización de la ICANN	Media
Recomendación 18 del SSR2: Informar los debates de políticas			
18.1	La organización de la ICANN debería hacer un seguimiento de los avances en la comunidad de investigación con revisión de pares, centrándose en las conferencias de investigación sobre redes y seguridad, que incluya al menos el Sistema de Clasificación Informática (CCS) de la Asociación de Maquinaria Informática (ACM), la Conferencia sobre la medición en Internet de ACM, Usenix Security, la revista CCR, el Grupo de Interés Especial sobre Comunicaciones de Datos (SIGCOMM), el Simposio sobre Seguridad y Privacidad de IEEE, así como las conferencias de seguridad operacional y el Foro de los Equipos de Respuesta a Incidentes y Seguridad (FIRST), y debería publicar un informe para la comunidad de la ICANN	Organización de la ICANN	Baja

	que resuma las implicancias de las publicaciones que son relevantes para la organización de la ICANN o el comportamiento de las partes contratadas.		
18.2	La organización de la ICANN debería asegurarse de que estos informes incluyan las observaciones pertinentes que puedan corresponder a las recomendaciones para la adopción de medidas, incluidos los cambios en los contratos con los registros y registradores, que puedan mitigar, prevenir o remediar los perjuicios en materia de SSR para los consumidores y la infraestructura identificados en la bibliografía revisada por pares.	Organización de la ICANN	Baja
18.3	La organización de la ICANN debería asegurarse de que estos informes también incluyan recomendaciones de estudios adicionales para confirmar las conclusiones revisadas por pares, una descripción de los datos que requeriría la comunidad para ejecutar los estudios adicionales, y cómo la organización de la ICANN puede ofrecerse para ayudar a la intermediación en el acceso a dichos datos, por ejemplo, a través del CZDS.	Organización de la ICANN	Baja
Recomendación 19 del SSR2: Desarrollo completo de la serie de pruebas de regresión del DNS			
19.1	La organización de la ICANN debería completar el desarrollo de una serie de pruebas de comportamiento del resolutor del DNS.	Organización de la ICANN	Baja
19.2	La organización de la ICANN debería asegurarse de que se implemente y mantenga la capacidad de seguir realizando pruebas funcionales de diferentes configuraciones y versiones de software.	Organización de la ICANN	Baja
Recomendación 20 del SSR2: Procedimientos formales para el traspaso de claves			
20.1	La organización de la ICANN debería establecer un procedimiento formal, respaldado por una herramienta de modelado de procesos formales y un lenguaje para especificar los detalles de los futuros traspasos de claves, incluidos los puntos de decisión, los tramos de excepción, el flujo de control completo, etc. La verificación del proceso de traspaso de claves debería incluir la publicación del procedimiento programático (por ejemplo, programa, máquina de estado finito (FSM)) para el comentario público, y la organización de la ICANN debería incorporar los comentarios de la comunidad. El proceso debería tener criterios de	Organización de la ICANN	Media

	aceptación empíricamente verificables en cada etapa, que deberían cumplirse para que el proceso continúe. Este proceso se debería reevaluar al menos con la misma frecuencia que el propio traspaso (es decir, con la misma periodicidad) para que la organización de la ICANN pueda utilizar las lecciones aprendidas para ajustar el proceso.		
20.2	La organización de la ICANN debería crear un grupo de partes interesadas en el que participe el personal pertinente (de la organización de la ICANN o de la comunidad) para realizar periódicamente ejercicios de simulación que sigan el proceso de traspaso de la KSK de la zona raíz.	Organización de la ICANN	Media
Recomendación 21 del SSR2: Mejorar la seguridad de las comunicaciones con los operadores de TLD			
21.1	Las operaciones de la organización de la ICANN y la entidad PTI deberían acelerar la implementación de nuevas medidas de seguridad del Sistema de Gestión de la Zona Raíz (RZMS) en lo que respecta a la autenticación y la autorización de los cambios solicitados y ofrecer a los operadores de TLD la oportunidad de aprovechar esas medidas de seguridad, en particular, la autenticación multifactorial (MFA) y el correo electrónico cifrado.	Organización de la ICANN y PTI	Media
Recomendación 22 del SSR2: Medidas de servicio			
22.1	Para cada servicio sobre el que la organización de la ICANN tiene autoridad, incluida la zona raíz y los servicios relacionados con gTLD, así como los registros de la IANA, la organización de la ICANN debería crear una lista de estadísticas y métricas que reflejen el estado operativo (como la disponibilidad y la capacidad de respuesta) de ese servicio, y debería publicar un directorio de estos servicios, conjuntos de datos y métricas en una única página en el sitio web icann.org, como en la Plataforma de Datos Abiertos. La organización de la ICANN debería elaborar mediciones para cada uno de estos servicios en forma de resúmenes tanto del año anterior como en forma longitudinal (para ilustrar el comportamiento básico de referencia).	Organización de la ICANN	Baja
22.2	La organización de la ICANN debería solicitar anualmente los comentarios de la comunidad sobre las mediciones. Esos comentarios deberían ser	Organización de la ICANN	Baja

	considerados, resumidos públicamente después de cada informe e incorporados en los informes de seguimiento. Los datos y las metodologías asociadas que se utilizan para medir los resultados de estos informes deberían archivarse y ponerse a disposición del público para fomentar la repetibilidad.		
Recomendación 23 del SSR2: Traspaso de algoritmos			
23.1	Las operaciones de PTI deberían actualizar la Declaración de Prácticas de las DNSSEC (DPS) para permitir la transición de un algoritmo de firma digital a otro, incluida una transición anticipada del algoritmo de firma digital RSA a otros algoritmos o a futuros algoritmos post cuánticos, que proporcionen la misma seguridad o mayor seguridad y preserven o mejoren la resiliencia del DNS.	PTI	Media
23.2	Dado que el traspaso de un algoritmo DNSKEY raíz es un proceso muy complejo y delicado, las operaciones de la entidad PTI deberían trabajar con otros socios de la zona raíz y con la comunidad mundial para desarrollar un plan de consenso para futuros traspasos de algoritmos DNSKEY raíz, teniendo en cuenta las lecciones aprendidas del primer traspaso de la KSK de la zona raíz en 2018.	PTI	Media
Recomendación 24 del SSR2: Mejorar la transparencia y las pruebas de extremo a extremo del proceso EBERO			
24.1	La organización de la ICANN debería coordinar las pruebas de extremo a extremo del proceso EBERO completo a intervalos predeterminados (al menos anualmente) utilizando un plan de pruebas que incluya los conjuntos de datos utilizados para las pruebas, los estados de progresión y las fechas límite, y que se coordine con las partes contratadas de la ICANN con antelación para garantizar que se ejerciten todos los tramos de excepción y se publiquen los resultados.	Organización de la ICANN	Media
24.2	La organización de la ICANN debería facilitar la búsqueda del Manual del Proceso de Transición Común mediante la provisión de enlaces en el sitio web de EBERO.	Organización de la ICANN	Media

2. Priorización

El Equipo de Revisión SSR2 ha alineado todas las recomendaciones del SSR2 con el Plan Estratégico 2021-2025 de la ICANN y sus metas y objetivos.[6] El equipo de revisión eliminó las recomendaciones de este informe que no se ajustaban claramente al plan estratégico. Todas las recomendaciones del Equipo de Revisión SSR2 se alinean con el plan estratégico de la organización de la ICANN y, por lo tanto, se consideran importantes.

El Equipo de Revisión SSR2 utilizó una herramienta de encuesta en línea (la solución basada en Internet Qualtrics) para sondear a todos los miembros del equipo a fin de conocer sus aportes sobre la prioridad de cada grupo de recomendaciones del presente informe.[7] Esta encuesta permitió clasificar a cada grupo en una escala de cinco puntos con los siguientes valores: Prioridad muy baja, Prioridad baja, Prioridad media, Prioridad alta y Prioridad muy alta.

El equipo de revisión determinó que, de los veinticuatro grupos de recomendaciones, veintisiete recomendaciones específicas debían considerarse de alta prioridad, la mayoría de las cuales se referían a la gestión de la seguridad interna de la organización de la ICANN y a las medidas contra el uso indebido. Nueve recomendaciones tienen una prioridad medio-alta. Dieciocho recomendaciones, predominantemente de las Secciones del DNS a escala global, se clasificaron como de prioridad media y las ocho recomendaciones restantes se clasificaron como de prioridad inferior.

C. Implementación del SSR1 y resultados esperados

En 2012, la Junta Directiva de la ICANN concluyó *"que las 28 recomendaciones contenidas en el informe final [del SSR1] son factibles y posibles de implementar"*, y aceptó unánimemente e instruyó al personal a implementar todas ellas.[8] Una de las tareas del Equipo de Revisión SSR2 era evaluar "*en qué medida las recomendaciones de la Revisión SSR anterior se han implementado y en qué medida la implementación de dichas recomendaciones ha logrado los resultados esperados"*.

El proceso y la metodología que usó el Equipo de Revisión SSR2 para evaluar las implementaciones y sus resultados se resumen en el Apéndice C: Proceso y metodología. Dicha sección describe el proceso de evaluación, los tipos de evidencia y datos usados, y la metodología adoptada para llegar a una conclusión sobre el nivel de implementación de las recomendaciones. Las conclusiones y el fundamento respaldatorio del Equipo de Revisión SSR2 para cada una de las recomendaciones del SSR1 se incluyen en el Apéndice D: Conclusiones relacionadas con las recomendaciones del SSR1.

[6] Véase el Anexo G: Mapeo de las recomendaciones del SSR2 para el Plan Estratégico 2021-2025 de la ICANN y los Estatutos de la ICANN.

[7] Véase https://www.qualtrics.com/.

[8] ICANN, "Reunión ordinaria de la Junta Directiva de la ICANN", última actualización realizada el 18 de octubre de 2012, https://www.icann.org/resources/board-material/minutes-2012-10-18-en e "Informe Final del Equipo de Revisión de la Seguridad, Estabilidad y Flexibilidad del DNS", Equipo de Revisión de SSR, 20 de junio de 2012, https://www.icann.org/en/system/files/files/final-report-20jun12-en.pdf.

Cada revisión es una oportunidad de aprendizaje y, habiendo evaluado las recomendaciones del SSR1, el Equipo de Revisión SSR2 señala la importancia y la necesidad de proporcionar recomendaciones que se basen en mediciones y con indicadores de desempeño mensurables, algo que generalmente faltó en las recomendaciones del SSR1. Esta observación está avalada por la necesidad de garantizar la implementación y evaluación eficaces de toda recomendación futura del equipo de revisión.

1. Resumen: Revisión de SSR1

El Equipo de Revisión SSR2 revisó las 28 recomendaciones del SSR1 y concluyó que, de las 28 recomendaciones, todas siguen siendo relevantes a la fecha de publicación de este informe (véase Tabla 2).[9] El equipo considera que ninguna recomendación se implementó en su totalidad, por los motivos expuestos en el Apéndice D: Conclusiones relacionadas con las recomendaciones del SSR1.

Tabla 2: Reseña de las recomendaciones del SSR1

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Relevante	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Implementada	P	P	P	P	P	N	P	P	-	P	P	P	N	N	P	P	-	N	-	P	P	P	P	P	P	P	P	P
Efectiva	N	N	N	Y	-	N	N	N	-	N	-	N	N	N	-	N	-	-	N	N	N	N	-	N	N	-	N	N

Clave: Y = Sí N = No P = Parcialmente - = No se puede determinar

El Equipo de Revisión SSR2 destaca las siguientes cuestiones repetitivas:

1. Por lo general, hay falta de indicadores, mediciones y directrices en las recomendaciones del SSR1, y los planes de implementación asociados que permitan a la comunidad y a la organización de la ICANN hacer un seguimiento y comprender el espacio de seguridad y sus propias actividades.

2. No hay evidencia, definiciones ni procedimientos que estén públicamente disponibles, lo que inhibe la observación independiente de las actividades relativas a la SSR. La escasez de información genera una falta de claridad respecto de si la organización de la ICANN ha implementado las recomendaciones del SSR1 y, de ser así, cómo lo ha hecho.

3. No hay revisión ni responsabilidad de la comunidad respecto de los diversos planes de implementación, lo que niega las oportunidades de la comunidad de la ICANN de brindar aportes sobre cuestiones relacionadas con la seguridad, estabilidad y flexibilidad.

4. La organización de la ICANN no tiene actualmente una estrategia general, metas identificables ni una política clara e integral sobre la SSR. Sin una estrategia funcional de SSR ni una gestión de riesgos y seguridad integrada (por ejemplo, políticas, procedimientos, estándares, bases, pautas), las responsabilidades relacionadas con la seguridad, estabilidad y flexibilidad no son asignadas, medidas y rastreadas, lo que genera una falta de transparencia y responsabilidad, y brechas evidentes en las responsabilidades de la organización de la ICANN en relación con la SSR.

[9] ICANN, Informe de implementación de la revisión de SSR, junio de 2015, https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf.

El Equipo de Revisión SSR2 reconoce que las pautas originales suministradas por el Equipo de Revisión SSR1 no fueron en todos los casos suficientemente medidas y, si bien la organización de la ICANN indicó que considera que se abordaron todas las recomendaciones, los planes de implementación de dichas recomendaciones, por lo general, también fueron poco claros y no fueron suficientemente medidos. Por ello, el Equipo de Revisión SSR2 no pudo concluir que la implementación de las recomendaciones del SSR1 estaba completa. La organización de la ICANN debería realizar otra revisión integral de la implementación de las recomendaciones del SSR1, teniendo en cuenta las conclusiones proporcionadas por el Equipo de Revisión SSR2.

Este informe también ofrece sugerencias que van más allá del alcance directo de la revisión del SSR2 (véase Apéndice A: Otras sugerencias) como una forma para que futuros equipos de revisión eviten algunos de los desafíos que enfrentó el Equipo de Revisión SSR2.

Recomendación 1 del SSR2: Revisión adicional del SSR1

1.1. La Junta Directiva de la ICANN y la organización de la ICANN deberían realizar una revisión adicional exhaustiva de las recomendaciones del SSR1 y ejecutar un nuevo plan para completar la implementación de dichas recomendaciones (véase el Apéndice D: Conclusiones relacionadas con las recomendaciones del SSR1).

D. Cuestiones clave de estabilidad dentro de la ICANN

Esta sección se centra en áreas que se relacionan con las secciones 4.6(c) (ii) A, 4.6(c) (ii) B y 4.6(c) (iii) de los Estatutos de la ICANN.[10] Estas áreas se centran en cuestiones relativas a la seguridad, estabilidad y flexibilidad, tanto físicas como aquellas relativas a las redes, en relación con la coordinación de los identificadores únicos de Internet; marco de planificación de contingencia de seguridad para los identificadores únicos de Internet; y compleción y efectividad de los procesos de seguridad interna de la organización de la ICANN y el marco de seguridad de la ICANN.

La cuestión fundamental que informa las recomendaciones de esta sección es la falta de evidencia disponible para el Equipo de Revisión SSR2 que demuestre un programa de SSR eficiente, integral y transparente para la organización de la ICANN. Durante la revisión que realizó el equipo de la seguridad interna de la organización de la ICANN, resultó evidente que la organización de la ICANN estaba llevando a cabo varios proyectos y medidas relevantes para la seguridad. No obstante, el Equipo de Revisión no observó evidencia suficientemente integral de un programa de seguridad y gestión de la información adecuadamente administrado y documentado (véase la sección D.3. Gestión de riesgos y seguridad), de procesos de continuidad de operaciones y recuperación ante desastres (véase la sección D.4. Administración de continuidad de operaciones). o de una estructura de seguridad ampliamente

[10] Véase el Apéndice H: secciones Estatutos y Plan Estratégico más relevantes para las recomendaciones del SSR2 de este informe para una copia de las secciones de los Estatutos y el Plan Estratégico de la ICANN para los años 2021-2025 que son más relevantes para la seguridad, estabilidad y flexibilidad.

independiente adecuada para una organización que soporte un sistema vital para el funcionamiento de Internet (véase la sección D.1. Mejoras a la estructura de la organización).

La organización de la ICANN, de conformidad con sus Estatutos, debe *"desempeñarse, en la máxima medida posible, de manera abierta y transparente, y en concordancia con los procedimientos diseñados para garantizar la equidad"*.[11] Las recomendaciones contenidas en esta sección se ofrecen con el fin de ayudar a la organización de la ICANN a mejorar la divulgación y la transparencia de la SSR en todos los aspectos de la organización en la mayor medida posible teniendo en cuenta los objetivos relativos a la seguridad. Al seguir estas recomendaciones, la organización de la ICANN resolverá, de manera eficiente y eficaz, la cuestión fundamental de transparencia de la información, y la falta claridad y evidencia comprobable del liderazgo y de la organización de seguridad.

1. Mejoras a la estructura de la organización: cargo de alta gerencia de seguridad

Actualmente, la organización de la ICANN divide sus actividades relacionadas con la seguridad, estabilidad y flexibilidad en toda la organización. El Equipo de Revisión SSR2 reconoce los roles de la Oficina del Director de Tecnologías (OCTO), cuyas responsabilidades son, a mero modo enunciativo:

Investigar cuestiones relacionadas con el sistema de identificadores únicos de Internet (nombres de dominio, direcciones IP/números AS, parámetros de protocolo, etc.)

Respaldar la mejora a la seguridad, estabilidad y flexibilidad de dichos identificadores.[12]

Y el Director de Tecnologías de la Información, que generalmente está a cargo del "monitoreo y mantenimiento de los sistemas de la ICANN y de las operaciones técnicas, la seguridad corporativa y la tecnología de la información, y el Equipo de Ingeniería del DNS de la ICANN (*http://www.dns.icann.org/*), *que administra la raíz L y los servicios de red del DNS de la ICANN",*[13] así como de la protección, supervisión y administración de los activos de datos, como los datos privados de las partes contratadas.

La organización de la ICANN debería crear un cargo de alta gerencia ejecutiva a cargo de todas las cuestiones relativas a la seguridad, entre ellas, establecer objetivos estratégicos, administrar el cumplimiento normativo y el presupuesto, y así proteger los activos de la organización.[14]

Varios mandatos contenidos en los Estatutos de la ICANN y compromisos contenidos en el Plan Estratégico de la ICANN para los años fiscales 2021-2025 recaerían en el ámbito de este

[11] Estatutos de la ICANN, sección3.1, https://www.icann.org/resources/pages/governance/bylaws-en/#article3

[12] Oficina del Director de Tecnologías (OCTO), ICANN, consultado el 27 de diciembre de 2019, https://www.icann.org/octo.

[13] ICANN, "Sistemas de información e innovación", consultado el 21 de enero de 2020, https://www.icann.org/resources/pages/technical-functions-cio.

[14] Instituto de Ciencias de la Educación (IES): Centro Nacional para Estadísticas de la Educación, "CAPÍTULO 3: política de seguridad: desarrollo e implementación", consultado el 9 de diciembre de 2020, https://nces.ed.gov/pubs98/safetech/chapter3.asp.

cargo. Además, la recomendación 24 del SSR1 exigía la creación de un Equipo de la Oficina del Director de Seguridad.[15] La estructura actual distribuye estas responsabilidades entre dos unidades separadas dentro de la organización de la ICANN. La administración centralizada impulsaría, de manera más eficiente, la alineación estratégica de todas las actividades relacionadas al consolidar el trabajo en un único rol, con un presupuesto proporcionado.[16] Esto respaldará los esfuerzos para hacer que documentación consistente y coherente esté disponible para la comunidad y futuros equipos de revisión.

Recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos

El Equipo de Revisión SSR2 considera necesario que la organización de la ICANN cuente con un funcionario a nivel de alta gerencia ejecutiva para coordinar y administrar estratégicamente la seguridad y las actividades de riesgo a la seguridad de la organización de la ICANN, e implemente la misión y los objetivos estratégicos de seguridad de la organización de la ICANN.[17]

2.1. La organización de la ICANN debería crear un cargo de Director de Seguridad (CSO) o de Director de Seguridad de la Información (CISO) a nivel de alta gerencia ejecutiva de la organización de la ICANN y contratar a una persona debidamente cualificada para dicho cargo y asignar un presupuesto específico suficiente para desempeñar las funciones de este puesto.

2.2. La organización de la ICANN debería incluir, como parte de la descripción de este cargo, que este puesto gestionará la función de seguridad de la organización de la ICANN y supervisará las interacciones del personal en todas las áreas relevantes que afecten a la seguridad. Este puesto debería ser responsable de proporcionar informes periódicos a la Junta Directiva de la ICANN y a la comunidad sobre todas las actividades relacionadas con la SSR dentro de la organización de la ICANN. Las funciones de seguridad existentes deberían reestructurarse y trasladarse organizativamente para estar subordinadas a este nuevo puesto.

2.3. La organización de la ICANN debería incluir, como parte de la descripción de esta función, que este puesto será responsable de la seguridad estratégica y táctica, y de la gestión de riesgos. Entre esas áreas de responsabilidad se incluye la de estar a cargo y coordinar estratégicamente una función centralizada de evaluación de riesgos, continuidad de operaciones y planificación de la recuperación ante desastres (véase la

[15] Véase el Apéndice D: Conclusiones relacionadas con las recomendaciones del SSR1.

[16] Véase la cláusula 5.1 de las normas de la Organización Internacional de Normalización y las series de normas ISO 27001, ISO/IEC 27001:2013 Tecnología de la Información — Técnicas de seguridad — Sistemas de administración de seguridad de la información — Requisitos, que también se relaciona con SSAE18 2017, Criterios de servicios de confianza, CC1.3/COSO, principio 3, https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/othermapping/trust-services-map-to-iso-27001.xlsx.

[17] La Junta Directiva de la ICANN puede obtener orientación de recursos tales como el Manual de riesgos a la ciberseguridad: Asociación Nacional de Directores Corporativos, “Manual del Director de la NACD sobre la supervisión de riesgos cibernéticos”, 2017, http://boardleadership.nacdonline.org/Cyber-Risk-Handbook-GCNews.html.

recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres) en todo el ámbito de la seguridad interna de la organización, incluido el Servidor Raíz Gestionado por la ICANN (IMRS, comúnmente conocido como Raíz L), y coordinar con otras partes interesadas que participan en el sistema de identificación global externo, así como publicar una metodología y un enfoque de evaluación de riesgos.

2.4. La organización de la ICANN debería incluir, como parte de la descripción de esta función, que esta función será responsable de todas las partidas presupuestarias y responsabilidades relevantes para la seguridad, y participará en todas las negociaciones contractuales relevantes para la seguridad (por ejemplo, acuerdos de registro y registrador, cadenas de suministro para hardware y software, y acuerdos de nivel de servicio asociados) que emprendió la organización de la ICANN, refrendando todos los términos contractuales relacionados con la seguridad.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN haya creado y cubierto el rol de Director de Seguridad con sus responsabilidades, tal como se define en las recomendaciones.

Esta recomendación podrá considerarse efectiva cuando la organización de la ICANN centralice las responsabilidades relativas a la seguridad de manera que pueda coordinar de modo demostrable las actividades y el presupuesto de SSR, y analizar cuestiones de seguridad al nivel administrativo pertinente.

2. Presupuestos e informes relativos a la SSR

Si bien la organización de la ICANN puede abarcar actividades relacionadas con la seguridad, estabilidad y flexibilidad en varias partidas de su presupuesto anual, no queda claro cómo dicha organización actualmente asigna fondos a funciones específicas relativas a la SSR. Esta sección del informe del SSR2 examina la intención y los resultados (en los casos detectables y mensurables) de las recomendaciones del SSR1 relacionadas con la presupuestación y los informes relativos a la SSR.

Las recomendaciones 20, 21 y 22 del SSR1 abordaron varios aspectos de la necesidad de contar con un conjunto más granular y transparente de procesos de presupuestación e informes para las partidas presupuestarias relacionadas con la SSR. Por ejemplo, la recomendación 20 del SSR1 pretendía un mayor grado de granularidad para evaluación y comentario público de las partidas presupuestarias relacionadas con la SSR, así como revisiones periódicas.[18] [19] La recomendación 21 del SSR1 indicaba que la organización de la ICANN debería establecer un proceso interno más estructurado para mostrar cómo las decisiones organizativas y presupuestarias se relacionan con el Marco de IS-SSR, incluido el análisis subyacente de costo-beneficio. La recomendación 22 del SSR aconsejó que la organización de la ICANN publicara, supervisara y actualizara documentación sobre los recursos presupuestarios y organizacionales necesarios para administrar cuestiones relativas a la SSR, en conjunto con la introducción de nuevos gTLD.

[18] Véase el Apéndice D: recomendaciones 20 y 22 del SSR1 para obtener información detallada sobre las conclusiones realizadas por el Equipo de Revisión SSR2 respecto de estas recomendaciones.

[19] ICANN, "Marco de Seguridad, Estabilidad y Flexibilidad del Sistema de Identificadores: año fiscal 2015-2016", 15 de septiembre de 2016, https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

El Equipo de Revisión SSR2 evaluó la medida de la implementación de estas recomendaciones por parte de la organización de la ICANN mediante el análisis de documentos públicamente disponibles, documentos que la organización de la ICANN puso a disposición del equipo de revisión, el informe de implementación del SSR1 y a través de las respuestas recibidas respecto de muchas preguntas enviadas al personal de la organización de la ICANN.[20] La organización de la ICANN no brindó al Equipo de Revisión SSR2 información adicional más allá de la granularidad de lo que el personal compartió con el SSR1, lo que dio como resultado dichas recomendaciones iniciales (recomendaciones 20, 21 y 22 del SSR1). El Equipo de Revisión concluyó que, si bien la presentación de informes anuales sobre las actividades relacionadas con la seguridad, estabilidad y flexibilidad no se realizó mediante los documentos del Marco de IS-SSR y los Informes Anuales, la mayoría de la información relacionada con las cuestiones presupuestarias de la SSR era demasiado general, lo cual no está en concordancia con las recomendaciones formuladas por el Equipo de Revisión SSR1. El presupuesto anual de la organización de la ICANN no brinda información detallada respecto de las actividades relativas a la SSR y los documentos del Marco de IS-SSR ya no se elaboran.[21]

Considerando específicamente el Programa de Nuevos gTLD de la organización de la ICANN, la estructura y el presupuesto del programa nuevo reflejaron, a nivel general, las cuestiones de SSR relacionadas con el Programa de Nuevos gTLD (por ejemplo, Panel de Estabilidad del Sistema de Nombres de Dominio, EBERO).[22] Sin embargo, la organización de la ICANN no logró los resultados esperados de datos más detallados y más claridad en la información respecto de la organización y el presupuesto para implementar el Marco de IS-SSR y desempeñar funciones relativas a la SSR relacionadas con el Programa de Nuevos gTLD. Especialmente, no hay ningún documento en el archivo de documentos de seguridad, estabilidad y flexibilidad del sistema de identificadores (IS-SSR) específico al Programa de Nuevos gTLD.[23] Al examinar los informes anuales y documentos del Marco de IS-SSR de 2016, los gTLD son mencionados dos veces, una vez en el Módulo A como una tendencia en el ecosistema de Internet y nuevamente en el Módulo B como parte del Plan Estratégico general de la ICANN.[24] En el marco anterior, publicado en marzo de 2013, la organización de la ICANN hace mención al Programa de Nuevos gTLD como una “tendencia” y un impulsor de políticas para la Organización de Apoyo para Nombres Genéricos (GNSO).[25] Las únicas menciones restantes del Programa de Nuevos gTLD se encuentran en la sección que informa sobre la

[20] Wiki del Equipo de Revisión SSR2 de la ICANN, materiales de referencia, consultados el 10 de diciembre de 2020, https://community.icann.org/display/SSR/Background+Materials.

[21] ICANN, “Información financiera actual de la ICANN (años fiscales 2020 y 2021)”, sin fecha, https://www.icann.org/resources/pages/governance/current-en, e ICANN, “Archivo de documentos de IS-SSR”, sin fecha, https://www.icann.org/ssr-document-archive. Nota: el presupuesto de la ICANN no informa sobre ningún gasto específico relacionado con la SSR. El archivo de documentos de IS-SSR no muestra ningún documento del Marco de IS-SSR con posterioridad al año fiscal 2015-2016.

[22] ICANN, “Presupuesto adoptado para el año fiscal 2021 de la Corporación para la Asignación de Nombres y Números en Internet (ICANN)”, 7 de mayo de 2020, 26-28, https://www.icann.org/en/system/files/files/adopted-budget-fy21-07may20-en.pdf.

[23] Archivo de documentos de IS-SSR, https://www.icann.org/ssr-document-archive

[24] ICANN, Marco de IS-SSR (año fiscal 2015-2016), https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

[25] ICANN, “Marco de Seguridad, Estabilidad y Flexibilidad”, marzo de 2013, 8, https://www.icann.org/en/system/files/files/ssr-plan-fy14-06mar13-en.pdf.

implementación de las recomendaciones del SSR1. Si bien la organización de la ICANN ha publicado un informe anual que incluye costos directos de recursos compartidos y los costos de las funciones de apoyo asignados a la SSR, este informe no brinda un desglose de los fondos, recursos y otras actividades relacionadas con el Programa de Nuevos gTLD.[26]

Para resumir las inquietudes del Equipo de Revisión respecto de esta área, si bien la organización de la ICANN puede abarcar actividades relacionadas con la seguridad, estabilidad y flexibilidad en varias partidas de su presupuesto anual, sigue sin quedar claro cómo dicha organización asigna fondos a funciones específicas relativas a la SSR. El Equipo de Revisión no pudo encontrar ninguna evidencia de informes sobre impactos al presupuesto y recursos asociados de los eventos de SSR por la organización de la ICANN; si dicho material existe, no es fácil de obtener.

Recomendación 3 del SSR2: Mejorar la transparencia presupuestaria relacionada con la SSR

3.1. El Director Ejecutivo de Seguridad a nivel de alta gerencia (véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos) debe informar a la comunidad, en nombre de la organización de la ICANN, sobre la estrategia, los proyectos y el presupuesto de la ICANN en materia de SSR dos veces al año. y debe actualizar y publicar resúmenes presupuestarios anualmente.

3.2. La Junta Directiva de la ICANN y la organización de la ICANN deberían garantizar que las partidas presupuestarias específicas relacionadas con el desempeño de la organización de la ICANN de las funciones relacionadas con la SSR estén vinculadas a las metas y objetivos específicos del Plan Estratégico de la ICANN. La organización de la ICANN debería implementar esos mecanismos a través de un proceso anual de presupuestación y presentación de informes consistente y detallado.

3.3. La Junta Directiva de la ICANN y la organización de la ICANN deberían crear, publicar y solicitar comentarios públicos sobre los informes detallados relativos a los costos y el presupuesto relacionados con la SSR como parte del ciclo de planificación estratégica.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN traslade todas las funciones y partidas presupuestarias relevantes al nuevo cargo de alta gerencia.

Esta recomendación podrá considerarse efectiva cuando la comunidad de la ICANN tenga una visión transparente del presupuesto relacionado con la seguridad, estabilidad y flexibilidad.

3. Gestión de riesgos y seguridad

La gestión de riesgos en materia de seguridad es un proceso continuo que permite que una organización identifique riesgos relacionados con la seguridad e implemente estrategias para mitigar dichos riesgos. El Equipo de Revisión concluyó que, si bien la organización de la ICANN

[26] ICANN, "Plan Operativo de actividades relacionadas con la SSR (año fiscal 2018)", sin fecha, https://community.icann.org/x/DqNYAw.

inició actividades integrales y pertinentes en el área de gestión de riesgos en materia de seguridad, de las cuales surgieron el informe del Grupo de Trabajo sobre el Marco de Riesgos en el DNS y el Marco de IS-SSR para el año fiscal 2015-2016, los resultados de dichas actividades no se han actualizado.[27] Esta falta de acción pone en duda los esfuerzos de gestión de riesgos en materia de seguridad, en especial, la repetibilidad y la definición de los procesos.

Al no haber documentación actual disponible, el Equipo de Revisión no pudo encontrar evidencia que demostrase el cumplimiento de las normas y mejores prácticas de la industria por parte de la organización de la ICANN.[28] La ausencia de documentación actual incluye la falta importante de auditorías externas sobre el enfoque y la implementación de la organización de la ICANN. Por el contrario, el Equipo de Revisión señala que varias partes contratadas y ccTLD cumplen con las normas relevantes de la industria y en materia de seguridad, y destaca que estas normas se aplican en y para el espacio del DNS.[29] Por último, el Equipo de Revisión no pudo determinar si el trabajo realizado por la organización de la ICANN en el área de gestión de riesgos en materia de seguridad es suficiente.

Ante la ausencia de información actual públicamente disponible, los miembros de la comunidad y otras partes (por ejemplo, gobiernos, registratarios) probablemente tampoco puedan evaluar el trabajo de la organización de la ICANN. Esta ausencia genera una falta de transparencia que afecta los valores fundamentales de la organización de la ICANN y la confianza global en dicha organización y el ecosistema del DNS. La gestión adecuada de riesgos y seguridad requiere procesos claros que cumplan con normas y pautas de mejores prácticas internacionales conocidas, así como responsabilidades y estructura públicamente accesibles. Las auditorías de terceros, si se realizan de acuerdo con normas aceptadas y están seguidas de informes de auditoría públicamente disponibles, brindarán una perspectiva diferente, confirmarán que las medidas son adecuadas y generarán una confianza más sólida entre la comunidad y la organización de la ICANN. La creación y el mantenimiento de estructuras y procedimientos de gestión de seguridad ayudarán a la organización de la ICANN a mantener su posición en materia de seguridad en forma más integral e independientemente de los miembros individuales del personal.

El Equipo de Revisión SSR2 es extremadamente consciente de que el intercambio excesivo de cierta información operativa puede ser problemático, en especial, en el área de seguridad. No obstante, la organización de la ICANN administra un sistema vital con impacto global y debería brindar información relevante a la seguridad y datos asociados a la comunidad. La supervisión de los procesos de divulgación (riesgos, seguridad y vulnerabilidades), incluso la determinación de un plazo de moratoria y divulgación pública, debería recaer en el mandato de la función de

[27] ICANN, "Informe sobre el Marco de Gestión de Riesgos en el DNS", Grupo de Trabajo sobre el Marco de Gestión de Riesgos en el DNS, modificado por última vez el 4 de octubre de 2013, https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en e ICANN, Marco de IS-SSR (año fiscal 2015-2016).

[28] Véase la recomendación 5 del SSR2: Cumplir con los sistemas de gestión de seguridad de la información apropiados y las certificaciones de seguridad, recomendación 6 del SSR2: Divulgación y transparencia sobre vulnerabilidades de SSR, y recomendación 7 del SSR2: Recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres.

[29] Ejemplos de varios ccTLD que están certificados de conformidad con ISO/IEC 27001:2013 o ISO 22301:2012: DENIC https://www.denic.de/en/content-pool/information-security-master/, IIS https://internetstiftelsen.se/docs/27001-eng-Certificate.pdf, nic.at https://www.nic.at/en/the-company/certificates-and-awards, Nominet https://www.nominet.uk/security-at-nominet/.

alta gerencia (véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos).

Recomendación 4 del SSR2: Mejorar los procesos y procedimientos de gestión de riesgos

4.1. La organización de la ICANN debería seguir centralizando su gestión de riesgos y debería articular claramente su marco de gestión de riesgos para la seguridad y asegurarse de que se ajuste estratégicamente a los requisitos y objetivos de la organización. La organización de la ICANN debería describir las medidas relevantes de éxito y cómo evaluarlas.

4.2. La organización de la ICANN debería adoptar e implementar la norma ISO 31000 "Gestión de riesgos" y validar su implementación con auditorías independientes apropiadas.[30] La organización de la ICANN debería poner a disposición de la comunidad los informes de auditorías, posiblemente en una versión editada. Las iniciativas de gestión de riesgos deberían incorporarse a los planes y procedimientos de continuidad de operaciones y recuperación ante desastres (véase la recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres).

4.3. La organización de la ICANN debería nombrar o designar a una persona responsable y dedicada a la gestión de riesgos de seguridad que esté subordinada al cargo de seguridad de alta gerencia (véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos). Esta función debería actualizar periódicamente y proporcionar informes sobre un registro de riesgos de seguridad y guiar las actividades de la organización de la ICANN. Las conclusiones deberían incorporarse a los planes y procedimientos de continuidad de operaciones y recuperación ante desastres (véase la recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres) y el Sistema de Gestión de Seguridad de la Información (ISMS) (véase la recomendación 6 del SSR2: Cumplir con los sistemas de gestión de seguridad de la información apropiados y las certificaciones de seguridad).

Esta recomendación podrá considerarse implementada cuando los procesos de gestión de riesgos de la organización de la ICANN estén suficientemente documentados en virtud de normas internacionales (por ejemplo, ISO31000) y la organización haya establecido un ciclo de auditorías periódicas para este programa que incluyan la publicación de informes de resumen de las auditorías.

Esta recomendación podrá considerarse efectiva cuando la organización de la ICANN tenga un programa de gestión de riesgos sólido y claramente documentado.

Recomendación 5 del SSR2: Cumplir con los sistemas de gestión de seguridad de la información apropiados y las certificaciones de seguridad

[30] Organización Internacional de Normalización, *ISO 31000, Gestión de Riesgos*, https://www.iso.org/iso-31000-risk-management.html.

5.1. La organización de la ICANN debería implementar un ISMS y ser auditada y certificada por un tercero según las normas de seguridad de la industria (por ejemplo, ITIL, serie ISO 27000, SSAE-18) por sus responsabilidades operativas. El plan debería incluir una hoja de ruta y fechas de hitos para obtener certificaciones, y señalar las áreas que serán objeto de mejoras continuas.

5.2. En base al ISMS, la organización de la ICANN debería elaborar un plan de certificaciones y requisitos de capacitación para los cargos en la organización, realizar un seguimiento de los índices de finalización, proporcionar un fundamento para sus decisiones y documentar cómo las certificaciones se ajustan a las estrategias de gestión de seguridad y riesgos de la organización de la ICANN.

5.3. La organización de la ICANN debería exigir a las partes externas que prestan servicios a la organización de la ICANN que cumplan las normas de seguridad pertinentes y documenten su verificación de antecedentes respecto de los proveedores y prestadores de servicios.

5.4. La organización de la ICANN debería contactar a la comunidad y otras partes con informes claros que demuestren lo que está haciendo la organización de la ICANN y lo que está logrando en materia de seguridad. Estos informes serían más beneficiosos si proporcionaran información que describiera cómo la organización de la ICANN sigue las mejores prácticas y procesos desarrollados y en constante mejora para gestionar los riesgos, la seguridad y las vulnerabilidades.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN tenga un Sistema de Gestión de Seguridad de la Información (ISMS) orientado junto a normas aceptadas (por ejemplo, ITIL, serie ISO 27000, SSAE-18) con auditorías periódicas que validen los procedimientos adecuados de administración y gestión de seguridad.

Esta recomendación podrá considerarse efectiva cuando la organización de la ICANN tenga un Sistema de Gestión de Seguridad de la Información que esté ampliamente documentado y aborde correctamente las amenazas actuales a la seguridad y ofrezca planes para abordar posibles amenazas futuras.

Recomendación 6 del SSR2: Divulgación y transparencia sobre vulnerabilidades de SSR

El Equipo de Revisión SSR2 recomienda que la organización de la ICANN mejore sus procesos internos en respaldo de la administración y la generación de informes sobre vulnerabilidades relacionadas con la SSR mediante las acciones siguientes:

6.1. La organización de la ICANN debería promover de forma proactiva la adopción voluntaria de las mejores prácticas relativas a la SSR y los objetivos de divulgación de las vulnerabilidades por las partes contratadas. Si las medidas voluntarias resultan insuficientes para lograr la adopción de dichas mejores prácticas y objetivos, la organización de la ICANN debería implementar las mejores prácticas y los objetivos en los contratos, acuerdos y memorandos de entendimiento.

6.2. La organización de la ICANN debería implementar el proceso para el informe de la divulgación coordinada de vulnerabilidades. Las divulgaciones y la información sobre

cuestiones relacionadas con la SSR, como las infracciones en cualquier parte contratada y en los casos de vulnerabilidades críticas descubiertas y comunicadas a la organización de la ICANN, deberían ser comunicadas rápidamente a las partes de confianza y pertinentes (por ejemplo, los afectados o requeridos para resolver el asunto en cuestión). La organización de la ICANN debería informar de forma periódica sobre las vulnerabilidades (al menos una vez al año) e incluir mediciones anónimas y emplear la divulgación responsable.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN promueva la adopción voluntaria de mejores prácticas relativas a la SSR para las divulgaciones de vulnerabilidades por las partes contratadas e implemente informes de divulgación de vulnerabilidades asociados.

Estas recomendaciones podrán considerarse efectivas cuando la organización de la ICANN y las partes contratadas hayan adoptado mejores prácticas y objetivos relativos a la SSR para la divulgación de vulnerabilidades.

4. Administración de continuidad de operaciones y planificación de recuperación ante desastres

Debido al carácter crítico de las funciones que desempeña la organización de la ICANN, desde el DNS a los registros de la IANA (incluidos la administración y el mantenimiento de registros vitales como la zona raíz, los números AS e IP, y los registros de protocolo), la organización de la ICANN debe comprometerse a realizar una administración de continuidad de operaciones bien planificada, ejecutada y documentada, así como a realizar la planificación de recuperación ante desastres. En función de este rol crítico, el Equipo de Revisión SSR2 considera que la organización de la ICANN debería tener programas de continuidad de operaciones y de recuperación ante desastres más sólidos y mejor organizados. La ICANN se beneficiaría si siguiera mejores prácticas de la industria, en especial, la implementación y documentación de cumplimiento de las normas internacionales aplicables (por ejemplo, ISO/IEC 27001, NIST 800-53). Las auditorías independientes deberían seguir estas acciones para confirmar la idoneidad de los procedimientos.

El equipo revisó la documentación disponible respecto de la continuidad de operaciones y la recuperación ante desastres. La documentación más actualizada databa del año 2017.[31] Tal como se define en las normas ISO 22301 y 22730, la mejor práctica requiere revisiones anuales de estos procedimientos y políticas. Las auditorías independientes son necesarias para garantizar que los planes de continuidad de operaciones y de recuperación ante desastres estén actualizadas y en consonancia con las mejores prácticas adecuadas para el carácter crítico del DNS. En general, el Equipo de Revisión SSR2 y los miembros del personal de la organización de la ICANN no pudieron encontrar y presentar documentación suficientemente detallada que permitiera una evaluación adecuada de la implementación de los planes de

[31] Wiki del SSR2, Equipo de Revisión, Documentos y borradores del Equipo de Revisión, "preguntas y respuestas del SSR2", sin fecha, 2, https://community.icann.org/pages/viewpage.action?pageId=64076120. Nota: en virtud de las entrevistas con el personal de la ICANN, "estos documentos son confidenciales y no se publican de manera pública por razones de seguridad. Existe un plan de recuperación ante desastres establecido para los sistemas, un plan de continuidad para las funciones de la IANA y un plan de continuidad más amplio en desarrollo para la organización de la ICANN en general que se entregará en el año 2019".

continuidad de operaciones y recuperación ante desastres de la organización de la ICANN. La organización de la ICANN tiene capacidad para mejoras significativas en la forma en que maneja la continuidad de operaciones y la recuperación ante desastres para las funciones esenciales que proporciona.[32]

El cumplimiento de normas internacionales bien establecidas, tal como lo confirmaron las auditorías externas realizadas por terceros, es vital para toda organización que opera infraestructura crítica para Internet, incluso si dicho cumplimiento no es exigido por ley. Los expertos externos contribuirían a la transparencia y legitimidad de los procedimientos y planes de continuidad de operaciones y recuperación ante desastres de la organización de la ICANN mediante una licitación pública de auditores, junto con la posterior publicación de informes finales (de ser necesario, editados) de auditoría. En particular, la norma ISO 31000 "Gestión de Riesgos", la serie de normas ISO/IEC 27000 "Sistemas de gestión de seguridad de la información" y la norma ISO 22301 "Gestión de Continuidad de Operaciones" serían de gran utilidad como guía y, más importante aún, servirían como normas objetivo para las auditorías independientes de terceros.[33] Si bien la organización de la ICANN es única en su infraestructura organizativa y misión, las normas ISO son flexibles y aplicables a la organización de la ICANN, en particular, en lo que respecta a la organización de la ICANN y las funciones de la IANA. El Equipo de Revisión también considera el uso de las normas NIST adecuadas, siempre que la organización de la ICANN documente ampliamente el proceso y sea auditada independientemente por un tercero respetado.[34]

Evaluar los procesos de continuidad de operaciones y recuperación ante desastres adecuados implica trabajo que se basa en actividades de evaluación de riesgos más generales, como se describe en la sección D.3. Gestión de riesgos y seguridad mencionada anteriormente. La ICANN brinda apoyo a un sistema crítico para el funcionamiento de Internet y, por lo tanto, está un nivel por encima de los requisitos normales para continuidad de operaciones y recuperación ante desastres. Un presunto compromiso de los procedimientos relativos a la clave para la firma de la llave de la zona raíz (KSK), en particular, durante una crisis, constituiría un problema considerable y debe ser evitado. Los turbulentos problemas mundiales del año 2020, desde la pandemia de la COVID-19 hasta significativos disturbios sociales, demuestran cómo tener dos sitios en el mismo país (en este caso, los Estados Unidos) no resulta suficiente y ha ocasionado niveles inesperadamente altos de riesgo para la función de continuidad de operaciones y recuperación ante desastres dentro de la organización de la ICANN. De igual modo, las prohibiciones de viajes afectan a diferentes sitios dentro de los Estados Unidos y también se produjeron eventos violentos en la mayoría de las ciudades importantes del país.

---

[32] El equipo tiene en cuenta que el ISMS, la continuidad de operaciones, la recuperación ante desastres y la gestión de riesgos conforme a las normas ISO interactúan y son interdependientes. No obstante, el equipo consideró apropiado brindar detalles sobre necesidades identificadas, implementación y pasos necesarios.

[33] Organización Internacional de Normalización, normas y series de normas *ISO 31000*, *ISO/IEC 27000:2018 Tecnología de la Información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Generalidades y vocabulario,* e *ISO 22301:2019 Seguridad y flexibilidad — Sistemas de gestión de continuidad de negocios — Requisitos.*

[34] Departamento de Comercio de Estados Unidos, Instituto Nacional de Normas y Tecnología. *Publicación especial (SP) de NIST 800-30 Rev. 1, Guía para realizar evaluaciones de riesgos*. Gaithersburg, MD: Departamento de Comercio de EE. UU, 2012. https://doi.org/10.6028/NIST.SP.800-30r1 y Departamento de Comercio de Estados Unidos, Instituto Nacional de Normas y Tecnología, Centro de Recursos de Seguridad Informática. *SP 800-53 Revisión 5 Controles de seguridad y privacidad para organizaciones y sistemas de información*. Gaithersburg, MD: Departamento de Comercio de EE. UU, 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

Además, si bien es muy poco probable, ambos sitios podrían verse afectados por otros eventos adversos, como terremotos, incendios u otros desastres naturales. Los tipos de riesgos que pueden afectar a las operaciones de la organización de la ICANN evolucionarán y la organización de la ICANN debe responder en consecuencia mediante evaluaciones periódicas y documentadas de los planes de continuidad de operaciones y recuperación ante desastres, incluidas la planificación y la ejecución adecuadas y oportunas donde se necesiten cambios.

Recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres

7.1. La organización de la ICANN debería establecer un Plan de Continuidad de Operaciones para todos los sistemas que sean de propiedad o estén bajo el ámbito de competencia de la organización de la ICANN, basado en la norma ISO 22301 "Gestión de Continuidad de Operaciones", en el que se identifiquen los plazos aceptables de continuidad de operaciones y recuperación ante desastres.[35]

7.2. La organización de la ICANN debería asegurarse de que el plan de recuperación ante desastres para las operaciones de los Identificadores Técnicos Públicos (PTI) (es decir, las funciones de la IANA) incluya todos los sistemas relevantes que contribuyan a la seguridad y estabilidad del DNS, y también incluya la Gestión de la Zona Raíz y esté en consonancia con la norma ISO 27031.[36] La organización de la ICANN debería desarrollar este plan en estrecha colaboración con el Comité Asesor del Sistema de Servidores Raíz (RSSAC) y los Operadores de Servidores Raíz (RSO).

7.3. La organización de la ICANN también debería establecer un plan de recuperación ante desastres para todos los sistemas que son propiedad o se encuentran dentro del ámbito de competencia de la organización de la ICANN, nuevamente en consonancia con la norma ISO 27031.

7.4. La organización de la ICANN debería establecer un nuevo sitio para la recuperación ante desastres para todos los sistemas que son propiedad o se encuentran dentro del ámbito de competencia de la organización de la ICANN con el objetivo de reemplazar los sitios de Los Ángeles o Culpeper o agregar un tercer sitio permanente. La organización de la ICANN debería localizar este sitio fuera de la región de América del Norte y de cualquier territorio de los Estados Unidos. Si la organización de la ICANN decide reemplazar uno de los sitios existentes, el sitio al que la organización de la ICANN reemplace no debería cerrarse hasta que la organización haya verificado que el nuevo sitio esté plenamente operativo y sea capaz de gestionar la recuperación ante desastres de estos sistemas para la organización de la ICANN.

7.5. La organización de la ICANN debería publicar un resumen de sus planes y procedimientos generales de continuidad de operaciones y recuperación ante desastres. De esta manera, mejoraría la transparencia y la confianza, además de abordar las metas y objetivos estratégicos de la organización de la ICANN. La

[35] ISO 22301:2019

[36] Organización Internacional de Normalización, normas y series de normas *ISO 27031, ISO/IEC 27031:2011 Tecnología de la Información — Técnicas de seguridad — Pautas para la preparación de la tecnología de la información y comunicación para la continuidad de operaciones.*

organización de la ICANN debería contratar a un auditor externo para verificar el cumplimiento de estos planes de continuidad de operaciones y recuperación ante desastres.

Esta recomendación podrá considerarse implementada cuando los planes y procesos de continuidad de operaciones y recuperación ante desastres de la organización de la ICANN estén completamente documentados de conformidad con las normas aceptadas de la industria, incluidas auditorías periódicas que indiquen que se están siguiendo dichos procesos y cuando un sitio que no sea norteamericano, que no sea de Estados Unidos, esté operativo.

Esta recomendación podrá considerarse efectiva cuando la organización de la ICANN pueda demostrar cómo puede manejar incidentes que afectan a todo Estados Unidos o Norteamérica.

E. Contratos, cumplimiento y transparencia en torno al uso indebido del DNS

Desde su fundación, la misión de la ICANN ha incluido *"coordinar el desarrollo y la implementación de políticas que sean desarrolladas a través de un proceso de múltiples partes interesadas, ascendente y basado en consenso, y diseñadas para garantizar el funcionamiento estable y seguro de los sistemas de nombres únicos de Internet"*.[37] El Equipo de Revisión SSR2 concluye que, a pesar del compromiso mencionado, el sistema actual coordinado de la ICANN no aborda con suficiencia el uso indebido del DNS y sus daños asociados. Los grupos dentro y fuera de la comunidad de la ICANN han notado esta brecha durante muchos años.[38] Algunas de las comunicaciones más señaladas sobre este tema provienen de representantes de los gobiernos del mundo mediante el Comité Asesor Gubernamental (GAC), quienes han afirmado durante más de una década que no consideran que los procesos y procedimientos de la ICANN sean suficientes para abordar los intereses en materia de seguridad pública.[39]

El uso indebido del DNS para fines fraudulentos o delictivos existe desde antes de la organización de la ICANN.[40] El escenario de las amenazas, que solía rondar en torno a spam, phishing y fraude, se ha ampliado para incluir ataques más sofisticados, por ejemplo, malware, ransomware y correo electrónico corporativo comprometido (BEC), que apuntan a empresas,

[37] Estatutos de la ICANN, Sección 1.1(a), https://www.icann.org/resources/pages/governance/bylaws-en/#article1.

[38] Ejemplos: "Carta abierta a la comunidad de la ICANN del Grupo de Partes Interesadas de Registros", 19 de agosto de 2020, https://docs.wixstatic.com/ugd/ec8e4c_00d2dbac27b24330b8342686e9c2e53a.pdf, y una carta de la Unidad Constitutiva de Negocios de la ICANN a la Junta Directiva de la ICANN, Göran Marby, Presidente y Director Ejecutivo de la ICANN,, Keith Drazek, Presidente del Consejo de la GNSO, y la comunidad de la ICANN, 28 de octubre de 2019, https://www.bizconst.org/assets/docs/positions-statements/2019/2019_10October_28%20BC%20Statement%20on%20DNS%20Abuse.pdf.

[39] Comité Asesor Gubernamental de la ICANN, "Declaración del GAC sobre el uso indebido del DNS", 18 de septiembre de 2019, 1, https://gac.icann.org/file-asset/public/gac-statement-dns-abuse-final-18sep19.pdf.

[40] Véase el Apéndice F: Datos de investigación sobre informes de tendencias del uso indebido del DNS para obtener más información sobre las tendencias históricas en este espacio.

gobiernos e Internet de las cosas (IoT).[41] Ahora, entre los actores maliciosos se incluyen actores comerciales y con patrocinio estatal que desarrollan plataformas industriales para respaldar el uso indebido. La pandemia de la COVID-19 y las cuarentenas asociadas han proporcionado un mayor espacio de ataques para los delincuentes oportunistas.[42]

Como se señala más abajo en la sección E.1. Medidas de protección no logradas para el Programa de Nuevos gTLD, el uso indebido del DNS fue una preocupación clave de todas las partes interesadas en ese momento, y la organización de la ICANN tuvo varias oportunidades para elaborar políticas diseñadas para garantizar el funcionamiento estable y seguro del sistema de nombres únicos de Internet durante la expansión del espacio de nombres global. La organización de la ICANN tuvo la oportunidad de servir como líder en guiar a todas las comunidades de seguridad y del DNS hacia un conjunto común de términos, definiciones y datos que facilitarían la comunicación y colaboración, como se señala en la sección E.2. Desafíos: definiciones y datos.

Estas oportunidades aún existen para la organización de la ICANN. Las recomendaciones incluidas en esta sección ofrecen a la organización de la ICANN sugerencias específicas respecto de dónde y cómo mejorar el cumplimiento de nuestra propia misión y servir como un líder más fuerte en las comunidades de seguridad y del DNS.

1. Medidas de protección no logradas para el Programa de Nuevos gTLD

El uso indebido del DNS fue una preocupación clave en el lanzamiento del Programa de Nuevos gTLD en 2010. Organismos de aplicación de la ley, gobiernos, comunidades de seguridad y grupos de interés comerciales y de usuarios debatieron sobre las obligaciones contractuales relativas a la mitigación del uso indebido tanto en el Acuerdo Base de Registro de los Nuevos gTLD como en el Acuerdo de Acreditación de Registradores (RAA) de 2013. Como parte de estas deliberaciones, la comunidad de la ICANN preparó un memorando en 2009 en el que se proponían medidas para mitigar la conducta maliciosa en el Programa de Nuevos gTLD.[43] El memorando incluía recomendaciones para investigar a operadores de registro, definir contratos y procedimientos relativos al uso indebido a nivel de registros, y acceso centralizado a los archivos de zona. Lamentablemente, había una brecha entre las medidas descriptas en este memorando y lo surgido de las negociaciones cerradas entre la organización de la ICANN y los registros. Intentos posteriores por mejorar las prácticas en materia de seguridad mediante enmiendas contractuales recibieron críticas debido a la falta de transparencia y participación de la comunidad en el proceso.[44]

[41] Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN, "SAC105: El DNS y la Internet de las Cosas: oportunidades, riesgos y desafíos" 28 de mayo de 2019, https://www.icann.org/en/system/files/files/sac-105-en.pdf.

[42] Interpol, "Panorama mundial sobre las amenazas cibernéticas durante la pandemia de la COVID-19", abril de 2020, https://www.interpol.int/en/content/download/15217/file/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf.

[43] ICANN, "Mitigación de conductas maliciosas", Memorando explicativo de nuevos gTLD, 3 de octubre de 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf.

[44] Unidad Constitutiva de Negocios de la GNSO de la ICANN, "Comentario sobre las enmiendas propuestas al Acuerdo base de Registro de Nuevos gTLD," presentación de la Unidad Constitutiva de Negocios, versión 3, 20 de julio de 2016, https://www.bizconst.org/assets/docs/positions-

En 2013, el Equipo de Revisión de Competencia, Confianza y Elección de los Consumidores (CCT) de la ICANN revisó la eficacia de estas medidas de protección destinadas explícitamente a mitigar las tasas de actividad maliciosa, delictiva y de uso indebido en estos nuevos gTLD. El equipo de CCT encargó un estudio de investigación independiente (de aquí en adelante, el informe de SAGAD) que usó fuentes de datos públicos para mostrar que las tasas de uso indebido en los nuevos gTLD eran más altas que en los TLD legados, lo que implicaba que las medidas de protección no eran eficaces.[45] El informe Final del CCT concluyó:

"Aunque el uso indebido no persiste de forma universal en todos los nuevos gTLD, es endémico en muchos de ellos. Lo que resulta más preocupante en la actualidad es que hay pocos recursos para que la comunidad detenga los registros y registradores de nuevos gTLD y asociados con altos niveles de uso indebido. Esto, a su vez, genera incentivos para que los operadores de redes bloqueen unilateralmente todo el tráfico de TLD o registradores específicos, lo cual va en contra de los objetivos de la comunidad para la aceptación universal de nuevos gTLD.

La incapacidad de prevenir la propagación de ciertas actividades relacionadas con el uso indebido a nuevos gTLD previamente identificados por la comunidad es significativa. El Equipo de Revisión de CCT reconoce la función de infraestructura que desempeñan los nombres de dominio para permitir actividades relacionadas con el uso indebido que afectan la seguridad, la estabilidad y la flexibilidad del DNS, socavan la confianza del consumidor y, en última instancia, afectan a usuarios finales de todo el mundo. En consecuencia, este es un tema de alta prioridad que debe abordarse antes de cualquier expansión adicional del DNS, y el Equipo de Revisión ofrece varias recomendaciones para remediar las deficiencias del statu quo y mejorar la seguridad del DNS".[46]

La revisión de CCT y el informe de SADAG asociado, así como otros informes de terceros, también detectaron que, después del lanzamiento del Programa de Nuevos gTLD, algunos registros y registradores oportunamente establecieron prácticas a fin de aumentar rápida y considerablemente las registraciones de dominios, por ejemplo, registraciones masivas, muchas de las cuales se usan para actividades delictivas y con fines de uso indebido.[47] Spamhaus (entre otros) también publica lo que estima como los registradores y TLD con mayor

statements/2016/2016_07july_20%20bc%20comment%20on%20proposed%20gtld%20base%20registry%20agreement%20final.pdf.

[45] Korczyński, Maciej , Maarten Wullink, Samaneh Tajalizadehkhoob, Giovane C.M. Moura y Cristian Hesselman, "Informe Final del análisis estadístico del uso indebido del DNS en los gTLD", SIDN Labs y Delft University of Technology, agosto de 2017, consultado el 2 de agosto de 2018, https://www.icann.org/public-comments/sadag-final-2017-08-09-en.

[46] Equipo de Revisión de Competencia, Confianza y Elección de los Consumidores, "Competencia, Confianza y Elección de los Consumidores: Informe Final", ICANN, 8 de septiembre de 2018, https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf, y Piscatello, Dave, "Transformación de nombres de dominio en armas: cómo la registración masiva ayuda a las campañas globales de spam", Spamhaus, 21 de marzo de 2020, https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns.

[47] Ibídem, y Piscitello, Dave, "Transformación de nombres de dominio en armas: cómo la registración masiva ayuda a las campañas globales de spam", Spamhaus, 21 de marzo de 2020, https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns.

uso indebido y ciertas entidades aparecen año tras año en estas listas.[48] Alpnames, destacado en el informe de SADAG como una de los registradores más notorios implicado en el uso indebido del DNS, ofrecía registraciones masivas a bajo precio y "*ha actuado como el registrador patrocinante para el 53.97 % (59 044) de los dominios de nuevos gTLD que han sido colocados en la lista negra por Spamhaus*".[49] El Departamento de Cumplimiento Contractual de la ICANN no abordó de manera suficiente este uso indebido continuo y sistemático, incluso después de que muchas organizaciones llamaron la atención al respecto.[50] Cumplimiento Contractual de la ICANN no desacreditó a Alpnames hasta después de que supo que Alpnames había dejado de operar.[51] Nuestra esperanza es que la organización de la ICANN y la industria del DNS puedan demostrar un progreso mensurable en la prevención y mitigación del uso indebido del DNS. De lo contrario, los gobiernos probablemente lleguen a la conclusión de que el modelo de autogobernanza de la industria de la ICANN ya no cumpla su propósito.

Como se señaló en la Revisión de WHOIS2/RDS, Cumplimiento Contractual de la ICANN tiene la oportunidad de ser más proactivo al abordar "*problemas sistémicos sospechosos, reclamos de inexactitud informados, estudios o revisiones de exactitud del RDS o Informes de Actividades de Uso Indebido de Dominios (DAAR) respecto de investigar, analizar y aplicar la ley frente a la inexactitud en los datos de registración*".[52]

Recomendación 8 del SSR2: Permitir y demostrar la representación del interés público en las negociaciones con las partes contratadas

8.1. La organización de la ICANN debería encargar a un equipo de negociación que incluya expertos en uso indebido y seguridad no afiliados o pagados por las partes contratadas que representen los intereses de las entidades no contratadas y que

[48] Spamhaus, "Los TLD que sufren más uso indebido en el mundo", consultado el 5 de diciembre de 2020, https://www.spamhaus.org/statistics/tlds/, y Spamhaus, "Los registradores de dominios que sufren más uso indebido del mundo", consultado el 5 de diciembre de 2020, https://www.spamhaus.org/statistics/registrars/. Nota: el material de respaldo en las páginas de Spamhaus ofrece una perspectiva sobre cómo determinan los registradores y dominios "malos".

[49] Informe de SADAG, 19, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf.

[50] Carta de Adobe Systems, DomainTools, eBay, Facebook, Microsoft y Time Warner (también conocidos como Grupo de Trabajo de Cumplimiento Independiente) a Jamie Hedlund, Vicepresidente Sénior, Cumplimiento Contractual y Medidas de Protección al Consumidor, y Director Ejecutivo de la Oficina de Washington, D.C., 27 de febrero de 2018, https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf.

[51] Carta de Jamie Hedlund, Vicepresidente Sénior, Cumplimiento Contractual y Medidas de Protección al Consumidor, y Director Ejecutivo de la Oficina de Washington, D.C., a Iain Roache, Alpnames Limited, "sobre: NOTIFICACIÓN DE RESCISIÓN DE ACUERDO DE ACREDITACIÓN DE REGISTRADORES", 15 de marzo de 2019, https://www.icann.org/uploads/compliance_notice/attachment/1113/hedlund-to-roache-15mar19.pdf.

[52] Equipo de Revisión RDS-WHOIS2, "Informe Final de Revisión de Servicio de Directorio de Registración (RDS)-WHOIS2", 3 de septiembre de 2019, https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf, 46. Nota: véase recomendación R4.1: "*La Junta Directiva de la ICANN debería iniciar acciones para asegurarse de que Cumplimiento Contractual de la ICANN supervise y haga cumplir de manera proactiva las obligaciones de los registradores con respecto a la exactitud de los datos del RDS (WHOIS) con los datos de los reclamos de inexactitud recibidos y los estudios o revisiones de exactitud del RDS para buscar y abordar problemas sistémicos. Se debería ejecutar un enfoque basado en los riesgos para evaluar y comprender los problemas de inexactitud y luego tomar las medidas apropiadas para mitigarlos.*

trabajen con la organización de la ICANN para renegociar los contratos de las partes contratadas de buena fe, con transparencia pública y con el objetivo de mejorar la SSR del sistema de nombres de dominio para los usuarios finales, las empresas y los gobiernos.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN haya incluido especialistas en seguridad y uso indebido en estas negociaciones y la administración del sistema de nombres de dominio esté en consonancia con la seguridad pública y los intereses del consumidor, y no solo aquellos de la industria de nombres de dominio.

Esta recomendación podrá considerarse efectiva cuando un grupo más amplio y más equilibrado de partes interesadas puedan tener aportes directos a los contratos negociados con las partes contratadas.

Recomendación 9 del SSR2: Supervisar y exigir el cumplimiento

9.1. La Junta Directiva de la ICANN debería ordenar al equipo de cumplimiento que supervise y exija el cumplimiento estricto de las partes contratadas de las obligaciones actuales y futuras en materia de SSR y de uso indebido en los contratos, los acuerdos base, las especificaciones temporarias y las políticas de la comunidad.

9.2. La organización de la ICANN debería supervisar y exigir de forma proactiva el cumplimiento de las obligaciones contractuales del registro y del registrador para mejorar la exactitud de los datos de registración. Esta supervisión y control del cumplimiento deberían incluir la validación de los campos de dirección y la realización de auditorías periódicas sobre la exactitud de los datos de registración. La organización de la ICANN debería centrar sus esfuerzos para garantizar el cumplimiento en aquellos registradores y registros que hayan sido objeto de más de 50 reclamos o denuncias por año ante la organización de la ICANN en relación con su inclusión de datos inexactos.

9.3. La organización de la ICANN debería asegurarse de que las actividades de cumplimiento sean auditadas externamente por lo menos una vez al año y publicar los informes de auditoría y la respuesta de la organización de la ICANN a las recomendaciones de la auditoría, incluidos los planes de implementación.

9.4. La organización de la ICANN debería encargar a la función de Cumplimiento Contractual la publicación de informes periódicos que enumeren las herramientas que les faltan y que les ayudarían a apoyar a la organización de la ICANN en su conjunto a utilizar eficazmente los mecanismos contractuales para hacer frente a las amenazas a la seguridad del DNS, incluidas las medidas que requerirían cambios en los contratos.

Esta recomendación podrá considerarse implementada cuando las auditorías se lleven a cabo periódicamente y se publiquen los resúmenes.

Esta recomendación podrá considerarse efectiva cuando la organización de la ICANN haya finalizado correctamente una auditoría e informado sus resultados a la comunidad.

Esta recomendación requiere acción de la Junta Directiva y la organización de la ICANN. Es posible que la Junta deba actualizar su posición y sus instrucciones una vez finalizado el

Proceso Expeditivo de Desarrollo de Políticas (EPDP) contra el uso indebido (véase la recomendación 15 del SSR2: Iniciar un EPDP para las mejoras de seguridad basadas en pruebas).

2. Desafíos: Definiciones y acceso a datos

El Equipo de Revisión SSR2 detectó dos tipos de desafíos persistentes para avanzar; uno relacionado con las definiciones y el alcance de uso indebido que las obligaciones contractuales de la ICANN pueden administrar y el otro relacionado con el acceso a los datos que pueden informar la detección, mitigación, prevención y respuesta respecto del uso indebido. Las recomendaciones 11 a 14 del SSR2 apuntan hacia una mejor transparencia y responsabilidad en las dos áreas.

A. Definición de uso indebido

Durante un diálogo llevado a cabo en abril de 2018 con el Equipo de Revisión SSR2, Cumplimiento Contractual de la ICANN afirmó que los contratos actuales con los registros y registradores no autorizan a la organización de la ICANN a exigirles a los registros que suspendan o eliminen nombres de dominio posiblemente usados indebidamente y, por ende, no son eficaces para permitirles buscar aquellos implicados en el uso indebido sistemático del DNS.[53] Este punto también fue afirmado de manera pública en la carta de Cumplimiento Contractual de la ICANN al Grupo de Trabajo de Cumplimiento Independiente.[54]

Un año más tarde, en abril de 2019, Cumplimiento Contractual de la ICANN informó al Equipo de Revisión SSR2 que la falta de una prohibición contractual sobre el "uso indebido sistemático del DNS" impide que Cumplimiento Contractual de la ICANN lo aborde de manera eficaz hasta que haya una política de consenso de la comunidad que lo defina o lo prohíba.[55] Además, la Junta Directiva de la ICANN recientemente anunció que se demoraría en avanzar con las recomendaciones 14 y 15 de la Revisión de CCT, las cuales recomiendan enmiendas a los acuerdos existentes para ayudar a prevenir el uso indebido del DNS. La Junta destacó que esta demora se debe a que "*aún hay discusiones en curso de la comunidad para llegar a un entendimiento común del uso indebido del DNS y los términos relacionados*".[56] El Equipo de Revisión SSR2 observa que la naturaleza no estructurada e ilimitada de estas discusiones no permite encontrar una solución, y que la organización de la ICANN y las partes contratadas

[53] Materiales informativos: Debate con Cumplimiento de la ICANN - Finalizado el 14 de mayo de 2019, Respuesta de Cumplimiento de la ICANN a preguntas del SSR2 al 26 de abril de 2019, https://community.icann.org/display/SSR/Briefing+Materials.

[54] Carta de Jamie Hedlund, Vicepresidente Sénior, Cumplimiento Contractual y Medidas de Protección al Consumidor, y Director Ejecutivo de la Oficina de Washington, D.C., al Grupo de Trabajo de Cumplimiento Independiente, "sobre: Carta del 27 de febrero de 2018 del Grupo de Trabajo de Cumplimiento Independiente", 4 de abril de 2018, https://www.icann.org/en/system/files/correspondence/hedlund-to-vayra-04apr18-en.pdf. Véase también nota al pie sobre: Carta del 27 de febrero de 2018 del Grupo de Trabajo de Cumplimiento Independiente.

[55] Materiales informativos, https://community.icann.org/display/SSR/Briefing+Materials, 4. Nota: véase la respuesta a la pregunta 6.

[56] Junta Directiva de la ICANN, "Resoluciones aprobadas | Reunión ordinaria de la Junta Directiva de la ICANN", orden del día principal, recomendaciones pendientes del Equipo de Revisión de Competencia, Confianza y Elección de los Consumidores(CCT-RT), 22 de octubre de 2020, https://www.icann.org/resources/board-material/resolutions-2020-10-22-en#2.a.

tienen un incentivo para posponer la solución de este problema de manera indefinida. Recomendamos un enfoque de tres vías a este problema, que incluya una especificación temporaria a corto plazo, un CCWG con tiempo limitado a mediano plazo y un EPDP a más largo plazo.

Hace más de una década que la organización de la ICANN tiene descripciones y definiciones de trabajo de "uso indebido del DNS" y términos relacionados integrados con sus actividades, incluidos, por ejemplo, marcos de seguridad, estabilidad y flexibilidad de la organización de la ICANN desde 2009 hasta 2017,[57] las conclusiones de consenso de la comunidad de la ICANN en el Programa de Nuevos gTLD así como el posterior consenso sobre las medidas de protección,[58] la obligación contractual de la Especificación 11b de 2013 que enumera las actividades que implican uso indebido,[59] y el propio proyecto de la ICANN de Informe de Actividades de Uso Indebido de Dominios (DAAR).[60]

El Consejo de la GNSO también solicitó que el Grupo de Trabajo sobre Políticas de Uso Indebido de Registraciones (RAPWG) examinara cuestiones en torno a usos ilícitos de nombres de dominio. El informe final indicó:

"*El RAPWG reconoce que el ciberdelito es un problema importante que padece la comunidad de la ICANN. La comunidad de Internet con frecuencia manifiesta preocupación a la ICANN sobre la conducta maliciosa y, en particular, la medida en que los delincuentes aprovechan los servicios de registro de dominios y resolución de nombres. Varias partes, entre las que se incluyen compañías, consumidores, gobiernos y organismos de aplicación de la ley, están solicitando a la ICANN y a sus partes contratadas que supervisen la conducta maliciosa y,*

[57] Archivo de documentos de IS-SSR, https://www.icann.org/ssr-document-archive.

[58] Grupo de Trabajo sobre Políticas de Uso Indebido de Registraciones de la GNSO de la ICANN, "Informe Final del Grupo de Trabajo sobre Políticas de Uso Indebido de Registraciones", 29 de mayo de 2010. https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf, 3. Nota: este informe definió uso indebido como *"una acción que: a) provoca un daño real y sustancial, o constituye un fundamento material de perjuicio, y b) es ilegal o ilegítimo, o de otro modo contrario a la intención y el diseño de un propósito legítimo indicado, si dicho propósito fuese revelado"*. Véase también, Investigación de políticas y operaciones de la ICANN, Medidas de seguridad del Programa de Nuevos gTLD contra el uso indebido del DNS", julio de 2016, https://newgtlds.icann.org/en/reviews/dns-abuse/safeguards-against-dns-abuse-18jul16-en.pdf, 3. Nota: este informe también usó la distinción del Grupo de Trabajo sobre Políticas de Uso Indebido de Registraciones (RAPWG) entre uso indebido de *registros* y de *abuso de uso*, y señaló que el uso indebido de registraciones se encuentra más claramente en el alcance de la formulación de políticas de la GNSO y la ICANN. Identificó ejemplos de uso indebido de registros tales como: ciberocupación, inversión ventajista (*front-running*), sitios críticos (*gripe*), nombres de dominio engañosos u ofensivos, notificaciones de renovación falsas, herramienta automática para la creación de variantes de nombres de dominio (*name spinning*), pago por clic, desvío de tráfico, afiliación falsa, estafa de registración en distintos TLD, práctica de registración repetitiva de dominios (*domain kiting/tasting*). Este RAPWG también identificó formas de uso indebido: phishing, span, malware/comando y control de botnet, DDoS y Fast Flux.

[59] ICANN, "Acuerdo Base de Registro, actualizado el 31 de julio de 2017", Especificación 11 (3)(a) y Especificación 11 (3) (b), https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf e ICANN, "Asesoramiento, Especificación 11 (3)(b) del Acuerdo de Registro de Nuevos gTLD," 8 de junio de 2017, https://www.icann.org/resources/pages/advisory-registry-agreement-spec-11-3b-2017-06-08-en.

[60] Véase pregunta: "¿Qué tipos de amenaza a la seguridad observa el DAAR?" Preguntas frecuentes del DAAR de la organización de la ICANN, https://www.icann.org/octo-ssr/daar-faqs/#security-threats. Específicamente: phishing, malware, comando y control de botnet, y spam.

cuando sea pertinente, tomen medidas razonables para detectar, bloquear y mitigar dicha conducta".[61]

El RAPWG recomendó un proceso de la comunidad, respaldado por recursos de la ICANN, para crear mejores prácticas no vinculantes con el fin de ayudar a los registradores y registros a abordar el uso ilícito de los nombres de dominio. Diez años más tarde, la organización de la ICANN aún no ha progresado mucho sobre estas cuestiones. [62] (Véase también la recomendación 9 del SSR2: Supervisar y exigir el cumplimiento).

B. Acceso a datos

El segundo mayor desafío implica el acceso a los datos sobre los nombres de dominio que informan investigación y operaciones de seguridad. Los cuatro tipo de datos que recibieron la mayor atención son datos de registración, los cuales facilitan el rastreo de actividad de uso indebido al titular y operador del dominio asociado, datos de archivos de zona de TLD (mediante el Servicio de Datos de Zona Centralizado (CZDS)), los cuales respaldan la investigación de seguridad, datos de uso indebido denunciado que se usan para informar el análisis del uso indebido del DNS por parte de la ICANN, y datos de cumplimiento contractual para respaldar el análisis de tendencias y la evaluación de enfoques operativos para mitigar el uso indebido.

i. Datos de registración

Desde al menos el año 2003, la organización de la ICANN reconoce la necesidad de equilibrar la necesidad de transparencia y responsabilidad de los metadatos de registración de nombre de dominio, es decir, información de contacto para los titulares de nombres, y requisitos legales de todo el mundo que a veces prohíben o complican el intercambio de dicha información.[63] El RAPWG consideró que la accesibilidad básica del Servicio de Directorio de Registración (RDS, formalmente conocido como WHOIS) tiene una relación inherente con el uso indebido de los procesos de registración de dominios y es una cuestión clave relacionada con el uso malicioso de los nombres de dominios.[64] Asimismo, consideró que los datos de RDS no siembre son accesibles de manera garantizada o exigible, no siempre son proporcionados por los registradores de modo confiable, coherente o predecible, y que los usuarios a veces reciben diferentes resultados de RDS según dónde o cómo realicen la búsqueda. Esto impulsó dos recomendaciones del RAPWG:

"La GNSO debería solicitar que el Departamento de Cumplimiento de la ICANN publicara más datos sobre la accesibilidad al WHOIS, al menos anualmente. Estos datos deberían incluir: a) la cantidad de registradores que muestran un patrón de restricción de acceso no razonable al

[61] Informe Final del RAPWG, 6, https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf.
[62] Carta de Claudia Selli, Presiente, Unidad Constitutiva de Negocios de la ICANN, a Maarten Botterman, Presidente, Miembros de la Junta Directiva, Corporación para la Asignación de Nombres y Números en Internet(ICANN), 9 de diciembre 2019, 1 y 3, https://www.icann.org/en/system/files/correspondence/selli-to-botterman-09dec19-en.pdf.
[63] ICANN, "Procedimiento revisado de la ICANN para el manejo de conflictos de WHOIS con las leyes de privacidad ", 18 de abril de 2017, https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-law.
[64] Informe Final del RAPWG, 71-80, https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf.

puerto 43 de los servidores del WHOIS, y b) los resultados de una auditoría anual del cumplimiento de todas las obligaciones contractuales de acceso al WHOIS".

Y

"*La GNSO debería determinar qué procesos e investigación adicionales pueden ser necesarios para asegurar que los datos del WHOIS sean accesibles de manera confiable, exigible y coherente*".[65]

En junio de 2018, en respuesta a las nuevas dificultades relacionadas con el GDPR para tener acceso a los datos de registración, el Comité Asesor de Seguridad y Estabilidad (SSAC) recomendó de manera urgente que la Junta Directiva de la ICANN trabajase para enmendar los contratos a fin de resolver los problemas persistentes relacionados con el acceso a los datos. Aún no se ha implementado ninguna de estas recomendaciones.[66] Según el informe de estado de la organización de la ICANN al Equipo de Revisión SSR2 (del 2 de julio de 2020), la organización de la ICANN delegó estas recomendaciones SSAC101 a la GNSO para su plan de trabajo de la fase 2 del EPDP sobre el acceso a los datos de registración.[67] Ninguna de estas recomendaciones formó parte del plan de trabajo de la fase 2 del EPDP, los temas no se analizaron en el EPDP y la GNSO no realizó ningún trabajo relacionado. El SSAC también realizó otros intentos, sin ningún impacto observable.[68] Algunos investigadores de seguridad han señalado que la Especificación Temporaria para los Datos de Registración de los gTLD ahora permite que los registradores de dominios de gTLD omitan todos los datos de contacto del dominio de la publicación en RDS, incluso aquellos registros no incluidos en una ley de privacidad como el GDPR.[69]

Este último EPDP es la versión más reciente y ampliada del debate sobre el acceso a los datos de registración.[70] Las declaraciones minoritarias consideraron uniformemente que las

[65] Ibídem, 79-80.

[66] Comité Asesor de Seguridad y Estabilidad de la ICANN, "SAC101: Documento de Asesoramiento del SSAC sobre el Acceso a los Datos de Registración de Nombres de Dominio", documento de asesoramiento del comité, 14 de junio de 2018, https://www.icann.org/en/system/files/files/sac-101-en.pdf. Nota: el SSAC publicó una "versión 2" del documento, la cual debilitó sustancialmente las recomendaciones de la versión 1 para que la Junta Directiva de la ICANN trabajase para enmendar los contratos con el fin de resolver los problemas persistentes con el acceso a los datos. https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf. Véase páginas 4 y 5 para consultar el texto completo de las recomendaciones contenidas en SSAC101v2.

[67] Lista de correo electrónico de Jennifer Bryce al Equipo de Revisión SSR2, 2 de julio de 2020, Asunto: estado de SAC097 y SAC102v2, https://mm.icann.org/pipermail/ssr2-review/2020-July/002280.html. Véase página 2 del adjunto del mensaje.

[68] Carta del Comité Asesor de Seguridad y Estabilidad de la ICANN a Russ Weinstein, Director, Servicios de Registro y Participación, y Jamie Hedlund, Vicepresidente Sénior, Cumplimiento Contractual y Protección al Consumidor, "Asunto: SSAC2019-02: Informes de consultas de servicios de datos de registración", 3 de mayo de 2019, https://www.icann.org/en/system/files/files/ssac2019-02-03may19-en.pdf. Nota: el SSAC publicó el documento SSAC 2019-2, en el que asesoraba que la organización de la ICANN emitiese pautas para todos los operadores de registro, que aclarase las metas, expectativas y obligaciones contractuales para informar las consultas al puerto 42 y las consultas al RDAP. No hay ninguna evidencia de que esto se haya llevado a cabo.

[69] Aaron, Greg, Lyman Chapin, David Piscitello y Dr. Colin Strutt, "Panorama del phishing 2020: estudio del alcance y la distribución de phishing", Interisle Consulting Group, LLC, 13 de octubre de 2020, http://www.interisle.net/PhishingLandscape2020.pdf.

[70] Organización de Apoyo para Nombres Genéricos de la ICANN, "Informe Final del Proceso Expeditivo de Desarrollo de Políticas de la fase 2 de la Especificación Temporaria para los Datos de Registración de los gTLD", 31

recomendaciones del informe no equilibraban adecuadamente los derechos de aquellos que brindaban los datos a los registros y registradores con el interés público con el fin de impedir perjuicios asociados a actividades maliciosas mediante la utilización del DNS.[71] El disenso sustancial del informe final implica que este proceso no ha podido lograr el consenso de la comunidad sobre la política relacionada con el acceso a los datos. Teniendo en cuenta que el "*sistema de divulgaciones actualmente fragmentado*" con una marco legal relativamente incierto es parte del problema, el Director Ejecutivo de la ICANN solicitó recientemente a la Comisión Europea que brinde claridad legal sobre las disposiciones de contraloría del GDPR.[72]

El RAA de 2013 incluyó un requisito de Validación Cruzada de Campos de Direcciones para los datos de direcciones de registración de dominios.[73] La Validación Cruzada de Campos de Direcciones es una comprobación de validez automatizada común (por ejemplo, si el número del domicilio existe en la calle, que existe en la ciudad y provincia, y si el código postal es correcto). A la fecha de este informe, la organización de la ICANN no ha aplicado este requisito de validación. Con respecto a las registraciones de servicios de representación (proxy), el Consejo de la GNSO de la organización de la ICANN respaldó, en forma unánime, una política de acreditación para los proveedores de privacidad/representación (proxy), la cual podría incluir mejoras a las prácticas operativas que impliquen respuestas a los organismos de aplicación de la ley y los titulares de propiedad intelectual.[74] La Junta Directiva de la ICANN aprobó la política en agosto de 2016.[75] A octubre de 2020, la ICANN no ha implementado estos requisitos y el sitio web dedicado a este tema de trabajo no se actualiza desde marzo de 2018.[76]

ii. Sistema de Datos de Zona Centralizado

El acceso a los archivos de zona siempre ha sido un aspecto importante de la investigación y la operaciones relacionadas con la seguridad. Como parte del programa de gTLD, la comunidad acordó que los registros de nuevos gTLD aceptasen obligaciones contractuales para "*brindar*

---

de julio de 2020, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf.

[71] Ibídem, Anexo F - declaración minoritaria, páginas 151-154. Incluye declaraciones minoritarias de: Comité Asesor At-Large (ALAC), Unidad Constitutiva de Negocios (BC) / Unidad Constitutiva de Propiedad Intelectual (IPC), Comité Asesor Gubernamental (GAC), Grupos de Partes Interesadas No Comerciales (NCSG), Grupo de Partes Interesadas de Registradores (RrSG), Grupo de Partes Interesadas de Registros (RySG), Comité Asesor de Seguridad y Estabilidad (SSAC).

[72] Carta de Göran Marby, Presidente y Director Ejecutivo de la Corporación para la Asignación de Nombres y Números en Internet (ICANN), a Roberto Viola, Director General, Dirección General de Redes de Comunicación, Comisión Europea de Contenido y Tecnología, Monique Pariat, Directora General, Dirección General de la Comisión Europea de Migración y Asuntos Internos, y Salla Saastamoinen, Directora General actuante, Dirección General de la Comisión Europea de Justicia y Consumidores, 2 de octubre de 2020, https://www.icann.org/en/system/files/correspondence/marby-to-viola-et-al-02oct20-en.pdf.

[73] ICANN, "Acuerdo de Acreditación de Registradores de 2013", consultado el 8 de diciembre de 2020, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en. Nota: véase la sección 1(e) de la Especificación del Programa de Inexactitud de WHOIS, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy.

[74] ICANN, "Servicios de privacidad y representación (proxy)", consultado el 8 de diciembre de 2020, https://whois.icann.org/en/privacy-and-proxy-services. Nota: véase la sección 2, "Proceso de adopción de recomendaciones de políticas".

[75] Ibídem.

[76] Grupo de Trabajo de Validación de WHOIS del Registrador, "documentos", actualizado por última vez el 21 de marzo de 2018, https://community.icann.org/display/AFAV/Documents.

datos de zona a solicitantes aprobados (por ejemplo, organismos de aplicación de la ley, asesores de IP, investigadores) al realizar la delegación técnica de sus gTLD".[77] Sin embargo, el acceso integral y utilizable a estos datos ha resultado problemático, por ejemplo, cuando se trata de solicitar y renovar el acceso, y obtener los archivos reales.[78] Al momento, los registros no otorgan acceso de la forma prevista y revocan el acceso periódicamente con largos procesos de renovación.[79] Estos datos se utilizan comúnmente para estudiar el uso indebido en el DNS.[80] El SSAC redactó un documento de asesoramiento sobre este tema en junio de 2017 (SAC097), hace más de tres años.[81] La Junta Directiva de la ICANN aceptó las recomendaciones, pero aún no las ha implementado.[82] El Equipo de Revisión SSR2 reconoce que ciertos TLD (como los TLD de marca) pueden requerir ajustes en lo que respecta al Sistema de Datos de Zona Centralizado (CZDS) debido a la protección de marca o preocupaciones por la seguridad, pero, en general, el acceso a datos críticos mediante CZDS sigue siendo problemático.[83]

Después de la resolución de la Junta de junio de 2018, el número de reclamos de acceso a archivos de zona aumentó y los reclamos siguen siendo más altos de lo que eran a mediados de 2018. Ahora constituyen la categoría más grande de reclamos sobre operadores de registro.[84] En algunas ocasiones, Cumplimiento Contractual de la ICANN no ha procesado los

[77] ICANN, "Sistema de Datos de Zona Centralizado (CZDS)", consultado el 7 de diciembre de 2020, https://czds.icann.org/home.

[78] Piscitello, Dave, "El lenguaje poco específico del contrato de CZDS hace que las aprobaciones de acceso a datos de zona estén libradas al azar", blog, The Security Skeptic, 13 de agosto de 2019, https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html.

[79] Piscitello, Dave, "El lenguaje poco específico del contrato de CZDS hace que las aprobaciones de acceso a datos de zona estén libradas al azar", blog en The Security Skeptic, 14 de agosto de 2019, https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html, and ICANN SSAC, "SAC 096: Documento de asesoramiento del SSAC respecto del Sistema de Datos de Zona Centralizado (CZDS) e informes mensuales de actividad de los operadores de registro", 16 de junio de 2017, https://www.icann.org/resources/files/1207653-2017-06-16-en.

[80] Claffy, KC y David Clark, "Informe del Taller sobre Economía de Internet (WIE 2019)", abril de 2020, https://ccronline.sigcomm.org/2020/ccr-april-2020/workshop-on-internet-economics-wie-2019-report%EF%BB%BF/.

[81] Comité Asesor de Seguridad y Estabilidad de la ICANN, "SAC097: Documento de asesoramiento del SSAC respecto del Sistema de Datos de Zona Centralizado (CZDS) e informes mensuales de actividad de los operadores de registro", 12 de junio de 2017, https://www.icann.org/en/system/files/files/sac-097-en.pdf.

[82] Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN, "Estado de asesoramiento del Comité Asesor de Seguridad y Estabilidad (SSAC)", actualizado por última vez el 31 de octubre de 2020, https://features.icann.org/board-advice/ssac. Véase "SAC097: Documento de asesoramiento del SSAC respecto del Sistema de Datos de Zona Centralizado (CZDS) e informes mensuales de actividad de los operadores de registro, R-1 (12 de junio de 2017)".

[83] Partridge, Mark VB y Jordan A. Arnot. "Expansión del sistema de nombres de dominio: ventajas, objeciones y solicitudes controvertidas". DePaul J. Art Tech. & Intell. Prop. L 22 (2011): 317 (véase la página 5 del artículo) y "plataforma de prueba de la API de CZDS -- Lista de correo electrónico para los usuarios de la API del CZDS para inscribirse y participar en temas de discusión de la API" https://mm.icann.org/mailman/listinfo/czds-api-testbed. Véase las cadenas de reclamos en el archivo (tenga en cuenta que el acceso está restringido a los suscriptores, pero la suscripción es abierta).

[84] ICANN, "Medición del desempeño de Cumplimiento Contractual", consultado el 7 de diciembre de 2020, https://features.icann.org/compliance/dashboard/report-list. Tenga en cuenta que los reclamos sobre acceso a archivos de zona representaron el 85,5 % de los reclamos a marzo de 2020, frente al 31,9 % en marzo de 2018.

reclamos por acceso a archivos de zona durante meses con posterioridad a la presentación de dichos reclamos.[85] En 2018, la organización de la ICANN solicitó al Grupo de Trabajo de la GNSO para el Proceso de Desarrollo de Políticas (PDP) sobre Procedimientos Posteriores a la Introducción de los Nuevos gTLD (comúnmente denominado SubPro WG) que abordase este problema.[86] El SubPro WG no incluyó ninguna mención al respecto en su reciente informe preliminar de 363 páginas.[87] No existe evidencia alguna de que la organización de la ICANN, la Junta Directiva de la ICANN o la comunidad de registros haya tomado las medidas suficientes para resolver las cuestiones relativas al acceso al CZDS. La recomendación 11 del SSR2, Resolver los problemas de acceso a los datos del CZDS, se centra en este problema.

iii. Informe de actividades de uso indebido del DNS

El proyecto Informe de Actividades de Uso Indebido de Dominios (DAAR) es una "*plataforma para estudiar la registración de nombres de dominio y el comportamiento (de uso indebido) de las amenazas a la seguridad en todos los registros y registradores de dominios de alto nivel (TLD)*" con un fin predominante "*para informar actividades de amenazas a la seguridad a la comunidad de la ICANN, la cual puede usar los datos para tomar decisiones informadas*".[88] La organización de la ICANN comenzó su programa DAAR en el año 2017. La organización de la ICANN afirmó que el DAAR tenía el fin de brindar a la comunidad un enfoque científico reproducible y transparente para informar el uso indebido del DNS.[89] Desde enero de 2018, la Oficina del Director de Tecnologías (OCTO) de la ICANN publica un informe mensual de alto nivel en función del análisis de los datos de DAAR, pero, a una granularidad que no permite conclusiones sobre qué registradores/registros albergan un uso indebido significativo. La organización de la ICANN no comparte los datos (sin procesar) completos con investigadores que podrían ayudar a mejorar la metodología o confirmar las conclusiones. El personal de la OCTO le comentó al Equipo de Revisión SSR2 que estos objetivos (datos procesables, validación) no eran objetivos de diseño del DAAR.[90] El Equipo de Revisión SSR2 considera que la forma en que la organización de la ICANN está supuestamente estructurando acuerdos con proveedores de datos es un importante inhibidor de estos objetivos y propone una revisión de su programa de análisis de uso indebido del DNS con transparencia, reproducibilidad y productos de datos procesables como sus objetivos principales.

La identificación de los registros y registradores que albergan niveles desproporcionados de uso indebido facilitaría la formulación de políticas informadas y agregaría una medida de

[85] "Plataforma de prueba de la API de CZDS -- Lista de correo electrónico para los usuarios de la API del CZDS para inscribirse y participar en temas de discusión de la API", https://mm.icann.org/mailman/listinfo/czds-api-testbed. Véase las cadenas de reclamos en el archivo (tenga en cuenta que el acceso está restringido a los suscriptores, pero la suscripción es abierta).

[86] ICANN, "Carta orgánica del Grupo de Trabajo de la GNSO para el Proceso de Desarrollo de Políticas (PDP) sobre Procedimientos Posteriores a la Introducción de los Nuevos gTLD", 21 de enero de 2016, https://gnso.icann.org/sites/default/files/filefield_48475/subsequent-procedures-charter-21jan16-en.pdf.

[87] Grupo de Trabajo de la GNSO para el Proceso de Desarrollo de Políticas (PDP) sobre Procedimientos Posteriores a la Introducción de los Nuevos gTLD de la ICANN, "Informe final preliminar de Procedimientos Posteriores a la Introducción de los Nuevos gTLD de la GNSO", consultado el 7 de diciembre de 2020, https://www.icann.org/public-comments/gnso-new-gtld-subsequent-draft-final-report-2020-08-20-en.

[88] Preguntas frecuentes de DAAR, https://www.icann.org/octo-ssr/daar-faqs/#security-threats.

[89] Piscitello, Dave, "El Sistema de Informe de Actividades de Uso Indebido de Dominios (DAAR)", informe de APWG EU, octubre de 2017, https://www.icann.org/en/system/files/files/presentation-daar-31oct17-en.pdf.

[90] Transcripción de llamada, "Llamada del SSR2 sobre el DAAR - 24 de junio de 2020 a las 15:00 UTC", https://community.icann.org/x/WIJIC.

transparencia y responsabilidad al sistema de registración de nombres de dominio que no existe hoy en día. De hecho, el Equipo de Revisión no está seguro del propósito del uso de la inversión de la ICANN en esta área si los datos y análisis no son procesables ni compartidos con el fin de reproducibilidad y validación. El Equipo de Revisión SSR2 considera que sería adecuado discontinuar el programa DAAR si la comunidad y la organización de la ICANN no pudieran revisar el DAAR a fin de lograr estos objetivos. La recomendación 12 del SSR2: Revisar el análisis del uso indebido del DNS y las iniciativas de presentación de informes para permitir la transparencia y la revisión independiente se centra en este problema.

iv. Reclamos

El informe de CCT señaló la dificultad de evaluar el impacto de las medidas de protección debido a la falta de transparencia del Departamento de Cumplimiento Contractual de la ICANN respecto de los reclamos y la falta de cumplimiento efectivo de los compromisos en pos del interés público de los contratos.[91] El Equipo de Revisión SSR2 consideró que una cuestión clave para los informantes de dominios maliciosos es la naturaleza complicada de la presentación de reclamos, requisitos divergentes entre las partes contratadas y, con frecuencia, una falta de acción o respuesta (oportuna). El Equipo de Revisión SSR2 considera que un sistema centralizado para presentar reclamos por uso indebido simplificaría el proceso de reclamos por uso indebido para quienes presenten reclamos, así como para las partes contratadas, y reduciría la cantidad de reclamos erróneamente dirigidos.

El Equipo de Revisión SSR2 considera que un programa de análisis de uso indebido del DNS revisado permitiría que Cumplimiento Contractual de la ICANN establezca expectativas estándar respecto de la prevalencia del uso indebido. Dado que las listas de bloqueo pueden no ser 100 % exactas y puede ser manipuladas, la ICANN deberá esforzarse por validar los resultados de los análisis y las partes contratadas deben tener la oportunidad de refutar la notificación de la ICANN.

Recomendación 10 del SSR2: Aclarar las definiciones de los términos relacionados con el uso indebido

10.1. La organización de la ICANN debería publicar una página web que incluya su definición de trabajo sobre el uso indebido del DNS, es decir, lo que utiliza para proyectos, documentos y contratos. La definición debería señalar explícitamente qué tipos de amenazas a la seguridad considera actualmente la organización de la ICANN dentro de su ámbito de competencia para hacer frente a través de mecanismos contractuales y de cumplimiento, así como los que la organización de la ICANN entiende que están fuera de su ámbito de competencia. Si la organización de la ICANN utiliza otra terminología similar, por ejemplo, amenaza a la seguridad, conducta maliciosa, la organización de la ICANN debería incluir tanto su definición de trabajo de esos términos como la forma precisa en que la organización de la ICANN los distingue del uso indebido del DNS. Esta página debería incluir enlaces a fragmentos de todas las obligaciones actuales relacionadas con el uso indebido en los contratos con las partes contratadas, incluidos los procedimientos y protocolos para responder ante el uso indebido. La organización de la ICANN debería actualizar esta página anualmente, fechar la última versión y enlazar con versiones anteriores con fechas de publicación asociadas.

[91] Informe de CCT, 9-10, https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

10.2. Establecer un grupo de trabajo intercomunitario (CCWG), apoyado por el personal, para establecer un proceso de evolución de las definiciones de uso indebido del DNS prohibido, al menos una vez cada dos años, en un calendario previsible (por ejemplo, cada dos años en enero), que no tardará más de 30 días hábiles en completarse. En este grupo, deberían participar las partes interesadas relacionadas con la protección del consumidor, la ciberseguridad operacional, la investigación académica o independiente sobre ciberseguridad, los organismos encargados de exigir el cumplimiento de la ley y el comercio electrónico.

10.3. Tanto la Junta Directiva de la ICANN como la organización de la ICANN deberían utilizar las definiciones consensuadas de forma coherente en los documentos públicos, contratos, planes de implementación de equipos de revisión y otras actividades, y que dichos usos hagan referencia a esta página web.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN publique la página web que incluya el primer resultado del CCWG, así como el proceso para mantener actualizada dicha página.

Esta recomendación podrá considerarse efectiva cuando la organización de la ICANN pueda ofrecer mayor transparencia y responsabilidad con respecto a descripciones aceptadas y comprobadas por la comunidad, y claridad para los debates de la comunidad e interpretación de documentos de políticas, lo que permitiría que otras partes interesadas definan códigos de conducta en torno al uso indebido del DNS.

Recomendación 11 del SSR2: Resolver los problemas de acceso a los datos del CZDS

11.1. La comunidad de la ICANN y la organización de la ICANN deberían tomar medidas para garantizar que el acceso a los datos del CZDS esté disponible, de manera oportuna y sin obstáculos innecesarios para los solicitantes, por ejemplo, falta de renovación automática de las credenciales de acceso.

Esta recomendación podrá considerarse implementada cuando la comunidad y la organización de la ICANN pongan a disposición el acceso a los datos del CZDS de manera oportuna y sin obstáculos innecesarios para los solicitantes.

La recomendación podrá considerarse efectiva cuando la organización de la ICANN informe una disminución de la cantidad de reclamos por acceso a archivos de zona y mejore la capacidad de los investigadores de estudiar las operaciones del DNS relacionadas con la seguridad.

Esta recomendación pretende establecer el acceso adecuado a los datos de archivos de zona relevantes a la seguridad usados por el sector académico y por especialistas en seguridad. Esta recomendación requiere acción de la Junta Directiva de la ICANN, la organización de la ICANN y la GNSO.

Recomendación 12 del SSR2: Revisar el análisis del uso indebido del DNS y las iniciativas de presentación de informes para permitir la transparencia y la revisión independiente

12.1. La organización de la ICANN debería crear un equipo asesor de análisis de uso indebido del DNS compuesto por expertos independientes (es decir, expertos sin conflictos de intereses financieros) para recomendar una revisión de la actividad de notificación de uso indebido del DNS con datos procesables, validación, transparencia y reproducibilidad independiente de los análisis como sus máximas prioridades.

12.2. La organización de la ICANN debería estructurar sus acuerdos con los proveedores de datos para permitir un mayor intercambio de datos para uso no comercial, específicamente para la validación o la investigación científica con revisión de pares. Esta licencia especial de uso de datos sin costo y sin fines comerciales puede conllevar un retraso para no interferir con las oportunidades de ingresos comerciales del proveedor de los datos. La organización de la ICANN debería publicar todos los términos del contrato de intercambio de datos en el sitio web de la ICANN. La organización de la ICANN debería rescindir todo contrato que no permita la verificación independiente de la metodología detrás de las listas de bloqueo.

12.3. La organización de la ICANN debería publicar informes que identifiquen los registros y registradores cuyos dominios más contribuyan al uso indebido. La organización de la ICANN debería incluir formatos legibles por computadoras de los datos, además de los datos gráficos de los informes actuales.

12.4. La organización de la ICANN debería cotejar y publicar informes de las medidas que los registros y registradores han adoptado, tanto de forma voluntaria como en respuesta a obligaciones legales, para responder a los reclamos de conductas ilícitas o maliciosas en base a las leyes aplicables en relación con el uso del DNS.

Esta recomendación podrá considerarse implementada cuando los esfuerzos de análisis de uso indebido del DNS de la organización de la ICANN incorporen mediciones que elaboren datos procesables, exactos y confiables.

Esta recomendación podrá considerarse efectiva cuando todos los datos disponibles a la organización de la ICANN también estén disponibles a la comunidad y los investigadores independientes, quizá con alguna demora de tiempo, para brindar validación y comentarios.

Recomendación 13 del SSR2: Aumentar la transparencia y la responsabilidad en la presentación de reclamos por uso indebido

13.1. La organización de la ICANN debería establecer y mantener un portal central de reclamos por uso indebido del DNS que dirija automáticamente todas las denuncias de uso indebido a las partes pertinentes. El sistema actuaría meramente como un flujo de entrada, en el cual la organización de la ICANN recopilaría y procesaría solo el resumen y los metadatos, incluidas las marcas de tiempo y los tipos de reclamos (categóricos). El uso del sistema debería ser obligatorio para todos los gTLD; la participación de cada ccTLD sería voluntaria. Además, la organización de la ICANN debería compartir los informes de uso indebido (por ejemplo, por correo electrónico) con todos los ccTLD.

13.2. La organización de la ICANN debería publicar la cantidad de reclamos presentados en un formulario que permita a terceros independientes analizar los tipos de reclamos en el DNS.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN simplifique el proceso para la presentación y recepción de reclamos por uso indebido, y ofrezca una perspectiva del número de reclamos y algunos metadatos (por ejemplo, tipo de uso indebido informado, fechas, plazo para su resolución) a los investigadores y miembros de la comunidad. Esta recomendación podrá ser considerada finalizada cuando el portal esté en funcionamiento.

Esta recomendación podrá considerarse efectiva cuando las partes contratadas deban dedicar menos tiempo a los reclamos erróneamente dirigidos y la comunidad de investigación, así como la comunidad de la ICANN en general, pueda observar y estudiar los datos asociados sobre dichos reclamos.

Debido a la complejidad de esta empresa, se espera que esta recomendación demore varios años (al menos tres) después de que la Junta Directiva de la ICANN apruebe su implementación.

3. Alternativas al Proceso de Desarrollo de Políticas (PDP)

Resulta importante abordar los reclamos de que una política de consenso desarrollada por un Proceso de Desarrollo de Políticas (PDP) es el único camino para implementar varias de nuestras recomendaciones. Hay muchas maneras en las que la Junta Directiva de la ICANN puede avanzar hacia la implementación de nuestras recomendaciones. La Junta puede optar por negociaciones contractuales, cursar notificaciones a las partes contratadas o usar un grupo de trabajo intercomunitario respaldado por expertos y por tiempo definido.[92] La organización de la ICANN podría incluso emitir una Especificación Temporaria basándose en una convicción de la Junta de que el uso indebido del DNS es una preocupación grave sobre la seguridad pública que necesita ser atendida con urgencia. El uso reciente de la Junta de la Especificación Temporaria en respuesta a las inconsistencias entre el GDPR de la Unión Europea y los Estatutos de la organización de la ICANN es un estudio de caso útil. La comunidad de la ICANN tuvo años para desarrollar una política de acceso a datos de registración que estuviera en consonancia con el GDPR, pero efectivamente pospuso el problema. Observamos un patrón similar con respecto al uso indebido del DNS y el acceso a los datos de registración para combatir el uso indebido.

La organización de la ICANN puede y, de hecho, realiza negociaciones contractuales bilaterales. Se han realizado cambios a los contratos entre registrador y registro de la organización de la ICANN sin una política de consenso creada por un PDP. Cuando la organización de la ICANN actualizó el RAA de 2013 al Acuerdo Base de Registro de 2017, la organización de la ICANN y el equipo de negociación que representaba a la industria respectiva administraron el proceso, sin ningún PDP. La comunidad tuvo la oportunidad de realizar comentarios sobre el texto preliminar, pero solo el equipo de negociación participó en las

[92] Ejemplos anteriores de notificaciones a partes contratadas están disponibles en el sitio web Notificación a los registradores (https://whois.icann.org/en/registrar-advisories).

discusiones y las decisiones.[93] Estas negociaciones a puertas cerradas entre la organización de la ICANN y las partes contratadas son un valioso método para progresar, pero son limitadas cuando se trata del uso indebido del DNS porque excluyen a todas las demás partes interesadas, incluidos gobiernos, empresas y el público que tienen un interés en reducir las registraciones abusivas. La recomendación 12 del SSR2: Revisar el análisis del uso indebido del DNS y las iniciativas de presentación de informes para permitir la transparencia y la revisión independiente aborda esta brecha.

En especial, a raíz de que el EPDP no puede resolver el acceso a los datos de registración, los inmensos conflictos de interés que ralentizan el proceso de PDP y el lento avance en el abordaje del proceso contra el uso indebido del DNS, el Equipo de Revisión considera que un proceso de EPDP dedicado al uso indebido no aportará una solución eficaz por sí solo. El EPDP sobre el acceso a los datos de registración demoró años en completarse y el producto final recibió disenso de una mayoría de la comunidad de la ICANN; hubo declaraciones minoritarias importantes del Comité Asesor At-Large (ALAC), la Unidad Constitutiva de Negocios y la Unidad Constitutiva de Propiedad Intelectual (BC/IPC), el Grupo de Partes Interesadas No Comerciales (NCSG), el Grupo de Partes Interesadas de Registradores (RrSG) y el Grupo de Partes Interesadas de Registros (RySG). El informe minoritario de BC/IPC advirtió: "*Los entes reguladores y legisladores deberían notar que el modelo de múltiples partes interesadas de la ICANN no pudo satisfacer las necesidades de protección de los consumidores, ciberseguridad y aplicación de la ley*".[94] El informe minoritario del SSAC también advirtió que el proceso de desarrollo de políticas de la ICANN no "*ha arrojado resultados que sean razonablemente adecuados para la seguridad y la estabilidad*".[95]

En resumen, las acciones para mitigar, prevenir y detener el uso indebido del DNS existente se ven desafiadas por la ambigüedad de los requisitos contractuales y terminología existentes, los conflictos de interés entre todas las partes que deberían actuar y diversos compromisos de gobiernos de todo el mundo para también abordar el uso indebido del DNS mediante otros procesos legales. Ya existen algunas obligaciones contractuales y políticas relacionadas con el uso indebido del DNS, pero la organización de la ICANN y las partes contratadas necesitan implementarlas y aplicarlas de manera más eficaz, y la comunidad debe desarrollar políticas, obligaciones contractuales y actividades adicionales para ir a la par con el uso indebido del DNS. El Equipo de Revisión SSR2 considera que el uso indebido del DNS es una necesidad crítica que garantiza y justifica el fuerte liderazgo de la ICANN en esta área. La Especificación Temporaria del GDPR demostró que la Junta Directiva de la ICANN mantiene la autoridad de formulación de políticas en respuesta a varias necesidades. Asimismo, la Junta tiene deberes fiduciarios para garantizar que las políticas de la organización de la ICANN y los contratos derivados se ajusten al propósito de la organización de la ICANN como una corporación de beneficio público sin ánimo de lucro a cargo de la supervisión de la seguridad, estabilidad y formulación de políticas relacionadas con el DNS en pos del interés público. Una nueva

[93] Acuerdo de Acreditación de Registradores de 2013, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en. Nota: la CANN puede enmendar contratos ya sea mediante una política de consenso o mediante una negociación entre la organización de la ICANN y las otras partes relevantes al contrato en virtud del RAA, sección 1.2, Políticas de consenso y Especificación de políticas temporarias, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary.

[94] Informe de la fase 2 del EPDP de la GNSO, declaración minoritaria de BC/IPC, 114-121, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf.

[95] Ibídem, 145-162, declaración minoritaria del SSAC.

Especificación Temporaria combinada con un nuevo EPDP puede llegar a ser el mejor enfoque.[96]

Recomendación 14 del SSR2: Crear una especificación temporaria para las mejoras de seguridad basadas en pruebas

14.1. La organización de la ICANN debería crear una especificación temporaria que exija a todas las partes contratadas mantener el porcentaje de dominios identificados por la actividad revisada de Informes de uso indebido del DNS (véase la recomendación 13.1 del SSR2) como abusivos por debajo de un umbral razonable y publicado.

14.2. Para permitir la adopción de medidas contra el uso indebido, la organización de la ICANN debería proporcionar a las partes contratadas listas de dominios de sus carteras identificados como abusivos, de conformidad con la recomendación 12.2 del SSR2 relativa a la revisión independiente de los datos y métodos para el bloqueo de dominios.

14.3. En caso de que la cantidad de dominios vinculados a actividades de uso indebido alcance el umbral publicado descripto en la recomendación 14.1 del SSR2, la organización de la ICANN debería investigar para confirmar la veracidad de los datos y el análisis, y luego emitir una notificación a la parte pertinente.

14.4. La organización de la ICANN debería conceder a las partes contratadas 30 días para reducir la fracción de dominios con uso indebido por debajo del umbral o para demostrar que las conclusiones o los datos de la organización de la ICANN son erróneos. Si una parte contratada no rectifica durante 60 días, el departamento de Cumplimiento Contractual de la ICANN debería pasar al proceso de desacreditación.

14.5. La organización de la ICANN debería considerar la posibilidad de ofrecer incentivos financieros: las partes contratadas con carteras con menos de un porcentaje específico de nombres de dominio con uso indebido deberían recibir una reducción de las tarifas sobre las transacciones cobrables hasta un umbral apropiado.

Recomendación 15 del SSR2: Iniciar un EPDP para las mejoras de seguridad basadas en pruebas

15.1. Después de crear la especificación temporaria (véase la recomendación 14 del SSR2: Crear una especificación temporaria para las mejoras de seguridad basadas en pruebas), la organización de la ICANN debería establecer un EPDP respaldado por el personal para crear una política contra el uso indebido. Los voluntarios del EPDP deberían representar a la comunidad de la ICANN, utilizando como plantilla los números y la distribución de la Especificación Temporaria para los Datos de Registración de los gTLD de la carta orgánica del equipo responsable del EPDP.[97]

15.2. El EPDP debería basarse en la definición de los fundamentos del CCWG propuesta en la recomendación 10.2 del SSR2. Este marco normativo debería definir las

[96] El Equipo de Revisión SSR2 considera que la organización de la ICANN ha compilado una colección de conocimientos suficientes, incluidos el conocimiento que dio lugar al programa DAAR y los informes del DAAR, para compilar un informe de cuestiones, y, así justificar el inicio de un EPDP en vez de un PDP.

[97] ICANN, "Carta orgánica del equipo para PDP", página editada por última vez el 23 de julio de 2018, 12-14, https://community.icann.org/display/EOTSFGRD/EPDP+Team+Charter.

contramedidas y medidas correctivas apropiadas para los diferentes tipos de uso indebido, los plazos para las acciones de las partes contratadas, como los plazos para la presentación de informes de uso indebido/informes de respuesta, y las medidas en pos del cumplimiento efectivo del departamento de Cumplimiento Contractual de la ICANN en caso de infracciones a las políticas. La organización de la ICANN debería insistir en la facultad de rescindir los contratos en caso de que exista en cualquier parte contratada un patrón y práctica de albergar usos indebidos. El resultado debería incluir un mecanismo para actualizar los puntos de referencia y las obligaciones contractuales relacionadas con el uso indebido cada dos años, mediante un proceso que no requiera más de 45 días hábiles.

Las recomendaciones 14 y 15 del SSR2 podrán considerarse implementadas cuando el Departamento de Cumplimiento Contractual de la ICANN tenga las herramientas necesarias para responder adecuadamente a las partes contratadas que no responden ante el uso indebido del DNS, en especial, la existencia de obligaciones contra el uso indebido en todos los contratos y acuerdos relevantes.

Las recomendaciones 14 y 15 del SSR2 podrán considerarse efectivas cuando el Departamento de Cumplimiento Contractual de la ICANN use dichas herramientas para lidiar con notorias infracciones de políticas de las partes contratadas.

El resultado esperado de las recomendaciones 14 y 15 del SSR2 es empoderar a Cumplimiento Contractual de la ICANN para lidiar con los peores infractores en lo que respecta al uso indebido del DNS, para lo que el equipo de Cumplimiento Contractual de la ICANN ha manifestado que no tiene las herramientas suficientes para hacerlo.

Estas recomendaciones requieren acción de la organización y de la comunidad de la ICANN, y tienen el propósito de guiar la creación de políticas. Estas recomendaciones son realizables, pero la organización de la ICANN solo puede llevarlas a cabo con el tiempo.

4. Privacidad y custodia de datos

La privacidad es una cuestión que está en constante evolución debido a la cantidad creciente de recopilación y análisis de datos por terceros (además de los tradicionales organismos gubernamentales), así como el cambiante panorama de la legislación sobre la privacidad. El Equipo de Revisión SSR2 concluye que la organización de la ICANN no ha sido tan proactiva como debería ser, dado el panorama cambiante, tal como lo demuestra sus inconsistencias en los datos disponibles en los Servicios de Directorio de Registración (RDS) o respecto de estos.[98]

Hay una proliferación de páginas web sin datos asociados en todo el sitio web de la ICANN que analizan varios aspectos de la privacidad de los datos de registración. Esta falta de marcas de tiempo no permitió que el Equipo de Revisión realizase una investigación razonable sobre la historia de la organización de la ICANN acerca de este tema.[99] A octubre de 2020, el sitio web

[98] Véase sección E.2.b.i. Datos de registración y sección E.2.b.ii. Sistema de Datos de Zona Centralizado en este informe.

[99] Entre los ejemplos se incluyen: https://whois.icann.org/en/privacy-and-proxy-services, https://whois.icann.org/en/privacy, https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-law y https://www.icann.org/rdap. Nota: todas estas páginas parecen tener muchos años y varias incluyen

del RDS y la documentación relacionada también están desactualizados, y no incluyen documentos relevantes de la comunidad ni hacen referencia a ellos. Hay unas pocas páginas web de la ICANN en el RDS, pero no hay referencia cruzada. La página web actual del RDS de la ICANN se actualizó por última vez en 2017 y, por ende, no hace referencia a las medidas actuales de la Especificación Temporaria o al estado del EPDP.[100] El Equipo de Revisión considera que la falta de información y consistencia en el sitio web refleja la propia falta de claridad y consistencia de la organización de la ICANN en cuestiones relativas a la seguridad.

En la sección E.2.b.i. Datos de registración, el Equipo de Revisión también señaló la necesidad de equilibrar la transparencia y la responsabilidad de los metadatos de registración de nombres de dominio en virtud de varias regulaciones de privacidad, como el GDPR. Al garantizar la consistencia en su propio sitio web, así como en las políticas de consenso y los acuerdos con los operadores de registro y los registradores, la organización de la ICANN ayudará a garantizar la administración y protección seguras de recopilación, retención, custodia, transferencia y visualización de los datos de registración, los cuales incluyen información de contacto del registratario, los contactos administrativos y técnicos, así como información técnica asociada a un nombre de dominio.

Recomendación 16 del SSR2: Requisitos de privacidad y RDS

16.1. La organización de la ICANN debería proporcionar referencias cruzadas coherentes en todo su sitio web para ofrecer información cohesiva y fácil de encontrar sobre todas las acciones (pasadas, presentes y planificadas) realizadas sobre el tema de la privacidad y la custodia de datos, con especial atención a la información sobre el RDS.

16.2. La organización de la ICANN debería crear grupos especializados dentro de la función de Cumplimiento Contractual que comprendan los requisitos y principios de privacidad (como la limitación de la recopilación, la calificación de los datos, la especificación de los fines y las medidas de seguridad para la divulgación) y que puedan facilitar las necesidades de aplicación de la ley en el marco del RDS a medida que ese marco sea enmendado y adoptado por la comunidad (véase también la recomendación 11 del SSR2: Resolver los problemas de acceso a los datos del CZDS).

16.3. La organización de la ICANN debería realizar auditorías periódicas de la adhesión a las políticas de privacidad implementadas por los registradores para garantizar que cuentan con procedimientos para abordar las infracciones a la privacidad.

Esta recomendación podrá considerarse implementada cuando las acciones de la organización de la ICANN respecto de la privacidad y su administración del RDS estén documentadas correctamente, y, en particular, los recursos asignados dentro de la organización de la ICANN mantengan a la organización en consonancia con las mejores prácticas y requisitos legales actuales en este ámbito.

una nota en la parte inferior: “El 17 de mayo de 2018, la Junta Directiva de la ICANN adoptó una Especificación Temporaria para los Datos de Registración de los gTLD. Esta página está en proceso de revisión y se actualizará para dar tratamiento a la Especificación Temporaria”.

[100] ICANN, “Acerca del WHOIS,” actualizado por última vez en julio de 2017, https://whois.icann.org/en/about-whois.

Esta recomendación podrá considerarse efectiva cuando la organización de la ICANN pueda demostrar el cumplimiento continuo de las mejores prácticas y los requisitos legales en el manejo y la privacidad de los datos.

F. Inquietudes adicionales relacionadas con el SSR respecto del DNS global

El Equipo de Revisión SSR2 reconoce que la organización de la ICANN es solo una de las muchas entidades del ecosistema del DNS. Dicho eso, la organización de la ICANN se encuentra entre aquellas en una posición única para influir y guiar las acciones relacionadas con la SSR en todo el ecosistema. Esta sección ofrece recomendaciones específicas para los sitios en los que la organización de la ICANN puede mejorar sus políticas y prácticas para sí misma y para todo el DNS global. Al modelar las mejores prácticas en la administración del servidor raíz gestionado por la ICANN (IMRS), intercambiar los aportes consolidados de los investigadores, ofrecer herramientas para pruebas y análisis, y otras posibles acciones analizadas en esta sección, la organización de la ICANN puede tomar medidas para mejorar sus propias acciones respecto de la SSR y ayudar a otros a comprender cómo pueden mejorar las suyas.

1. Colisión de nombres

Si bien la organización de la ICANN brinda material detallado y cursos de capacitación sobre la colisión de nombres, no hay restricción alguna para que los registratarios utilicen un identificador único para una zona privada que colisiona con una zona pública. El Equipo de Revisión SSR2 considera que el estudio recientemente concluido y publicado (de aquí en adelante, denominado estudio de NCAP 2019) es un paso en la dirección correcta para manejar las colisiones de nombres no deseadas.[101] Sin embargo, este estudio no abordó la necesidad continua de contar con mecanismos para detectar colisiones de nombres no informadas, ya sean maliciosas o accidentales. El estudio también concluyó que no hay investigación reciente sobre colisiones de nombres (desde 2017) y tomó la disminución en colisiones de nombres informadas como un indicador de que los mecanismos actuales funcionan.[102] Por otro lado, la investigación revisada por pares en 2016 concluyó que la última ronda de gTLD exacerbó considerablemente el problema de colisión de nombres.[103] Es posible que la disminución de colisiones de nombres informadas como indican los mecanismos de presentación de informes tradicionales no implique la ausencia de colisiones de nombres. En cambio, la naturaleza de las colisiones de nombres puede haber cambiado de manera tal de evadir dichos mecanismos tradicionales. Asimismo, ha habido una disminución en la

[101] Scarfone, Karen, "Gestión de riesgos de las colisiones de nombres de dominio de alto nivel: conclusiones del estudio del Proyecto de Análisis de Colisiones de Nombres (NCAP)", OCTO de la ICANN, 27 de mayo de 2020, https://www.icann.org/en/system/files/files/managing-risks-tld-2-name-collision-07may20-en.pdf.

[102] Ibídem, 43.

[103] Chen, Qi Alfred, Eric Osterweil, Matthew Thomas y Z. Morley Mao. "Ataque MitM por colisión de nombres: análisis de causas y evaluación de vulnerabilidades en la era de los nuevos gTLD". Simposio del IEEE de 2016 sobre seguridad y privacidad (SP) (mayo de 2016), 675-690. doi:10.1109/sp.2016.46.

delegación de nuevos TLD en los años recientes, lo que podría también afectar a las cantidades absolutas de colisiones de nombres informadas.[104]

Aunque se propuso un marco de interrupción controlada para evitar posibles colisiones de nombres de nombres de dominio en un informe encargado por la ICANN en el año 2014 (de aquí en adelante, denominado Informe de la fase uno), este marco de interrupción controlada nunca fue evaluado en relación con los cambiantes escenarios de ataques de colisión de nombres.[105] Por ejemplo, el SSAC aconsejó que *"En lugar de un solo período con interrupción controlada, la ICANN debería incorporar períodos de interrupción sucesivos, desglosados por períodos de funcionamiento normal, para permitir que los sistemas del usuario final afectados continúen funcionando durante el período de prueba de 120 días con menos riesgo de impacto comercial catastrófico".*[106] En el Informe de la fase uno, los autores basaron algunas de sus inferencias en la falta de correo electrónico y llamadas telefónicas de los registratarios de dominios de segundo nivel, lo que no refleja adecuadamente la complejidad del problema.[107] Asimismo, el Informe de la fase uno también analizó diversos enfoques alternativos al marco de interrupción controlada, incluso el uso de herramientas de seguridad informática honeypot, DNAME, y enfoques de cadena de caracteres a cadena de caracteres, pero nunca se consideró la implementación de estos enfoques.[108] El Equipo de Revisión SSR2 concluye, a diferencia del Informe de la fase uno, que la colisión de nombres aún es un desafío que amerita más estudio y mitigación.

Recomendación 17 del SSR2: Medición de colisiones de nombres

17.1. La organización de la ICANN debería crear un marco para caracterizar la naturaleza y la frecuencia de las colisiones de nombres, y las preocupaciones que generan. Este marco debería incluir mediciones y mecanismos para medir el grado de éxito de la interrupción controlada en la identificación y eliminación de colisiones de nombres. Esto podría apoyarse en un mecanismo que permita la divulgación protegida de los casos de colisión de nombres. Este marco debería permitir el manejo adecuado de datos sensibles y amenazas a la seguridad.

17.2. La comunidad de la ICANN debería desarrollar una política clara para evitar y manejar las nuevas colisiones de nombres en relación con los gTLD e implementar esta política antes de la próxima ronda de gTLD. La organización de la ICANN debería asegurarse de que la evaluación de esta política sea llevada a cabo por las partes que no tengan ningún interés financiero en la expansión de los gTLD.

---

[104] ICANN, sitio web de nuevos gTLD, https://newgtlds.icann.org/en/program-status/statistics. Nota: al 12 de diciembre de 2020, solo 9 gTLD continúan en proceso de los 1930 originalmente disponibles.

[105] ICANN, "Informe de la fase uno sobre mitigación del riesgo de colisiones en el espacio de nombres del DNS", 6 de julio de 2014, 6, https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf, e ICANN, "Marco de Gestión de Incidentes de Colisiones de Nombres", 30 de julio de 2014, 2-3, https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf.

[106] SSAC de la ICANN, "SAC066: Comentario del SSAC respecto del Informe de la fase uno de JAS sobre la mitigación del riesgo de colisiones en el espacio de nombres del DNS", 6 de junio de 2014, 4, https://www.icann.org/en/system/files/files/sac-066-en.pdf.

[107] Informe de la fase uno de JAS sobre la mitigación del riesgo de colisiones en el espacio de nombres del DNS, 22, https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf.

[108] Ibídem.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN elabore un marco que produzca conclusiones que caractericen la naturaleza y frecuencia de las colisiones de nombres y las inquietudes resultantes mediante la identificación de mediciones y el diseño de mecanismos que mensuren la medida en que el mecanismo de interrupción controlada es exitoso.

La recomendación podrá considerarse efectiva cuando la organización de la ICANN y la comunidad puedan detectar, actuar en consecuencia y, por último, minimizar la existencia de colisiones de nombres y responder ante los cambiantes escenarios de colisión de nombres.

Esta recomendación debe ser implementada antes de la próxima ronda de gTLD.

2. Investigación y resúmenes informativos

Ahora se está produciendo una enorme cantidad de actividad en la comunidad de investigación del sector académico relacionada con cuestiones de seguridad, estabilidad y flexibilidad en el nombre, el enrutamiento y las capas de direcciones. La comunidad de la ICANN tiene la oportunidad de aprovechar esta actividad y experiencia para informar políticas y desarrollo tecnológico que reducirán considerablemente los perjuicios relacionados con la SSR en el ecosistema. Pero no existe ninguna función que asegure que la organización de la ICANN y la comunidad a la que presta servicios se mantengan al tanto de estos avances.

Recomendación 18 del SSR2: Informar los debates de políticas

18.1. La organización de la ICANN debería hacer un seguimiento de los avances en la comunidad de investigación con revisión de pares, centrándose en las conferencias de investigación sobre redes y seguridad, que incluya, al menos, el Sistema de Clasificación Informática (CCS) de la Asociación de Maquinaria Informática (ACM), la Conferencia sobre la medición en Internet de ACM, Usenix Security, la revista CCR, el Grupo de Interés Especial sobre Comunicaciones de Datos (SIGCOMM), el Simposio sobre Seguridad y Privacidad de IEEE, así como las conferencias de seguridad operacional y el Foro de los Equipos de Respuesta a Incidentes y Seguridad (FIRST), y debería publicar un informe para la comunidad de la ICANN que resuma las implicancias de las publicaciones que son relevantes para la organización de la ICANN o el comportamiento de las partes contratadas.[109]

18.2. La organización de la ICANN debería asegurarse de que estos informes incluyan las observaciones pertinentes que puedan corresponder a las recomendaciones para la

[109] Enlaces a conferencias: CSS de ACM <https://dl.acm.org/conference/ccs>, Conferencia de Medición de Internet de ACM <https://www.sigcomm.org/events/imc-conference>, Usenix Security <https://www.usenix.org/conferences>, CCR <https://www.ccrsummit.com/>, SIGCOMM <https://www.sigcomm.org/>, Simposio del IEEE sobre seguridad y privacidad <https://www.ieee-security.org/index.html>, FIRST <https://www.first.org/>. Nota: la implementación sugerida podría ser contactar a los organizadores (presidentes de comités de programas técnicos, organizadores de grupos directivos, etc.) y solicitar compendios de los procedimientos o invitar miembros de los comités de estos sitios para presentar compendios relevantes de sus procedimientos en forma anual, en uno de los eventos de la comunidad de la ICANN. En esa implementación, la organización de la ICANN preservaría las sesiones de lectura en un informe archivado.

adopción de medidas, incluidos los cambios en los contratos con los registros y registradores, que puedan mitigar, prevenir o remediar los perjuicios en materia de SSR para los consumidores y la infraestructura identificados en la bibliografía revisada por pares.

18.3. La organización de la ICANN debería asegurarse de que estos informes también incluyan recomendaciones de estudios adicionales para confirmar las conclusiones revisadas por pares, una descripción de los datos que requeriría la comunidad para ejecutar los estudios adicionales, y cómo la organización de la ICANN puede ofrecerse para ayudar a la intermediación en el acceso a dichos datos, por ejemplo, a través del CZDS.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN cree y mantenga un archivo público de compendios o sesiones de lectura de varias conferencias sobre redes e investigación de seguridad.

Esta recomendación podrá considerarse efectiva cuando la información proveniente de la comunidad de investigación sobre cuestiones relacionadas con la seguridad, estabilidad y flexibilidad sea más accesible para las personas que formulan decisiones sobre políticas.

3. Plataforma de prueba del DNS

Dado que el ecosistema del DNS ya es grande y sigue creciendo, es fundamental mantener y supervisar una serie de pruebas de regresión y una plataforma de prueba a fin de analizar los comportamientos y las interacciones del DNS. El Equipo de Revisión SSR2 ha concluido que las actividades continuas de la plataforma de prueba del DNS a cargo de la OCTO, una vez finalizadas, abordan suficientemente esta inquietud.[110] Además, el Equipo de Revisión considera que el apoyo y mantenimiento de esta plataforma de prueba (así como el uso de sus resultados y conclusiones) es un requisito de la organización de la ICANN.

La finalización y el mantenimiento oportunos de esta plataforma de prueba permitirían que la comunidad de la ICANN probara e investigara el comportamiento de los resolutores, lo que es fundamental para garantizar la integridad y disponibilidad global del DNS.

Recomendación 19 del SSR2: Desarrollo completo de la serie de pruebas de regresión del DNS

19.1. La organización de la ICANN debería completar el desarrollo de una serie de pruebas de comportamiento de los resolutores del DNS.

19.2. La organización de la ICANN debería asegurarse de que se implemente y mantenga la capacidad de seguir realizando pruebas funcionales de diferentes configuraciones y versiones de software.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN finalice el desarrollo de una serie de pruebas de acceso público para pruebas e investigación de la comunidad respecto del comportamiento de los resolutores.

[110] "Plataforma de prueba de resolutores", repositorio GitHub de la ICANN, https://github.com/icann/resolver-testbed.

Esta recomendación podrá considerarse efectiva cuando haya una serie de pruebas disponible con un ciclo de actualización anual que ayude a garantizar la integridad y disponibilidad global del DNS.

4. Inquietudes sobre la zona raíz y los registros

A. Traspaso de clave

La clave para la firma de la llave (KSK) de las DNSSEC para la zona raíz se traspasó el 11 de octubre de 2018 por primera vez desde el establecimiento de la clave de la Zona Raíz Intencionalmente No Validable (DURZ).[111] Durante el proceso de traspaso, hubo muchos debates y llamadas para analizar los detalles del traspaso.[112] Un resultado del análisis del Equipo de Revisión SSR2 fue el entendimiento de que se necesitan tramos de excepción que funcionen correctamente para garantizar un traspaso de clave seguro y exitoso.[113] La organización de la ICANN demoró el traspaso durante un año mientras que la organización tomaba medidas para aliviar las inquietudes. Dentro de la comunidad de la ICANN ya han comenzado debates acerca del momento y el proceso para futuros traspasos, incluida la consideración de posibles complejidades nuevas, por ejemplo, los traspasos de algoritmos.[114] Posteriormente, la organización de la ICANN realizó una convocatoria abierta para la presentación de comentarios sobre el proceso del próximo traspaso planificado de la KSK.[115]

Debido al carácter crítico de las protecciones de seguridad que son (y serán) derivadas de la zona raíz firmada con las DNSSEC, es fundamental contar con análisis de procesos formalmente verificables a fin de garantizar la seguridad, estabilidad y flexibilidad del proceso por el cual se mantienen las protecciones de las DNSSEC durante los traspasos de clave KSK de la zona raíz.[116] El modelo de proceso formal emplea una metodología o un entorno de programación para especificar cada tarea del proceso, evaluar su ejecución (realizado correctamente, realizado con errores, otros, etc.) y especificar las acciones de seguimiento según los diferentes resultados. Las especificaciones de proceso como esta han demostrado ser útiles en procesos interhumanos complejos que incluyen seguridad en las elecciones,

---

[111] ICANN, "El primer traspaso de la KSK de la zona raíz se llevó a cabo con éxito", 15 de octubre de 2018, https://www.icann.org/news/announcement-2018-10-15-en.

[112] ICANN, "El reciente traspaso de la KSK: resumen y pasos a seguir", blog de la ICANN, 30 de enero de 2018, https://www.icann.org/news/blog/the-recent-ksk-rollover-summary-and-next-steps, y Moritz Müller, Matthew Thomas, Duane Wessels, Wes Hardaker, Taejoong Chung, Willem Toorop y Roland van Rijswijk-Deij, "Traspase su raíz: análisis integral del primer traspaso de la KSK de la raíz de las DNSSEC", octubre de 2019, https://dl.acm.org/doi/10.1145/3355369.3355570.

[113] Transcripción de la sesión plenaria n.° 97 del SSR2, sesión matutina, 17 de enero de 2020, 35, https://community.icann.org/x/HJkzBw.

[114] Informe del procedimiento de comentarios públicos confeccionado por el personal: propuesta para futuros traspasos de la KSK de la zona raíz, 7 de agosto de 2020, https://www.icann.org/en/system/files/files/report-comments-proposal-future-rz-ksk-rollovers-07aug20-en.pdf. Nota: presentaron comentarios los servicios de registro de Japón, la Unidad Constitutiva de Negocios de la ICANN, el Grupo de Partes Interesadas No Comerciales de la ICANN, el Comité Asesor del Sistema de Servidores Raíz de la ICANN y varias personas individuales.

[115] "propuesta para futuros traspasos de la KSK de la zona raíz", 1 de noviembre de 2019, https://www.icann.org/public-comments/proposal-future-rz-ksk-rollovers-2019-11-01-en.

[116] Osterweil, Eric. "Un terminarca de ciberseguridad: úselo antes de que lo perdamos". *Seguridad y Privacidad del IEEE* 18, n.° 4 (2020): 67-70.

seguridad médica del proceso y más.[117] En estos casos, las tareas de las personas (en el espacio humano) son complejas y modeladas en lenguajes de especificaciones de procesos formales, y elecciones vitales (vitales para la vida), y las consecuencias son simbólicamente modeladas y formalmente rastreadas. Este modelado permite prescripciones y predicciones cuantitativas de lo que debería realizarse y de lo que puede esperarse que resulte de las elecciones, las excepciones y las ejecuciones exitosas.[118] En comparación con las elecciones y los procesos médicos, el traspaso de la clave para la firma de la llave de la zona raíz del DNS se presenta como un ámbito tratable cuya seguridad e integridad son globalmente críticas.

Recomendación 20 del SSR2: Procedimientos formales para el traspaso de claves

20.1. La organización de la ICANN debería establecer un procedimiento formal, respaldado por una herramienta de modelado de procesos formales y un lenguaje para especificar los detalles de los futuros traspasos de claves, incluidos los puntos de decisión, los tramos de excepción, el flujo de control completo, etc. La verificación del proceso de traspaso de claves debería incluir la publicación del procedimiento programático (por ejemplo, programa, máquina de estado finito (FSM)) para el comentario público, y la organización de la ICANN debería incorporar los comentarios de la comunidad. El proceso debería tener criterios de aceptación empíricamente verificables en cada etapa, que deberían cumplirse para que el proceso continúe. Este proceso se debería reevaluar al menos con la misma frecuencia que el propio traspaso (es decir, con la misma periodicidad) para que la organización de la ICANN pueda utilizar las lecciones aprendidas para ajustar el proceso.

20.2. La organización de la ICANN debería crear un grupo de partes interesadas en el que participe el personal pertinente (de la organización de la ICANN o de la comunidad) para realizar periódicamente ejercicios de simulación que sigan el proceso de traspaso de la KSK de la zona raíz.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN desarrolle un proceso de verificación formal que ofrezca la verificación del proceso de traspaso de claves después de cada traspaso, y cuando la organización de la ICANN comience a realizar ejercicios de simulación periódicos para evaluar y familiarizar a los participantes con el proceso de traspaso de claves.

Esta recomendación podrá considerarse efectiva cuando la SSR del proceso para el cual se mantienen las protecciones de las DNSSEC durante los traspasos de la clave para la firma de la llave de la zona raíz se puedan verificar formalmente.

[117] Osterweil, Leon J., Matt Bishop, Heather Conboy, Huong Phan, Borislava I. Simidchieva, George Avrunin, Lori A. Clarke y Sean Peisert, “Análisis iterativo para mejorar las propiedades clave de procesos vitales con actividad humana intensa: un ejemplo de seguridad en las elecciones”, transacciones de ACM sobre privacidad y seguridad (TOPS), Vol. 20, N.° 2, mayo de 2017, pág. 5:1-31. (UM-CS-2016-012), y Clarke, Lori A., Yao Chen, George S. Avrunin, Bin Chen, Rachel Cobleigh, Kim Frederick, Elizabeth A. Henneman y Leon J. Osterweil. “Programación de proceso para respaldar la seguridad médica: un estudio de caso sobre transfusión de sangre”. Taller sobre proceso de software, pág. 347-359. Springer, Berlin, Heidelberg, 2005.

[118] Análisis iterativo para mejorar las propiedades clave de procesos vitales con actividad humana intensa: Un ejemplo de seguridad en las elecciones, Leon J. Osterweil, Matt Bishop, Heather Conboy, Huong Phan, Borislava I. Simidchieva, George Avrunin, Lori A. Clarke, Sean Peisert, transacciones de ACM sobre privacidad y seguridad (TOPS), Vol. 20, N° 2, mayo de 2017, pág. 5:1-31. (UM-CS-2016-012).

Esta recomendación debe realizarse en conjunto con cada traspaso de clave.

B. Gestión de cambio de la zona raíz

El Equipo de Revisión SSR2 observó que la entidad PTI tuvo éxito en la implementación de mecanismos que reducen la posibilidad de manipular los datos de los TLD y la zona raíz.[119] La gestión de la zona raíz sigue un sistema de flujo de trabajo para administrar las etiquetas de los TLD en la zona raíz denominado Sistema de Gestión de la Zona Raíz (RZMS), Este flujo de trabajo sigue un enfoque conservador respecto de la gestión de cambios, dado que cada cambio requiere una revisión de las diversas partes.[120]

Aunque no existen problemas conocidos respecto de la seguridad y la estabilidad que impliquen el uso indebido del RZMS, existe el potencial para ciberataques triviales durante el proceso de autenticación para todas las partes que participan en el flujo de trabajo del RZMS. La comunicación con los operadores de TLD ahora se realiza mediante el envío de correos electrónicos con texto claro y acceso al sistema mediante una simple combinación de usuario y contraseña. La autenticación de solicitudes de cambio debería ser más estricta e implicar autenticación de factor múltiple (MFA) y comunicación segura (por ejemplo, cifrado) al usar correo electrónico.

En la actualidad, el equipo de funciones de la IANA está creando su RZMS de próxima generación, que implica una reformulación sustancial del modelo de autorización.[121] El RZMS de próxima generación debería implicar un modelo de autenticación y autorización sólido y seguro para la presentación y aprobación de las solicitudes, así como funciones adicionales que mejoren la seguridad y estabilidad del sistema del DNS global, entre ellas:

- Garantizar la integridad y autenticidad de las solicitudes de cambio para los datos de los TLD.
- Imponer comunicaciones seguras en todos los niveles que impliquen la gestión de solicitudes.
- Ser resilientes a posibles actividades engañosas que impliquen servidores autoritativos del DNS para las zonas raíz y de los TLD.
- Responder con rapidez a solicitudes de eliminación (remoción de registros DS o NS).
- Consideración de procedimientos y controles técnicos automatizados adicionales (que impliquen el proceso de evaluación y aprobación pública del SSAC y del RSSAC) para la rápida subsanación de problemas que pueden afectar las operaciones uniformes de los TLD en el DNS.
- Consideración por parte del SSAC y del RSSAC de la implementación de RFC 8078 y actualizaciones relacionadas para el mantenimiento automatizado de confianza de delegación de DNSSEC (CDS/CDNSKEY).122

[119] Lista de correo electrónico de Jennifer Bryce al Equipo de Revisión SSR2, 27 de marzo de 2019, Asunto: respuestas sobre SSR del DNS, https://mm.icann.org/pipermail/ssr2-review/2019-March/001569.html.
[120] Nombres y Números de Internet (IANA), “Proceso de solicitud de cambio a la zona raíz”, consultado el 8 de diciembre de 2020, https://www.iana.org/help/root-zone-process.
[121] PTI, “Reunión de miembros de la ccNSO: actualización de la función de nombres de la IANA”, ICANN 60, 31 de octubre de 2017, diapositivas 11-14, https://ccnso.icann.org/sites/default/files/field-attached/presentation-pti-members-31oct17-en.pdf.
[122] Gudmundsson, O. y P. Wouters, "Administración de registros DS del principal mediante CDS/CDNSKEY", RFC 8078, DOI 10.17487/RFC8078, marzo de 2017, <https://www.rfc-editor.org/info/rfc8078>.

Si bien la organización de la ICANN anunció anteriormente el desarrollo y la implementación del nuevo sistema de RZMS con requisitos de seguridad más exigentes en torno a la comunicación, el Equipo de Revisión SSR2 no encontró ninguna indicación en cuanto a cuándo la organización de la ICANN planea poner en funcionamiento el nuevo sistema.

Recomendación 21 del SSR2: Mejorar la seguridad de las comunicaciones con los operadores de TLD

> 21.1. Las operaciones de la organización de la ICANN y la entidad PTI deberían acelerar la implementación de nuevas medidas de seguridad del RZMS en lo que respecta a la autenticación y la autorización de los cambios solicitados y ofrecer a los operadores de TLD la oportunidad de aprovechar esas medidas de seguridad, en particular, la autenticación multifactorial (MFA) y el correo electrónico cifrado.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN y la entidad PTI tengan un RZMS de próxima generación que implique un modelo de autenticación y autorización sólido y seguro para la presentación y aprobación de las solicitudes, así como funciones adicionales que mejoren la seguridad y estabilidad del sistema del DNS global.

Esta recomendación podrá considerarse efectiva cuando la organización de la ICANN mitigue los posibles problemas de seguridad y estabilidad que impliquen el uso indebido del RZMS mediante procedimientos mejorados para la gestión de identidades.

C. Datos de la zona raíz y registros de la IANA

Los registros de la IANA incluyen parámetros vitales especificados por las RFC en el Grupo de Trabajo en Ingeniería de Internet (IETF), el Equipo de Investigación sobre Internet (IRTF) y el Área de Presentación Independiente.[123] La disponibilidad e integridad de estos registros de parámetros son fundamentales y deben ser ilustradas claramente a la comunidad mediante indicadores clave de desempeño (KPI) formales. En la actualidad, las mediciones sobre la disponibilidad de los servicios proporcionados por la organización de la ICANN no están a disposición de la comunidad. Las partes interesadas necesitan dicha información para evaluar los aspectos de SSR de estos servicios con el transcurso del tiempo.

La organización de la ICANN también puede considerar que la creación de los KPI para la zona raíz del DNS (incluso las DNSSEC, la disponibilidad, la integridad, el uso indebido, etc.) es la manera eficiente de medir, seguir y comunicar a la comunidad las tendencias de datos que implican la zona raíz.

Los KPI útiles pueden incluir, en forma no taxativa:

- La demora de propagación de los cambios de la zona raíz a las instancias.
- La zona raíz del DNS (incluidas la disponibilidad, integridad de las DNSSEC, etc.), para que terceros puedan realizar un seguimiento de los aspectos de SSR.
- Medidas que demuestren el tamaño, el crecimiento y la composición de los registros de la IANA, y la disponibilidad global de redes en estos registros.

[123] IANA, "Procedimientos de registración de protocolos", 3 de enero de 2020, https://www.iana.org/help/protocol-registration.

Recomendación 22 del SSR2: Medidas de servicio

22.1. Para cada servicio sobre el que la organización de la ICANN tiene autoridad, incluidos la zona raíz y los servicios relacionados con gTLD, así como los registros de la IANA, la organización de la ICANN debería crear una lista de estadísticas y mediciones que reflejen el estado operativo (como la disponibilidad y la capacidad de respuesta) de ese servicio, y debería publicar un directorio de estos servicios, conjuntos de datos y mediciones en una única página en el sitio web icann.org, por ejemplo, en la Plataforma de Datos Abiertos. La organización de la ICANN debería elaborar mediciones para cada uno de estos servicios en forma de resúmenes tanto del año anterior como en forma longitudinal (para ilustrar el comportamiento básico de referencia).

22.2. La organización de la ICANN debería solicitar anualmente los comentarios de la comunidad sobre las mediciones. Esos comentarios deberían ser considerados, resumidos públicamente después de cada informe e incorporados en los informes de seguimiento. Los datos y las metodologías asociadas que se utilizan para medir los resultados de estos informes deberían archivarse y ponerse a disposición del público para fomentar la repetibilidad.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN haga que las mediciones de estado operativo sobre los servicios que la organización de la ICANN respalda estén a disposición de la comunidad.

Esta recomendación podrá considerarse efectiva cuando la comunidad observe un aumento en la transparencia de las operaciones relativas a la SSR de la organización de la ICANN.

D. Criptografía del DNS

El Equipo de Revisión SSR2 investigó dos temas en el área de criptografía del DNS. En primer lugar, el equipo investigó la transición del algoritmo de RSA a un algoritmo de curva elíptica para las firmas de las DNSSEC. En segundo lugar, el equipo investigó la necesidad de realizar una transición a un algoritmo de firma digital poscuántico.[124] Para seguir el ritmo de los avances en la tecnología informática tradicional, el tamaño de las claves de RSA debe aumentarse con el transcurso del tiempo. De manera alternativa, las DNSSEC podrían cambiar de RSA a criptografía de curva elíptica (ECC), la cual ofrece la misma seguridad con claves públicas más pequeñas y firmas más pequeñas. Además, existe una preocupación de que el invento de una computadora cuántica a gran escala podría quebrar tanto el RSA como la ECC. Antes de que se llegue a aprobar una computadora cuántica a gran escala, las DNSSEC deben cambiar a un algoritmo que seguro para el cómputo cuántico. La ICANN y la entidad PTI no tienen disposiciones en la Declaración de Prácticas de las DNSSEC (DPS) que permitan dicho cambio.

La organización de la ICANN no es la única organización que debe considerar los avances previstos en criptografía. Los grupos de estándares de la industria también se están preparando para un futuro poscuántico. La actividad más conocida es el proyecto de criptografía poscuántica NIST, que trabaja con investigadores de todo el mundo para desarrollar nuevos elementos básicos criptográficos que no sean susceptibles de ser atacados

[124] Véase “Apéndice G: criptografía” para obtener detalles sobre la investigación del equipo.

por computadoras cuánticas.[125] Se puede esperar que el proyecto demore varios años más antes de que los algoritmos resultantes estén listos para su normalización, pero está muy bien encaminado.

Mientras tanto, los investigadores acuerdan que las firmas basadas en hash son seguras para la tecnología poscuántica. El Equipo de Investigación sobre Internet (IRTF) ha especificado estos algoritmos de firmas en su Grupo de Investigación del Foro de Criptografía (CFRG), mediante el uso de claves públicas y privadas pequeñas con un bajo costo informático.[126] Sin embargo, las firmas son bastante grandes y una clave privada solo puede producir una cantidad finita de firmas. Estas dos propiedades hacen que las firmas basadas en hash no sean recomendables en el entorno de las DNSSEC.

La documentación de la organización de la ICANN no tiene en cuenta la necesidad de realizar una transición del algoritmo actual a otro. Esto hace que la organización de la ICANN no esté preparada para los avances previstos en los algoritmos de firma de clave criptográfica.

Recomendación 23 del SSR2: Traspaso de algoritmos

23.1. Las operaciones de la entidad PTI deberían actualizar la Declaración de Prácticas de las DNSSEC (DPS) para permitir la transición de un algoritmo de firma digital a otro, incluida una transición anticipada del algoritmo de firma digital RSA a otros algoritmos o a futuros algoritmos poscuánticos, que proporcionen la misma seguridad o mayor seguridad y preserven o mejoren la resiliencia del DNS.

23.2. Dado que el traspaso de un algoritmo DNSKEY de la raíz es un proceso muy complejo y delicado, las operaciones de la entidad PTI deberían trabajar con otros socios de la zona raíz y con la comunidad mundial para desarrollar un plan de consenso para futuros traspasos de algoritmos DNSKEY de la raíz, teniendo en cuenta las lecciones aprendidas del primer traspaso de la KSK de la zona raíz en 2018.

Esta recomendación podrá considerarse implementada cuando la entidad PTI actualice la DPS para permitir la transición de un algoritmo de firma digital a otro, y desarrolle un plan consensuado para futuros traspasos de algoritmos de DNSKEY de la raíz.

Esta recomendación podrá considerarse efectiva cuando la organización de la ICANN esté preparada para el uso de algoritmos más avanzados para la firma de claves, incluido todo aumento en la longitud de la clave y el plazo para el traspaso de la clave.

5. Operador de Registro Back-End de Emergencia (EBERO)

Un proveedor de EBERO funciona como un componente específico de la infraestructura de recuperación ante desastres (DR) y representa un rol importante en ofrecer sistemas y

[125] Instituto Nacional de Normas y Tecnología (NIST), Laboratorio de Tecnología de la Información, Recursos de Seguridad Informática, Centro, "Criptografía poscuántica", elaborado el 3 de enero de 2017, actualizado el 23 de noviembre de 2020, https://csrc.nist.gov/projects/post-quantum-cryptography.
[126] IRTF, Grupo de Investigación del Foro de Criptografía, https://irtf.org/cfrg.

capacidad operativa necesarios para asumir todas las funciones críticas de un registro de gTLD con fallas.

Un proveedor de EBERO se activa de manera temporaria si un operador de gTLD está en riesgo de no poder sostener las funciones críticas del registro.[127] Este proceso garantiza la disponibilidad de las funciones del operador de gTLD, protege a los registratarios y brinda una capa adicional de protección al DNS. Tal como indican varias normas reconocidas como la ISO 22301, la guía de mejores prácticas requiere que los procesos de DR se testeen periódicamente (véase la recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres).

El Equipo de Revisión SSR2 no pudo verificar que la organización de la ICANN coordinase las pruebas de extremo a extremo necesarias de todo el proceso de EBERO descriptas en el "Manual de Proceso de Transición Común, versión 3".[128] La organización de la ICANN y los proveedores de EBERO probaron las partes del proceso (se realizó una prueba con .doosan y otra con .mtpc); la prueba más reciente se llevó a cabo en 2017.[129] El Equipo de Revisión SSR2 encontró los resultados de dichas pruebas en procedimientos de reuniones en vez de cualquier página web dedicada de la ICANN.[130] El Equipo de Revisión reconoce que los detalles de la forma en que un proceso de EBERO de extremo a extremo es probado están fuera del alcance de una revisión de SSR; sin embargo, poder verificar que se realizaron estas pruebas y revisar sus resultados es fundamental para la transparencia de la comunidad.

También cabe mencionar que, si bien los procesos de EBERO están documentados en el Manual de Proceso de Transición Común, este documento fue extremadamente difícil de encontrar ya que está incluido en el acuerdo de EBERO.

Recomendación 24 del SSR2: Mejorar la transparencia y las pruebas de extremo a extremo del proceso EBERO

24.1. La organización de la ICANN debería coordinar las pruebas de extremo a extremo del proceso EBERO completo a intervalos predeterminados (al menos anualmente) utilizando un plan de pruebas que incluya los conjuntos de datos utilizados para las pruebas, los estados de progresión y las fechas límite, y que se coordine con las partes contratadas de la ICANN con antelación para garantizar que se ejerciten todos los tramos de excepción y se publiquen los resultados.

24.2. La organización de la ICANN debería facilitar la búsqueda del Manual del Proceso de Transición Común mediante la provisión de enlaces en el sitio web de EBERO.

[127] ICANN, "Operador de Registro Back-End de Emergencia", sin fecha, https://www.icann.org/resources/pages/ebero-2013-04-02-en.

[128] ICANN, "Acuerdo de Operador de Registro Back-End de Emergencia", agosto de 2019, https://www.icann.org/en/system/files/files/cira-ebero-15aug19-en.pdf. Nota: véase Anexo B: Procesos de transición comunes.

[129] ICANN, Informe de ejercicio de EBERO, presentación en el Día de la Tecnología, ICANN 55, 7 de marzo de 2016, https://meetings.icann.org/en/marrakech55/schedule/mon-tech/presentation-ebero-07mar16-en.pdf, y Murphy, Kevin, "Segundo registro de emergencia probado con marca de punto muerto", Domain Incite, 27 de abril de 2017, http://domainincite.com/21724-second-emergency-registry-tested-with-dead-dot-brand.

[130] Arias, Francisco, "Ejercicios de EBERO", presentación en el Día de la Tecnología, ICANN60, 30 de octubre de 2017, https://ccnso.icann.org/sites/default/files/field-attached/presentation-ebero-exercises-30oct17-en.pdf.

Esta recomendación podrá considerarse implementada cuando la organización de la ICANN coordine pruebas anuales de extremo a extremo de todo el proceso de EBERO con documentación pública para el resultado.

Esta recomendación podrá considerarse efectiva cuando la organización de la ICANN pueda validar que el proceso de EBERO funciona de la forma prevista, y que proteja a los registratarios y brinde una capa adicional de protección al DNS.

Apéndice A: Otras sugerencias

A lo largo del proceso de revisión, el Equipo de Revisión SSR2 notó varias áreas donde los cambios mejorarían la eficiencia y las capacidades de futuros equipos de revisión. Si bien estos temas están fuera del ámbito de competencia del Equipo de Revisión, esperamos que la organización de la ICANN considere las siguientes sugerencias como aportes a futuras iniciativas de revisión. Se enumeran en orden de prioridad.

Sugerencia 1

La organización de la ICANN debería implementar una función de seguimiento del progreso en línea para cada recomendación de cada equipo de revisión. Al brindar visibilidad en línea del progreso a lo largo de la implementación, toda la comunidad puede observar los detalles de implementación y brindar comentarios sobre cualquier deficiencia. Para lograr la transparencia y visibilidad deseadas, se necesitan mayor granularidad respecto de los planes de implementación y progreso que puedan observarse en las páginas web de implementación del CCT hoy en día.[131] El Equipo de Revisión SSR2 considera que la recomendación 1 no habría sido necesaria si dicha función hubiese sido establecida para la implementación de las recomendaciones del Equipo de Revisión SSR1. Además, basándose en el concepto de un mentor de implementación de CCT, la organización de la ICANN debería proporcionar informes trimestrales a los miembros del equipo de revisión que elaboró las recomendaciones, lo que permitiría que los mismos miembros del equipo de revisión brinden comentarios periódicos sobre si la implementación se está realizando de la manera prevista y evitaría preguntas de la próxima generación del equipo de revisión cuando evalúe la implementación. El Equipo de Revisión SSR2 considera que la evaluación de las recomendaciones del Equipo de Revisión SSR1 habría sido sencilla si dicha función hubiese estado implementada antes de que se reuniese el Equipo de Revisión SSR2.

Sugerencia 2

Para evitar malos entendidos y expectativas no cumplidas, la organización de la ICANN debería desarrollar un proceso claro y por escrito para obtener recursos contratados para los equipos de revisión, incluidos hitos y puntos para la aprobación del equipo de revisión. Cada equipo de revisión necesitará un redactor técnico, por lo que la organización de la ICANN debería suministrar al equipo de revisión un redactor técnico a partir de la primera reunión del dicho equipo.

Sugerencia 3

Para facilitar la investigación, inmediatamente después de finalizado el período de comentario público y para “abordar las crecientes necesidades de inclusión, responsabilidad y transparencia”, como se indica en el objetivo estratégico 2.1, el Equipo de Revisión SSR2 sugiere que la organización de la ICANN cree una lista de correo electrónico para anuncios sobre los períodos de comentario público. Por el momento, encontrar información sobre comentarios públicos puede resultar bastante difícil. La implementación de esta sugerencia servirá para aumentar el conocimiento entre los suscriptores de la lista de correo electrónico de periodos de comentario público, sin requerir un esfuerzo adicional. La existencia de estos

[131] ICANN, “Recomendaciones aceptadas del Equipo de Revisión de Competencia, Confianza y Elección de los Consumidores (CCT-RT) – Plan para la implementación y próximos pasos”, consultado el 19 de diciembre de 2020, https://www.icann.org/public-comments/cct-rt-implementation-plan-2019-09-11-en.

mensajes permitirá que los miembros de futuros equipos de revisión y otras partes relevantes busquen información fácilmente mediante herramientas de búsqueda en archivos de correo electrónico ya disponibles.

El Equipo de Revisión SSR2 sugiere que la organización de la ICANN debería enviar al menos tres mensajes por período de comentario público a esta lista de correo electrónico. El primer mensaje debería enviarse al momento de la apertura del período de comentario público y debería incluir un URL estable al documento preliminar relevante. El segundo mensaje debería enviarse al momento del cierre del período de comentario público y debería incluir un URL estable a la recopilación de comentarios presentados. El tercer mensaje debería indicar si se llegó a un consenso y, de ser así, debería incluir un URL estable al documento final. También podrían ser de utilidad otros mensajes, como una extensión al período de comentario público. Además, el Equipo de Revisión SSR2 sugiere que la organización de la ICANN cree una página web dedicada para enumerar todas las convocatorias públicas para comentarios, que luego debería enlazarse a la página de los documentos relevantes.

Sugerencia 4

Para que las discusiones sobre seguridad sean transparentes, la organización de la ICANN debería considerar establecer una plataforma abierta de garantía de información para compartir información de seguridad y uso indebido a fin de permitir que la información sea más fluida y su divulgación sea más rápida.

Apéndice B: Definiciones y acrónimos

Definiciones

Una evaluación de este tipo requiere una comprensión común de los términos clave asociados con la revisión. Inicialmente, el Equipo de Revisión SSR2 se desempeñó en virtud de las siguientes definiciones.[132]

- Uso indebido: véase “uso indebido del DNS” más adelante
- Correo electrónico corporativo comprometido (BEC): tipo de estafa dirigido a compañías donde las cuentas de correo electrónico de los empleados son suplantadas o vulneradas para realizar transferencias electrónicas.
- Botnet: red de computadoras infectadas con malware y controladas como un grupo sin el conocimiento de los propietarios de las computadoras.
- Fraude de certificado digital: un atacante vulnera una autoridad de certificación (CA) para generar y obtener certificados fraudulentos para lanzar más ataques; un atacante también puede usar certificados fraudulentos para autenticarse como otro individuo o sistema, o para falsificar firmas digitales.
- Ataque de Denegación de Servicio Distribuido (DDoS): intento malicioso para interrumpir un servidor, servicio o red específico al abrumar el objetivo o su infraestructura circundante con un aluvión de tráfico en Internet de varias fuentes (distribuidas).
- Uso indebido del DNS: uso incorrecto intencional de los identificadores universales proporcionados por el DNS para infraestructura de ciberdelito y que direcciona usuarios a sitios web que permiten otras formas de delito, como explotación infantil, infracción a la propiedad intelectual y fraude.
- Sistema de Nombres de Dominio (DNS): el DNS es un servicio de base de datos en línea distribuido que traduce los nombres de dominio fáciles de recordar a direcciones de protocolo de Internet (IP) numéricas; por ejemplo, el DNS traducirá www.icann.org a 192.0.34.65 (especificado en las RFC 1034 y 1035).
- Marco de Seguridad, Estabilidad y Flexibilidad de Sistemas de Identificadores (IS-SSR): documento, actualizado periódicamente, que “describe el rol y los límites de la ICANN al respaldar una Internet única con interoperabilidad mundial y los desafíos para los sistemas de identificadores únicos de Internet”:
- Malware: software específicamente diseñado para interrumpir, dañar u obtener acceso no autorizado a un sistema informático.
- Phishing: intento fraudulento para obtener información sensible que se oculta como una entidad de confianza en una comunicación electrónica.
- Ransomware: malware diseñado para bloquear el acceso a un sistema informático hasta que se pague una suma de dinero.
- Flexibilidad: capacidad del sistema de identificadores de resistir, tolerar y sobrevivir eficazmente a los ataques maliciosos y otros eventos disruptivos sin interrupción o suspensión del servicio.
- Estafa: engaño fraudulento realizado para que parezca una actividad comercial u oportunidad de inversión real diseñado para ganar dinero.
- Seguridad: capacidad de proteger y evitar el uso indebido de los identificadores únicos de Internet.

[132] ICANN, “Rol y ámbito de competencia de SSR”, consultado el 27 de diciembre de 2019, https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en.

- Amenaza a la seguridad: phishing, estafa, malware, ransomware, spam, ataques de DDoS, fraude de certificado digital y botnets son algunas de las amenazas más críticas a la seguridad.
- Spam: correo electrónico masivo no deseado.
- Estabilidad: capacidad de garantizar que el sistema de identificadores funcione de la manera prevista y que los usuarios de identificadores únicos confíen en que funciona según lo esperado.
- Identificadores únicos: la misión técnica de la ICANN incluye ayudar a coordinar, a nivel general, la asignación del sistema de identificadores únicos de Internet; en particular, nombres de dominio de alto nivel, bloques de direcciones de Protocolo de Internet (IP) y números del sistema autónomo (AS) asignados a los registros regionales de Internet, y parámetros de protocolo como lo exige el IETF.

Acrónimos

- AS: Sistema Autónomo
- BC: Continuidad de Operaciones
- CISO: Director de Seguridad de Tecnologías de la Información
- CSO: Director de Seguridad
- CZDS: Sistema de Datos de Zona Centralizado
- DAAR: Informe de Actividades de Uso Indebido de Dominios
- DNS: Sistema de Nombres de Dominio
- DNSSEC: Extensiones de Seguridad del DNS (como se especifica en las RFC 4033, 4034 y 4035)
- DoH: DNS sobre HTPPS
- DoT: DNS sobre TLS
- DPS: Declaración de Prácticas de DNSSEC
- DR: recuperación ante desastres
- DURZ: Zona Raíz Intencionalmente No Validable
- EBERO: Operador de Registro Back-End de Emergencia
- EPDP: Proceso Expeditivo de Desarrollo de Políticas
- FSM: máquina de estado finito
- gTLD: dominio genérico de alto nivel
- GNSO: Organización de Apoyo para Nombres Genéricos
- HTTP: Protocolo de transferencia de hipertexto
- HTTPS: Protocolo de Transferencia de Hipertexto Seguro
- IANA: Autoridad de Números Asignados en Internet
- IETF: Grupo de Trabajo en Ingeniería de Internet
- IMRS: servidor raíz gestionado por la ICANN
- IP: Protocolo de Internet
- IRTF: Equipo de Investigación sobre Internet
- Marco de IS-SSR: Marco de Seguridad, Estabilidad y Flexibilidad de Sistemas de Identificadores de Internet
- ISMS: Sistema de Gestión de Seguridad de la Información
- ISO: Organización Internacional de Normalización
- ITIL: biblioteca de infraestructura de TI
- KSK: clave para la firma de la llave de la zona raíz
- NCAP: Proyecto de Análisis de Colisiones de Nombres
- NIST: Instituto Nacional de Normas y Tecnología
- OCTO: Oficina del Director de Tecnologías
- PII: Información de identificación personal

- PTI: Identificadores Técnicos Públicos
- RDS: Servicios de Directorio de Registración
- RAA: Acuerdo de Acreditación de Registradores
- RAPWG: Grupo de Trabajo sobre Políticas de Uso Indebido de Registraciones
- RDAP: Protocolo de Acceso a los Datos de Registración de Nombres de Dominio
- RSSAC: Comité Asesor del Sistema de Servidores Raíz
- SADAG: Análisis estadístico del uso indebido del DNS en los gTLD
- SMART: específico, mensurable, asignable, relevante y rastreable
- SOP: planes operativos y estratégicos
- SSAC: Comité Asesor de Seguridad y Estabilidad
- SSAE: declaración sobre normas para compromisos de certificación
- SSR: Seguridad, Estabilidad y Flexibilidad
- SSR1: primer proceso de revisión de SSR
- SSR2: segundo proceso de revisión de SSR
- TLS: Seguridad de la Capa de Transporte

Apéndice C: Proceso y metodología

Proceso y metodología para la revisión de las recomendaciones del SSR1

El proceso de evaluación del Equipo de Revisión SSR2 descripto más adelante se basa en resúmenes informativos de miembros del personal de la organización de la ICANN y debates con ellos; la revisión sistemática de una cantidad sustancial de documentos de la ICANN relevantes e informes de implementación creados por la organización de la ICANN; y entrevistas e investigaciones adicionales.[133] El equipo también usó sesiones de difusión y alcance en las reuniones públicas de la ICANN en Barcelona y Kobe para establecer contactos con partes interesadas relevantes de la comunidad. La evaluación fue cuantitativa y cualitativa, donde fue posible, según la recomendación específica.

Muchas recomendaciones del SSR1 eran generales y carecían de especificidad. El Equipo de Revisión SSR2 no tenía autoridad para acceder y analizar los trabajos internos de la ICANN y, por ende, solicitó a la organización de la ICANN que suministrase sus planes de implementación y evidencia de implementación exitosa a los miembros del Equipo de Revisión SSR2. Las recomendaciones en sí y la documentación proporcionada por la organización de la ICANN carecían de KPI y objetivos definidos, metas mensurables y planes de implementación. Esto dificultó la medición o el seguimiento de las implementaciones. Además, la redacción de algunas de las recomendaciones dejó lugar a interpretaciones. En ocasiones, esto generó un entendimiento diferente de la recomendación por parte del equipo SSR2 de aquel usado por el personal de la organización de la ICANN.

Para cada recomendación, el personal de la organización de la ICANN brindó al equipo respuestas iniciales sobre la implementación en 2017, e informó sobre cómo implementó las recomendaciones del SSR1. El personal de la ICANN citó páginas web o documentos, organizó presentaciones de varios departamentos con la organización de la ICANN y también brindó al equipo resúmenes informativos sobre las recomendaciones durante nueve meses. Asimismo, el equipo revisó una cantidad importante de documentos de referencia relevantes a esta revisión. El equipo llevó a cabo entrevistas con el personal de la organización de la ICANN, solicitó información adicional y usó los aportes de partes interesadas relevantes y su propia investigación para realizar posteriores análisis en los casos necesarios.

Después de recibir respuestas de la organización de la ICANN a las preguntas presentadas y de finalizar su investigación y verificación de antecedentes del mejor modo posible, el equipo elaboró evaluaciones preliminares para cada recomendación de mediados a fines de 2018, las cuales se debatieron en línea, en las llamadas semanales del equipo y en reuniones presenciales. El equipo editó el texto según fue necesario y aprobó las conclusiones y los hallazgos para cada recomendación del SSR1 con la intención de su inclusión en el informe preliminar del Equipo SSR2, con los protocolos de consenso aprobados del equipo, y señaló las objeciones minoritarias donde era aplicable.

[133] Wiki del Equipo de Revisión SSR2 de la ICANN, https://community.icann.org/display/SSR/SSR2+Review. Véase, en particular, Materiales de referencia y Materiales informativos.

Después de debatir en línea y en llamadas, y de realizar varias iteraciones, el equipo decidió estructurar su evaluación preliminar de acuerdo con la siguiente metodología, que se centró en la finalización de la tarea, la relevancia y el posterior trabajo requerido:

1. ¿Qué se realizó para implementar la recomendación?
2. ¿Se implementó la recomendación en su totalidad?
3. ¿La implementación tuvo el resultado esperado?
4. ¿Cómo se llevó a cabo la evaluación?
5. ¿La recomendación es todavía relevante hoy en día?
6. De ser así, ¿qué otras tareas se necesitan? Si no es así, ¿por qué no?

La primera pregunta se refiere a qué realizó la organización de la ICANN para implementar la recomendación. La segunda pregunta brinda la evaluación del equipo del nivel de implementación a la "fecha de implementación completa" brindada por el personal. El equipo encontró muchas recomendaciones que parecen haberse implementado solo en forma parcial o donde faltaban planes de implementación. En estos casos, el equipo identificó áreas específicas que necesitan mejoras. En algunos casos, resultó difícil establecer condiciones previas y objetivos claros necesarios para la correcta implementación debido a la de falta planes de implementación, documentación e indicadores de desempeño. La tercera pregunta aborda si la implementación tuvo el resultado esperado y, de ser así, en qué medida. La cuarta pregunta se refiere a la forma en que el Equipo de SSR2 realizó la evaluación. Los lectores pueden buscar documentos y otras pruebas que usó el equipo por recomendación. Basándose en la quinta pregunta, el equipo también evaluó si cada recomendación siguió siendo relevante en el año 2018. Por último, el equipo decidió si las circunstancias actuales justifican trabajo adicional para implementar una forma de esta recomendación, que luego informaría el conjunto de recomendaciones del Equipo SSR2.

Proceso y metodología para SSR de la ICANN, SSR del DNS y futuros desafíos

El Equipo de Revisión SSR2 realizó una serie de entrevistas con el personal de la organización de la ICANN.[134] Las preguntas se centraron en la compleción y efectividad de los procesos de seguridad de la organización de la ICANN y la efectividad del marco de seguridad de dicha organización.

El Equipo de Revisión SSR2 se organizó en torno a un proceso específico para afirmar las conclusiones y elaborar recomendaciones para ser consideradas por la ICANN, entre ellas:

- Revisar, analizar y resumir documentación relevante.
- Llevar a cabo investigaciones dentro de las áreas identificadas que generan inquietudes.
- Realizar entrevistas relevantes según resulte pertinente.
- Elaborar un resumen de los fundamentos, conclusiones y recomendaciones.

El Área de Trabajo 2 se centró en las preocupaciones relativas a la SSR dentro de la organización de la ICANN, mientras que el Área de Trabajo 3 se centró en la SSR de los sistemas de identificadores globales: el DNS global, las bases de datos de números de la IANA (asignaciones de IP y ASN) y los registros de protocolos de la IANA. Específicamente, el

[134] Wiki del Equipo de Revisión SSR2 de la ICANN, https://community.icann.org/display/SSR/SSR2+Review. Véase, en particular, Materiales informativos.

Equipo de Revisión consideró informes y otros aportes sobre los riesgos, amenazas y uso indebido del DNS, y luego mapeó los datos resultantes a los componentes, procedimientos y políticas relevantes de la ICANN.
Dentro del Área de Trabajo 4, respecto de futuros desafíos para la seguridad, estabilidad y flexibilidad, el Equipo de Revisión SSR2 consideró la investigación actual sobre el uso indebido del DNS, el impacto de la evolución continua de los tipos y volumen de los dispositivos en el DNS, la tecnología emergente, las áreas identificadas que generan preocupación en otras áreas de trabajo que pueden tener futuras implicancias, y las metodologías institucionalizadas de la ICANN para análisis y mitigación de amenazas.
El Equipo de Revisión SSR2 reconoció que esta área de trabajo dependió de los temas emergentes de las otras áreas dependientes. Más específicamente, además de los desafíos comúnmente identificados, la estabilidad y la flexibilidad del DNS pueden enfrentar otros desafíos específicos bajo el área de trabajo en lo relacionado a la SSR de la ICANN y a la SSR del DNS.

Apéndice D: Conclusiones relacionadas con las recomendaciones del SSR1

Esta sección incluye una evaluación detallada de cada una de las recomendaciones del SSR1. Las conclusiones contenidas aquí analizan las implementaciones específicas, sus cuestiones y las ideas del equipo respecto al trabajo futuro. El Equipo de Revisión SSR2 destacó las siguientes cuestiones repetitivas:

1. Faltan indicadores, mediciones y directrices que permitan a la comunidad y a la organización de la ICANN hacer un seguimiento y comprender el espacio de seguridad y sus propias actividades.

2. Falta evidencia, definiciones y procedimientos públicamente disponibles, lo que inhibe la observación de las actividades en materia de SSR y lo que conlleva falta de claridad respecto de lo que se está realizando, cuándo se realiza, quién lo realiza y cómo.

3. No hay revisión ni responsabilidad de la comunidad, lo que niega las oportunidades de la comunidad de la ICANN de brindar aportes sobre cuestiones relacionadas con la seguridad, estabilidad y flexibilidad.

4. La organización de la ICANN no tiene actualmente una estrategia general, metas identificables ni una política clara e integral sobre la SSR. Sin una estrategia funcional de SSR ni una gestión de riesgos y seguridad integrada (por ejemplo, políticas, procedimientos, estándares, bases, pautas), las responsabilidades relacionadas con la seguridad, estabilidad y flexibilidad no son asignadas, medidas y rastreadas, lo que genera una falta de transparencia y responsabilidad.

Recomendación 1 del SSR1

"La ICANN debería publicar una única declaración clara y consistente de su ámbito de competencia de SSR y su misión técnica limitada. La ICANN debería recabar y obtener aportes públicos a fin de lograr una declaración basada en el consenso".

Conclusión del SSR2: esta recomendación sigue siendo relevante ya que fue implementada en forma parcial pero no logró por completo el resultado esperado de tener una declaración clara, consistente y basada en el consenso que describiese el ámbito de competencia de SSR y la misión técnica de la organización de la ICANN.

Fundamentos:

- El equipo observó que existe una declaración y que la organización de la ICANN actualizó (pero ya no mantiene) esa declaración como resultado de una revisión realizada por la comunidad.[135] A pesar de la existencia de esta declaración y sus definiciones claras de "Seguridad, Estabilidad y Flexibilidad", el uso de estas definiciones sigue siendo

[135] Rol y ámbito de competencia de SSR, https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en, y "Equipo de Revisión de Seguridad, Estabilidad y Flexibilidad del DNS – Informe preliminar: Informe de comentarios públicos", modificado por última vez el 18 de mayo de 2012, http://www.icann.org/en/system/files/files/report-comments-ssr-rt-draft-report-18may12-en.pdf.

inconsistente. Conversaciones paralelas con miembros del equipo que tienen acceso al texto de contratos de la organización de la ICANN con varias partes contratadas han indicado que las definiciones de “seguridad” y “estabilidad” usadas dentro de dichos contratos son diferentes.[136]
- No se proporcionaron mediciones para evaluar si la implementación tuvo el resultado esperado de brindar información clara y consistente sobre su ámbito de competencia de SSR y los límites de su misión técnica. Dados los diferentes modos en que se utiliza el término “SSR” en toda la ICANN, no se llegó a la definición común que esperaba el Equipo de Revisión SSR1.

Recomendación 2 del SSR1

“La definición de la ICANN y la implementación de su ámbito de competencia de SSR y su misión técnica limitada deberían ser revisadas a fin de mantener el consenso y obtener aportes de la comunidad. El proceso debería repetirse en forma periódica, quizá junto con el ciclo de futuras revisiones de SSR”.

Conclusión del SSR2: esta recomendación sigue siendo relevante y no fue implementada en su totalidad. El resultado esperado de tener un proceso de revisión público periódico para el ámbito de competencia de SSR de la ICANN y su misión técnica asociada no se logró.

Fundamentos:
- El Equipo de Revisión SSR2 no encontró evidencia alguna de que se hayan llevado a cabo revisiones periódicas del ámbito de competencia de SSR. No hubo oportunidades de comentar específicamente sobre la declaración de misión y ámbito de competencia desde 2013.

Recomendación 3 del SSR1

“Una vez que la ICANN emita una declaración basada en consenso de su ámbito de competencia de SSR y su misión técnica limitada, la ICANN debería usar terminología y definiciones consistentes de esta declaración en todos los materiales”.

Conclusión del SSR2: esta recomendación aún es relevante, pero no fue implementada en su totalidad. El resultado esperado de trabajar sobre una terminología y un conjunto de descripciones consistentes para los materiales relacionados con la SSR no fue logrado.

Véase la recomendación 13 del SSR2: Aumentar la transparencia y la responsabilidad en la presentación de reclamos por uso indebido para la recomendación de SSR2 que amplía la recomendación original del SSR1.

Fundamentos:
- Una publicación de blog de junio de 2013 enumera la terminología de seguridad de la organización de la ICANN disponible para todas la comunidad; no obstante, estas

[136] Véase también la sección 7.3 de Acuerdo Base de Nuevos gTLD https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html en comparación con las definiciones de seguridad y estabilidad de la organización de la ICANN https://www.icann.org/groups/ssac

definiciones no parecen estar integradas de manera consistente en otros documentos relacionados con la SSR.[137]

- El informe del personal de la organización de la ICANN sobre esta recomendación indica que el personal agregaría términos clave al glosario público de la organización de la ICANN de manera periódica como parte del Plan Operativo y Estratégico (SOP); a medida que las actividades relativas a la SSR evolucionen, se actualizarán la terminología y las descripciones como parte del SOP. No obstante, el glosario (encontrado en la publicación de blog mencionada anteriormente) no se actualiza desde febrero de 2014.

Recomendación 4 del SSR1

"La ICANN debería documentar y definir con claridad la naturaleza de las relaciones de SSR que tiene dentro de la comunidad de la ICANN a fin de brindar un único punto focal para comprender las interdependencias entre las organizaciones".

Conclusión del SSR2: esta recomendación sigue siendo relevante, pero no fue implementada en su totalidad. El resultado esperado de brindar un recurso abierto y transparente que describa las relaciones de SSR de la organización de la ICANN no fue logrado.

Véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- El personal de la organización de la ICANN creó un documento para el Equipo de Revisión SSR2 que realiza un seguimiento de los roles y responsabilidades relacionados con la SSR, y enumera cada una de las organizaciones con las que la organización de la ICANN haya alguna vez tenido una relación formal.138 El documento incluye referencias específicas a documentos que sustentan cada una de esas relaciones y una descripción de los componentes de SSR de dicha relación. Muchas de las referencias mencionadas en ese documento, no obstante, no pueden localizarse en línea. El documento generalmente muestra los componentes de SSR de las relaciones como "desconocidos".

Recomendación 5 del SSR1

"La ICANN debería usar la definición de sus relaciones de SSR para mantener acuerdos de trabajo efectivos y demostrar cómo se utilizan estas relaciones para lograr cada meta relativa a la SSR".

Conclusión del SSR2: esta recomendación aún es relevante, pero no fue implementada en su totalidad. El Equipo de Revisión no pudo determinar si la organización de la ICANN logró el resultado esperado de acuerdos de trabajo efectivos en respaldo a cada meta de SSR.

Véase la recomendación 3 del SSR2: Mejorar la transparencia presupuestaria relacionada con la SSR para la recomendación del SSR2 que amplía la recomendación original del SSR1.

[137] ICANN, "Terminología de seguridad de la ICANN", blog, modificado por última vez el 8 de julio de 2013, https://www.icann.org/news/blog/icann-s-security-terminology.

[138] "Relaciones de SSR", ICANN, 23 de enero de 2017, https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf.

Fundamentos:

- El equipo esperaba que el Marco de IS-SSR incluyera información sobre cómo las relaciones clave exigidas en la recomendación 4 del SSR1 se utilizan para lograr las metas de SSR; sin embargo, esta información no es fácil de obtener.[139]
- El equipo SSR2 no tuvo información suficiente para evaluar si las relaciones de trabajo son funcionales.

Recomendación 6 del SSR1

"La ICANN debería publicar un documento que detalle claramente los roles y responsabilidades del SSAC y del RSSAC a fin de delinear con claridad las actividades de los dos grupos. La ICANN debería buscar consenso para esto en los dos grupos, reconociendo la historia y las circunstancias de la formación de cada uno. La ICANN debería considerar la dotación de recursos adecuados para ambos grupos, de acuerdo con las exigencias que se les imponen".

Conclusión del SSR2: esta recomendación aún es relevante, pero no fue implementada en su totalidad. La organización de la ICANN no logró el resultado esperado de hacer que los roles del SSAC y del RSSAC sean claros para todas las partes interesadas.

Fundamentos:

- Los roles y responsabilidades del SSAC y del RSSAC están contenidos en un documento.[140] Sin embargo, este documento público aún está marcado como "BORRADOR EN REVISIÓN". Al parecer, el trabajo se inició respecto de esta recomendación, pero concluyó sin abordar las revisiones organizacionales del SSAC y del RSSAC Si se llegó a un consenso, el Equipo de Revisión SSR2 no pudo localizar el documento final.
- El documento se basa en los Estatutos de la ICANN que datan de antes de la transición de la IANA. Las partes de los Estatutos que describen el SSAC y el RSSAC son mayormente iguales, pero el RSSAC ahora tiene la tarea explícita de responder "a las solicitudes de información u opiniones de la Junta Directiva". La actualización no resolvió la potencial superposición de roles y responsabilidades entre el SSAC y el RSSAC en los Estatutos de la ICANN:

  > *"El SSAC debe informar a la comunidad y Junta de la ICANN sobre cuestiones relativas a la seguridad e integridad de los sistemas de asignación de nombres y direcciones de Internet;*
  >
  > *el RSSAC debe informar a la comunidad y Junta de la ICANN sobre cuestiones relativas a la operación, administración, seguridad e integridad del Sistema de Servidores Raíz de Internet".*

Recomendación 7 del SSR1

"La ICANN debería basarse en su Marco de SSR actual mediante el establecimiento de un conjunto claro de objetivos y la priorización de sus iniciativas y actividades de acuerdo con estos objetivos".

---

[139] Ibídem.

[140] ICANN, "BORRADOR EN REVISIÓN: Los roles y responsabilidades del Comité Asesor de Seguridad y Estabilidad y del Comité Asesor del Sistema de Servidores Raíz de la ICANN", 5 de marzo de 2015, https://www.icann.org/en/system/files/files/draft-rssac-ssac-roles-responsibilities-05mar15-en.pdf.

Conclusión del SSR2: la recomendación sigue siendo relevante y fue implementada en forma parcial. El resultado esperado de tener objetivos de SSR claros y públicamente revisados, y su esfuerzo de priorización asociado, no fue logrado.

Véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos, y la recomendación 3 del SSR2: Mejorar la transparencia presupuestaria relacionada con la SSR para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- Las actividades relacionadas con la SSR se informan de manera periódica como parte de los Planes Operativos y Estratégicos (SOP), incluidos los informes de gestión de carteras de proyectos y los informes trimestrales sobre la SSR.[141] Los SOP fueron informados por el Marco de IS-SSR, que incluyó prioridades, objetivos y actividades respecto de la SSR. Sin embargo, ese marco ya no se elabora, lo que deja una brecha en torno a la forma en que el SOP toma en cuenta las acciones relacionadas con la SSR. El proceso para actualizar documentos relacionados con la SSR no es claro, ya que la última publicación del Marco de IS-SSR se publicó en el año 2016.[142]
- El Marco de IS-SSR ofreció la oportunidad de que la comunidad informara la estrategia para SSR. La organización de la ICANN ya no elabora dicho marco, lo que no genera suficientes oportunidades de recopilar aportes de la comunidad de todos los grupos de partes interesadas de la ICANN sobre cómo dicha organización trata las actividades de SSR.
- La planificación estratégica para las cuestiones de seguridad, estabilidad y flexibilidad parecen centrarse en la Oficina del Director de Tecnologías (OCTO) y, debido a la existencia del SOP, el Equipo de Revisión reconoció que existe un nivel de planificación en torno a las actividades de SSR dentro de la OCTO. No obstante, el nivel de detalle y planificación previsto en la recomendación no incluye debates públicos de manera equitativa entre todas las partes interesadas de la organización de la ICANN.

Recomendación 8 del SSR1

"La ICANN debería continuar perfeccionando sus objetivos del Plan Estratégico, en particular, el objetivo de mantener e impulsar la disponibilidad del DNS. Alineamiento claro del Marco y Plan Estratégico".

Conclusión del SSR2: si bien esta recomendación hoy en día sigue siendo relevante y fue implementada en forma parcial, la implementación de esta recomendación no logró el resultado esperado de brindar un enlace más claro entre la estrategia relacionada con la SSR y el trabajo operativo.

---

[141] ICANN, "Plan Estratégico de la ICANN para los años fiscales 2021 a 2025

", sin fecha, https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf , y Dave Piscitello, "Informe de actividades de SSR del Sistema de Identificadores", blog de la ICANN, modificado por última vez el 21 de enero de 2015, https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

[142] ICANN, Marco de IS-SSR (año fiscal 2015-2016), https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

Véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos, y la recomendación 3 del SSR2: Mejorar la transparencia presupuestaria relacionada con la SSR para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- Documentos disponibles en la página de inicio de la implementación de la Revisión SSR1 indican que las pautas sobre la SSR se incluyen y abordan en informes, estrategias y procedimientos relevantes.[143] Sin embargo, los informes disponibles no brindan información suficiente sobre las actividades relativas a la SSR ni ofrecen detalles respecto de la implementación y la ejecución de las actividades de SSR.
- El SOP no indica qué actividades, prioridades y gastos en el SOP se relacionan con la SSR. Fundamentalmente, los mecanismos previstos por el SSR1 han sido reemplazados por otras herramientas organizacionales y procesales, lo que complica la evaluación y la implementación.

Recomendación 9 del SSR1

"La ICANN debería evaluar las opciones de certificación con las normas internacionales comúnmente aceptadas (por ejemplo, ITIL, ISO y SAC-70) para sus responsabilidades operativas. La ICANN debería publicar un plan de acción claro respecto de la certificación".

Conclusión del SSR2: esta recomendación sigue siendo relevante. El Equipo de Revisión SSR2 no pudo determinar si esta recomendación fue totalmente implementada ni si logró el resultado esperado, ya que la recomendación original no tenía la especificidad necesaria respecto de a qué certificación o certificaciones la organización debería apuntar o qué fines se esperaban.

Véase la recomendación 4 del SSR2: Mejorar los procesos y procedimientos de gestión de riesgos, y la recomendación 5:

Cumplir con los sistemas de gestión de seguridad de la información apropiados y las certificaciones de seguridad para las recomendaciones del SSR2 que amplían la recomendación original del SSR1.

Fundamentos:

- De acuerdo con las entrevistas con el personal de la organización de la ICANN, la organización de la ICANN ha buscado algunas certificaciones centradas en la IANA, por ejemplo, SOC2/3 Certificación del Sistema de KSK de la zona raíz, SOC2 Certificación de los Sistemas de Asignación y Mantenimiento de Registros, y SysTrust para la implementación de las DNSSEC a nivel de la raíz.144 Más allá de las funciones de la IANA, la organización de la ICANN genera informes mediante el uso de marcos de mejora continua en TI y ciberseguridad, tiene una auditoría financiera anual, realiza una revisión de documentación y autoevaluación de EFQM, y obtiene asesoramiento profesional para ayudar a medir el desempeño e impulsar las mejoras.145

[143] Wiki, página de inicio de la implementación del SSR1, actualizada por última vez el 22 de agosto de 2017, https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home.
[144] Véase el documento de trabajo, "Preguntas y respuestas del SSR2", sin fecha, 6, https://community.icann.org/pages/viewpage.action?pageId=64076120.
[145] Ibídem, 24.

- La organización de la ICANN también informa que todo el personal de seguridad de la información se capacita mediante las ofertas de SANS.146
- La organización de la ICANN informa que los resultados de las auditorías internas se informan únicamente a la Junta Directiva de la ICANN.147
- El Equipo de Revisión SSR2 no pudo encontrar ningún documento que pudiera usarse como plan de acción para la certificación de procesos de SSR, lo que imposibilita la revisión de la comunidad.

Recomendación 10 del SSR1

"La ICANN debería continuar con sus esfuerzos para aumentar el cumplimiento contractual efectivo y brindar recursos adecuados para esta función. La ICANN también debería elaborar e implementar un proceso más estructurado para supervisar las cuestiones e investigaciones relativas al cumplimiento".

Conclusión del SSR2: esta recomendación sigue siendo relevante y no fue implementada en su totalidad. El resultado esperado de tener recursos adecuados destinados al cumplimiento contractual efectivo y de desarrollar un proceso estructurado continuo para supervisar el cumplimiento no fue logrado.

Véase la recomendación 8 del SSR2: Permitir y demostrar la representación del interés público en las negociaciones con las partes contratantes y la recomendación 9 del SSR2: Supervisar y exigir el cumplimiento de las recomendaciones del SSR2 que amplían la recomendación original del SSR1.

Fundamentos:

- La evaluación se basa en información públicamente disponible (por ejemplo, la página de Informes de Cumplimiento Contractual), así como un informe del personal de la ICANN que proporcionó evidencia de la implementación de la recomendación.[148] Los informes públicos periódicos de las actividades de cumplimiento son parte del Plan Operativo y Estratégico (SOP) de la organización de la ICANN. La organización de la ICANN tiene una página pública exclusiva para los informes de Cumplimiento Contractual, incluidos datos sobre datos mensuales, trimestrales y anuales; diez informes diferentes consultables durante un período de 13 meses sucesivos; y mediciones y datos como los solicitan explícitamente diferentes grupos de trabajo. En la actualidad, hay implementados algunos programas de difusión y alcance y auditorías de Cumplimiento Contractual. La organización de la ICANN creó nuevos cargos después de la Revisión SSR1 para garantizar el cumplimiento de las metas y los objetivos en esta área.
- Los mecanismos de reclamos fueron actualizados mediante la migración al sitio web de la organización de la ICANN, la automatización y el lanzamiento de una herramienta de reclamos masivos. Además, el personal de la ICANN indicó que se llevó a cabo una

146 Ibídem, 11.

147 Ibídem, 6.

148 El informe de implementación del SSR1 está disponible en https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2 (diapositivas 28 a 30) y el resumen informativo del SSR2-RT sobre esta recomendación está disponible en https://community.icann.org/download/attachments/66085372/SSR1%20Compliance%20Briefing%20June%202017%20v3.pdf?version=2&modificationDate=1499814488000&api=v2.

encuesta de opinión.[149] La organización de la ICANN inició un control de calidad de inexactitudes dentro de los datos de RDS. El Informe de Exactitud de RDS ha estado en curso desde que el Equipo de Revisión de WHOIS recomendó la acción en 2012.

- Los informes de cumplimiento efectivo para los años 2017 y 2016 contienen muy poca evidencia de las acciones en pos del cumplimiento efectivo de SSR, a pesar del acuerdo base de registro de nuevos gTLD (julio de 2017) que contiene obligaciones específicas en las partes contratadas en relación con la seguridad y estabilidad, y pueden ayudar a la posterior implementación.150 No queda claro para el Equipo de Revisión SSR2 cómo el objetivo de la organización de la ICANN de reducir la incidencia y el impacto del uso indebido de registros y conductas maliciosas se lleva a cabo mediante acciones de cumplimiento u otras iniciativas. La mayoría de las cuestiones en el informe de implementación de SSR1 del personal señala cuestiones relativas al WHOIS. Además, el Acuerdo de Registradores (RAA de 2013) contiene derechos ambiguos para exigir el cumplimiento para la organización de la ICANN en relación con los registradores cuya operación pone en peligro los servicios de registradores y registros, el DNS o la Internet.
- La organización de la ICANN elabora informes mensuales sobre su trabajo en pos del cumplimiento efectivo, pero no queda claro la medida en que las cuestiones de SSR se administran dentro del proceso de cumplimento efectivo.151

Recomendación 11 del SSR1

"La ICANN debe finalizar e implementar medidas de éxito para los nuevos gTLD y avance acelerado de IDN (Nombres de Dominio Internacionalizados), que expresamente se relacionen con sus objetivos del programa en lo que respecta a la SSR, que también incluyan medidas para la efectividad de los mecanismos de mitigación del uso indebido de nombres de dominio.

Conclusión del SSR2: esta recomendación sigue siendo relevante, pero no es mensurable. Si bien se han tomado medidas para mitigar el uso indebido de nombres de dominio, no fue posible determinar si esto afectó la mitigación del uso indebido de dominios y, de ser así, en qué medida.

El panorama del DNS cambió desde que el Equipo de Revisión SSR1 realizó sus recomendaciones como resultado de la expansión de nuevos gTLD, en particular. Sin embargo, la recomendación de incluir las recomendaciones de SSR como una medida de éxito clave en la administración del espacio del DNS sigue siendo igual de relevante, o quizá más, hoy en día que en el año 2011.

Véase la recomendación 8 del SSR2: Permitir y demostrar la representación del interés público en las negociaciones con las partes contratadas y la recomendación 12 del SSR2: Revisar el análisis del uso indebido del DNS y las iniciativas de presentación de informes para permitir la transparencia y la revisión independiente, y la recomendación 13 del SSR2: Aumentar la transparencia y la responsabilidad en la presentación de reclamos por uso indebido para las recomendaciones de SSR2 que amplían la recomendación original del SSR1.

---

[149] Véase "Implementación de la recomendación 10 de SSR" en el informe consolidado sobre la implementación del SSR1, https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2.

[150] ICANN, 31 de julio de 2017, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf.

[151] Véase los informes "Medición de Desempeño de Cumplimiento Contractual" de la ICANN, https://features.icann.org/compliance/dashboard/report-list.

Fundamentos:

- El Equipo de Revisión SSR2 no pudo encontrar ningún documento que describiera las medidas para el éxito, incluidas mediciones para la efectividad de los mecanismos para mitigar el uso indebido de nombres de dominio, que tenga consenso de la comunidad. Esta falta de criterios mensurables también se ha notado en el informe y las recomendaciones recientes en relación con CCT.[152]
- La Especificación 11 del nuevo Acuerdo de Registro contiene obligaciones de SSR importantes que recaen sobre los registros, incluidas obligaciones de realizar análisis técnicos y mantener informes estadísticos de manera periódica para evaluar si los dominios en el TLD se utilizan para perpetrar amenazas a la seguridad, como pharming, phishing, malware y botnets. Estas obligaciones exactas han sido parte del Acuerdo de Registro de los Nuevos gTLD estándar desde que se abrieron las solicitudes en 2012. La organización de la ICANN tiene un gráfico de cumplimiento, pero mide la cantidad de reclamos y categorías.[153] Esto sigue siendo difícil de rastrear dado que sus informes están esparcidos en diversas páginas.

Recomendación 12 del SSR1

"La ICANN debería trabajar con la comunidad para identificar mejores prácticas relacionadas con la SSR y respaldar la implementación de dichas prácticas mediante contratos, acuerdos y memorandos de entendimiento, entre otros mecanismos".

Conclusión del SSR2: la recomendación 12 del SSR1 no fue implementada en su totalidad y sigue siendo particularmente relevante hoy en día. El resultado de haber definido e implementado mejores prácticas relacionadas con la SSR no fue logrado.

Véase la recomendación 8 del SSR2: Permitir y demostrar la representación del interés público en las negociaciones con las partes contratantes y la recomendación 9 del SSR2: Supervisar y exigir el cumplimiento de las recomendaciones del SSR2 que amplían la recomendación original del SSR1.

Fundamentos:

- La Especificación 11 del nuevo Acuerdo de Registro (RA) contiene obligaciones importantes relativas a la SSR que recaen en los registros. Las obligaciones contenidas en este RA son parte del Acuerdo de Registro de los Nuevos gTLD estándar desde que se abrieron las solicitudes en 2012. Sin embargo, la organización de la ICANN por lo visto no usó estas disposiciones como base para evaluar la efectividad con la que cumple las metas de la recomendación 12 del SSR1.
- El informe titulado "Metodología de Mitigación de Ataques al Sistema de Identificadores" data de febrero de 2017. Este documento establece sugerencias que aparentemente han sido generadas "*dentro de la ICANN y por expertos en seguridad de los sistemas de identificadores de toda la comunidad*".[154] Sin embargo, no queda claro qué proceso se siguió para llegar a las mejores prácticas estipuladas en el documento. No hay evidencia

[152] Informe de CCT, 9, https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

[153] Véase los Informes de Desempeño de Cumplimiento Contractual de la ICANN, https://features.icann.org/compliance y los informes de "Medición de Desempeño de Cumplimiento Contractual", https://features.icann.org/compliance/dashboard/report-list.

[154] Phifer, Lisa y David Piscitello, "Metodología de Mitigación de Ataques al Sistema de Identificadores", libro blanco de la ICANN, 13 de febrero de 2017, https://www.icann.org/en/system/files/files/identifier-system-attack-mitigation-methodology-13feb17-en.pdf.

alguna en el documento vinculado de una integración de dichas mejores prácticas en los acuerdos que celebra la organización de la ICANN. No hay evidencia de trabajo anterior a 2017 contenida en el informe.
- El informe Metodología de Mitigación de Ataques al Sistema de Identificadores describía una lista no exhaustiva de ataques contra el sistema de identificadores. Si bien ha habido algunos acuerdos, renovaciones, especificaciones y memorandos de entendimiento desde febrero de 2017, nada específicamente de ese documento se ha incluido en los contratos con las partes contratadas.
- La página Localizador de Recursos de Concientización sobre Seguridad de la ICANN no se actualiza desde 2014.[155]
- El Equipo de Revisión SSR2 no encontró evidencia alguna de que el personal informara de forma periódica a las organizaciones de apoyo y comités asesores de mejores prácticas, o los invitara a identificar otras adicionales.
- El informe del personal sobre esta recomendación del SSR1 indica que se completó el trabajo con el Comité de Política en materia de Internet del Grupo de Trabajo Anti-Phishing (APWG) sobre la publicación de recomendaciones para la protección de solicitudes web y el desarrollo de recursos para concientización de la seguridad. Había un documento de asesoramiento del APWG sobre "Qué hacer si su sitio web ha sido pirateado", pero fue elaborado antes del SSR1. Si bien hay un informe del Cuarto Simposio Mundial sobre Seguridad, Estabilidad y Flexibilidad celebrado en Puerto Rico en 2012, el sitio web de la ICANN no parece tener un conjunto de recomendaciones para protección de las solicitudes web y el desarrollo de recursos para concientización de la seguridad.[156]

Recomendación 13 del SSR1

"La ICANN debería alentar a todas las organizaciones de apoyo a desarrollar y publicar mejores prácticas relacionadas con la SSR para sus miembros".

Conclusión del SSR2: esta recomendación sigue siendo relevante, pero no fue implementada. El resultado esperado de tener un proceso periódico para las organizaciones de apoyo para publicar mejores prácticas relacionadas con la SSR para sus miembros no fue logrado.

Véase la recomendación 8 del SSR2: Permitir y demostrar la representación del interés público en las negociaciones con las partes contratantes y la recomendación 9 del SSR2: Supervisar y exigir el cumplimiento de las recomendaciones del SSR2 que amplían la recomendación original del SSR1.

Fundamentos:
- La organización de la ICANN considera trabajar en esta recomendación continua e informa que, como parte del SOP, el personal de la ICANN se pone en contacto con todas las organizaciones de apoyo y comités asesores para alentar la identificación y publicación de una página de repositorio de mejores prácticas. La organización de la ICANN informa, además, que su personal participa en diversas actividades continuas para alentar el uso global de mejores prácticas relativas a la SSR, como parte del SOP. El Equipo de Revisión SSR2 no pudo encontrar evidencia de que la organización realizó esta actividad de difusión,

[155] Localizador de Recursos de Concientización sobre Seguridad de la ICANN, actualizado por última vez el 8 de agosto de 2014, https://www.icann.org/resources/pages/security-awareness-resource-2014-12-04-en.
[156] "Seguridad, Estabilidad y Flexibilidad del DNS", Informe de la reunión del Cuarto Simposio Mundial, la ICANN y el APWG, 25 de octubre de 2012, https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf.

ni evidencia de que las organizaciones de apoyo publicaron una guía de mejores prácticas sobre SSR para sus miembros.

- El personal de la organización de la ICANN informó que no conocía ninguna medida reciente que se haya tomado para alentar a las organizaciones de apoyo y comités asesores a elaborar y publicar repositorios de mejores prácticas para la información relacionada con la SSR, e indicó que "*probablemente la información de 2012 contenida en el sitio web de ccTLD sea el ejemplo más reciente de información al respecto publicada por una organización de apoyo*".[157] Asimismo, el personal informó que solo la ccNSO publica actualmente las mejores prácticas relacionadas con la SSR para sus miembros.

Recomendación 14 del SSR1

"La ICANN debería garantizar que sus actividades de difusión y alcance relacionadas con la SSR evolucionen de manera continua a fin de que sigan siendo relevantes, oportunas y adecuadas".

Conclusión del SSR2: esta recomendación sigue siendo relevante, pero no fue implementada y, por ende, no logró su resultado esperado de mejorar la puntualidad, relevancia y adecuación de las actividades de difusión y alcance relacionadas con la SSR de la ICANN.

Véase la recomendación 18 del SSR2: Informar los debates de políticas para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- La interfaz de participación no abordó directamente la forma en que las actividades de difusión y alcance "evolucionan" para seguir siendo relevantes.[158] En cambio, la implementación se centró en informar las acciones que se realizan en un momento determinado. Dado que no se aborda el enfoque sobre actividades cambiantes, la recomendación no se implementó.

Recomendación 15 del SSR1

"La ICANN debería actuar como facilitador en la divulgación y diseminación responsables de las amenazas a la seguridad del DNS y las técnicas de mitigación".

Conclusión del SSR2: esta recomendación sigue siendo relevante y no fue implementada en su totalidad. Si bien existe un proceso "por escrito", no es posible evaluar si dicho proceso es funcional y eficaz.

Véase la recomendación 8 del SSR2: Permitir y demostrar la representación del interés público en las negociaciones con las partes contratadas y la recomendación 12 del SSR2: Revisar el análisis del uso indebido del DNS y las iniciativas de presentación de informes para permitir la transparencia y la revisión independiente, y la recomendación 13 del SSR2: Aumentar la transparencia y la responsabilidad en la presentación de reclamos por uso indebido para las recomendaciones de SSR2 que amplían la recomendación original del SSR1.

---

[157] Wiki del SSR2, Equipo de Revisión, Documentos y borradores del Equipo de Revisión, "tabla de recomendaciones del SSR1", sin fecha, 26, https://community.icann.org/pages/viewpage.action?pageId=64076120.

[158] ICANN, interfaz de participación, consultado el 13 de diciembre de 2020, https://features.icann.org/events-near-you.

Fundamentos:

- Si bien la organización de la ICANN ha implementado un proceso de divulgación de vulnerabilidades, no hay estadísticas públicas u otra información sobre la frecuencia con la que se ha invocado un proceso.
- La organización de la ICANN implementó un programa de divulgación de vulnerabilidades para los activos de la ICANN que se muestran al público.159 Cuando se informan vulnerabilidades de la infraestructura del DNS a la organización de la ICANN, la organización de la ICANN (cuando sea posible) las difunde a los terceros externos responsables. Sin embargo, es responsabilidad del tercero corregir cualquier vulnerabilidad dentro de su plataforma.
- Desde 2013, ninguno de los informes de IS-SSR contienen estadísticas o mediciones relativas a los informes de divulgación. Es imposible deducir de los materiales publicados si la metodología de informes de divulgación de vulnerabilidades se ha invocado alguna vez o si es funcional. No hay datos disponibles, ni siquiera datos anónimos, sobre la organización de la ICANN como coordinador de vulnerabilidades, ni sobre su trabajo en coordinación de emergencias y gestión de crisis relativa a la SSR.

Recomendación 16 del SSR1

"La ICANN debería continuar con sus iniciativas de difusión y alcance para ampliar la participación y los aportes de la comunidad al proceso de desarrollo del Marco de SSR. La ICANN también debería establecer un proceso para obtener aportes más sistemáticos de otros participantes del ecosistema".

Conclusión del SSR2: esta recomendación sigue siendo relevante y solo fue implementada en forma parcial. Dada la falta de evidencia de que las actividades de difusión y alcance actuales hayan generado mayor participación de la comunidad, no puede considerarse que esta recomendación logró su resultado esperado.

Véase la recomendación 8 del SSR2: Permitir y demostrar la representación del interés público en las negociaciones con las partes contratadas y la recomendación 12 del SSR2: Revisar el análisis del uso indebido del DNS y las iniciativas de presentación de informes para permitir la transparencia y la revisión independiente, la recomendación 13 del SSR2: Aumentar la transparencia y la responsabilidad en la presentación de reclamos por uso indebido y la recomendación 18 del SSR2: Informar los debates de políticas para las recomendaciones del SSR2 que amplían la recomendación original del SSR1.

Fundamentos:

- La participación continua en comunidades relacionadas ha acompañado el objetivo de "participación", pero no se pudo determinar la forma en que se incorpora información "sistemáticamente". Esta recomendación prevé más participación pública con iniciativas de SSR, incluidos marcos e informes anuales. Esta recomendación no dio como resultado cambios evidentes a la forma en que se crean el Marco de IS-SSR y los informes anuales.
- Hay actividades de difusión y alcance continuas a comunidades relacionadas con relaciones existentes con la organización de la ICANN, lo que logra el objetivo de "participación". Sin embargo, la recomendación solicita actividades de difusión y alcance a otras comunidades de SSR.

[159] ICANN, "Proceso para informar vulnerabilidades dentro de los servicios en línea de la organización de la ICANN", consultado el 13 de diciembre de 2020, https://www.icann.org/vulnerabilities.

- No existe evidencia alguna de que las actividades de difusión y alcance actuales hayan generado mayor participación de la comunidad.
- La recomendación solicita específicamente un proceso más sistemático para obtener aportes de otros participantes del ecosistema. Esto hace que el resultado final del informe de estado de la implementación parezca fuera de lugar.160
- El informe de implementación establece que el personal "respaldaría varias iniciativas de creación de capacidades por el Equipo de Seguridad".161 El Equipo de Revisión SSR2 no pudo determinar si estas iniciativas de creación de capacidades generarían una mayor participación en el desarrollo de los Marcos de IS-SSR y, de ser así, cómo generarían dicha participación, porque la organización de la ICANN ya no actualiza dichos marcos.
- El Equipo de Revisión SSR2 no pudo encontrar evidencia del registro público sobre cuáles eran las iniciativas de creación de capacidades o cuándo fueron llevadas a cabo.

Recomendación 17 del SSR1

"La ICANN debería establecer un proceso interno más estructurado para mostrar cómo las actividades y las iniciativas se relacionan con metas, objetivos y prioridades estratégicos en el Marco de SSR".

Conclusión del SSR2: esta recomendación sigue siendo relevante. Debido a la falta de indicadores rastreables, es imposible aseverar el estado de implementación a partir de los materiales públicamente disponibles. La recomendación no logró su resultado esperado, debido a que la organización de la ICANN ya no conserva el Marco de SSR.

Véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- El informe de implementación hace referencia a los entregables de la recomendación 2 del SSR1 como guía para saber cómo se implementó la recomendación 17 del SSR1. No obstante, las recomendaciones 2 y 17 del SSR1 tienen diferentes metas. La recomendación 2 del SSR1 solicita que el ámbito de competencia y las actividades relacionadas con la SSR se sometan a consulta pública periódica, mientras que la recomendación 17 del SSR1 sugiere que las iniciativas relacionadas con la SSR se relacionen con metas, objetivos y prioridades estratégicos específicos. Los entregables de la recomendación 2 del SSR1 no cumplen con los requisitos de la recomendación 17 del SSR1.
- El Informe Anual más reciente revisado por el SSR2 (año fiscal 2018) enumera dieciocho iniciativas separadas para el año fiscal y luego describe cómo dichas iniciativas se vinculan con la misión general de la Oficina del Director de Tecnologías y al plan estratégico general de la ICANN. El Plan Anual luego se vincula con los informes de actividades que describen el trabajo finalizado en un período de presentación de informes (seis meses).
- La vinculación entre el Informe Anual sobre SSR y el Plan Estratégico de la ICANN no es clara. Además, el Plan Estratégico no menciona los Informes Anuales sobre SSR y apenas menciona actividades relacionadas con la SSR. Si existe un proceso interno más estructurado para mostrar cómo las actividades e iniciativas se relacionan con metas,

[160] ICANN, Informe de implementación de la revisión de SSR, junio de 2015, https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf.
[161] Ibídem, 7.

objetivos y prioridades estratégicos en el Marco de IS-SSR, no está públicamente disponible o a disposición del Equipo de Revisión SSR2. No obstante, la sección del informe anual más reciente que identifica iniciativas anuales no intenta relacionarlas con el Plan Estratégico de la ICANN.
- Otras recomendaciones del SSR1 intentan alinear e integrar actividades relativas a SSR de la ICANN con el Plan Estratégico general. La implementación de la recomendación 17 del SSR1 está muy lejos de brindar un proceso interno estructurado y revisado.

Recomendación 18 del SSR1

"La ICANN debería llevar a cabo una revisión operativa 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".

Conclusión del SSR2: esta recomendación sigue siendo relevante. El Equipo de Revisión SSR2 no pudo encontrar ninguna evidencia de un proceso de revisión interna ni de un proceso de revisión pública que haya generado actualizaciones periódicas al Marco de IS-SSR y, por ende, no puede determinar si esta recomendación logró sus resultados esperados.

Véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:
- La recomendación 18 del SSR1 sugiere un enfoque recursivo donde la revisión de una actividad de un año anterior tenga influencia en las decisiones respecto de las iniciativas en el futuro. El Equipo de Revisión SSR2 no encontró evidencia de un proceso interno informal o no documentado, ni de una revisión operativa pública anual de la implementación del Marco de IS-SSR.

Recomendación 19 del SSR1

"La ICANN debería establecer un proceso que permita que la comunidad haga un seguimiento de la implementación del Marco de SSR. Se debería brindar información con suficiente claridad para que la comunidad pueda realizar un seguimiento de la ejecución de la ICANN de sus responsabilidades relativas a la SSR".

Conclusión del SSR2: esta recomendación sigue siendo relevante. Debido a la falta de especificidad de "suficiente claridad", esta recomendación no puede ser medida en su totalidad. Esta recomendación no logró su resultado esperado, dado que la comunidad sigue sin poder hacer un seguimiento de las actividades relacionadas con la SRR en un plazo razonable y de manera abierta y transparente.

Véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- La organización de la ICANN informa que la publicación del Marco de IS-SSR anual162 realiza un seguimiento del progreso en comparación con las actividades consignadas en el marco del año anterior. Además, los informes de gestión de proyectos, planes operativos y presupuestos realizados en forma periódica son considerados herramientas que brindan detalles sobre las actividades relativas a la SSR. No obstante, la publicación de un Marco anual de IS-SSR en el sitio web no parece servir el propósito de informar a la comunidad y permitirle realizar un seguimiento de la implementación del marco. La documentación de la implementación viene muy rezagada respecto de la implementación, por lo que no ofrece a la comunidad un modo de realizar un seguimiento de las actividades relacionadas con la SSR.
- Además, al parecer, el Equipo de Revisión SSR1 brindó un ejemplo de tener un tablero de control público para realizar el seguimiento de las actividades relacionadas con la SSR, como se realizó para implementar una de las recomendaciones del ATRT. Sin embargo, no hay ninguna evidencia de que dicho tablero de control esté disponible a la comunidad o al público para las actividades relacionadas con la SSR.

Recomendación 20 del SSR1

"La ICANN debería aumentar la transparencia de información sobre la organización y el presupuesto en relación con la implementación del Marco de SSR y el desempeño de las funciones relacionadas con la SSR".

Conclusión del SSR2: esta recomendación sigue siendo relevante y fue implementada en forma parcial. El resultado esperado de mayor transparencia en torno a los detalles relativos a la SSR en lo que respecta a la organización y al presupuesto no fue logrado.

Véase la recomendación 3 del SSR2: Mejorar la transparencia presupuestaria relacionada con la SSR para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- El proceso de planificación de la ICANN consta de tres etapas: un plan estratégico, un plan operativo para un periodo de cinco años y un plan operativo y presupuesto anual.[163] El ciclo culmina con los informes sobre progresos y logros. La fase 1, como se describe en los Informes de implementación del espacio wiki de la implementación de SSR1, ahora está implementada para brindar información pública sobre los planes, presupuestos y actividades relacionados con la SSR (como se describe en la recomendación 2 del SSR1); esto está integrado al Marco de IS-SSR de la ICANN y los informes sobre actividades y gastos relativos a la SSR.[164] La presentación periódica de informes sobre actividades relativas a la SSR amplían esta información pública.[165] La fase II está en curso para identificar mecanismos que brinden información pública más detallada sobre presupuestos y gastos relacionados con la SSR en diversos departamentos de la ICANN. Actualmente, la

[162] Archivo de documentos de IS-SSR, https://www.icann.org/ssr-document-archive.
[163] "Proceso de planificación de la ICANN", https://www.icann.org/resources/pages/governance/planning-en.
[164] Página de inicio de la implementación de Revisión SSR1, https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home.
[165] Informe de actividades de SSR del Sistema de Identificadores, https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

información pública sobre este tema para el año 2018 puede consultarse en la página wiki Recomendación 20.[166]

- Asimismo, el personal elaboró un informe posterior al evento que incluye los impactos de presupuesto y recursos relacionados con la administración de un evento.[167] A marzo de 2020, no se publicó ningún informe posterior al evento. Se puede encontrar una plantilla para una versión pública de estos informes en la página wiki Recomendación 20.
- El informe anual sobre actividades relacionadas con la SSR sí tiene lugar en los informes anuales y documentos del marco. Los documentos de presupuesto tienen partidas muy generales a las actividades relacionadas con la SSR. Esas mismas actividades no parecen estar informadas en los informes periódicos de gestión de proyectos de la ICANN. El informe de implementación menciona que la ICANN "*integrará el Marco de SSR y los informes sobre actividades y los gastos respecto de la SSR en el marco y proceso de planificación para brindar información pública sobre planes, presupuestos y actividades relacionados con la SSR*".[168] Sin embargo, como se señala para la recomendación 19 del SSR1, el sistema de gestión de carteras de proyectos y el tablero de control de proyectos de KPI tienen muy poca información que la comunidad pueda usar para realizar un seguimiento de los esfuerzos relativos a la SSR.
- El presupuesto aprobado para el año fiscal 2018 tiene tres áreas de carteras de proyectos relacionadas con la SSR: evolución de los identificadores; seguridad, estabilidad y flexibilidad de los identificadores de Internet; y reputación técnica. Sólo las primeras dos (evolución de identificadores y SSR de identificadores de Internet) tiene presupuestos dedicados al nivel de la cartera; no se brindan detalles de estos presupuestos. El informe de implementación del personal también menciona que la ICANN "*identificará mecanismos que brinden información pública más detallada sobre los presupuestos y los gastos relacionados con la SSR en diversos departamentos de la ICANN*", lo que sugiere que se prevé más trabajo en este aspecto de la implementación.

Recomendación 21 del SSR1

"La ICANN debería establecer un proceso interno más estructurado para mostrar cómo las decisiones organizativas y presupuestarias se relacionan con el marco de SSR, incluido el análisis subyacente de costo-beneficio".

Conclusión del SSR2: esta recomendación sigue siendo relevante y fue implementada en forma parcial. No logró el resultado esperado de un proceso abierto y transparente respecto de las decisiones presupuestarias relacionadas con la SSR.

Véase la recomendación 3 del SSR2: Mejorar la transparencia presupuestaria relacionada con la SSR para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- En el informe de implementación del personal, hay tres resultados mencionados:

[166] Implementación de la Revisión SSR1, recomendación 20, actualizada por última vez del 18 de septiembre de 2018, https://community.icann.org/display/SSR/Rec+%2320.

[167] Informe de actividades de SSR del Sistema de Identificadores, https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

[168] Véase las actualizaciones del informe de implementación del SSR1 respecto de la recomendación 20, https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2.

- Integración del Marco de IS-SSR e informes en el marco y proceso de planificación para brindar información pública sobre planes, presupuestos y actividades relacionados con la SSR.
- Identificación de mecanismos que brinden información pública más detallada sobre presupuestos y gastos relacionados con la SSR en diversos departamentos de la ICANN.
- Informes de exploración posteriores al evento que incluyan los impactos de presupuesto y recursos relacionados con la administración del evento.

- El informe del personal menciona específicamente una plantilla de informes para publicar información relacionada con los presupuestos y los recursos que se ven afectados por eventos de seguridad.[169] El informe del personal sugiere que este se publicará en forma anual, cada año fiscal, a partir del año fiscal 2018. Un análisis de las páginas relacionadas con la SSR en el sitio web de la ICANN indica que no se publicó ningún informe. El informe anual sobre actividades relacionadas con la SSR sí tiene lugar en los informes anuales y documentos del marco. El documento de presupuesto tiene partidas muy generales para las actividades relacionadas con la SSR. Sin embargo, esas mismas actividades no parecen estar informadas en los informes periódicos de gestión de proyectos de la ICANN. Esta observación es la misma que en las conclusiones del SSR1 para la recomendación 20 del SSR1. Además, los informes sobre los impactos de los eventos de SSR en el presupuesto y los recursos aparentemente nunca se realizaron, y la plantilla para respaldar esos informes no parece estar disponible para revisión o comentario público.
- El proceso de planificación de la ICANN garantiza que las actividades planificadas y presupuestadas, incluidas aquellas relacionadas con la SSR, son identificadas por objetivos específicos. No ha habido un plan para solicitar comentarios públicos sobre la plantilla utilizada para publicar información pública más detallada sobre los presupuestos y gastos relacionados con la SSR. Al parecer, la plantilla se ha reemplazado por el informe anual correspondiente al año fiscal.

Recomendación 22 del SSR1

"La organización de la ICANN debería publicar, supervisar y actualizar la documentación sobre los recursos presupuestarios y organizacionales necesarios para administrar cuestiones relativas a SSR en conjunto con la introducción de nuevos gTLD".

Conclusión del SSR2: esta recomendación sigue siendo relevante y fue implementada en forma parcial. La implementación no logró el resultado esperado en su totalidad.

Véase la recomendación 3 del SSR2: Mejorar la transparencia presupuestaria relacionada con la SSR para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- La información pública sobre presupuestos y gastos relacionados con la SSR en diversos departamentos de la ICANN se publicó para el año fiscal 2018 y está disponible aquí: https://community.icann.org/x/DqNYAw. Este informe se actualiza anualmente y abarca los costos directos resultantes de las actividades requeridas para desempeñar las funciones de SSR, los costos directos de recursos compartidos y los costos de las funciones de apoyo asignadas a la SSR. Este informe no brinda un desglose de fondos, recursos u otras actividades relacionadas con el Programa de Nuevos gTLD.

[169] Implementación de la revisión SSR1, recomendación 20, https://community.icann.org/display/SSR/Rec+%2320.

- La organización de la ICANN también ha explorado mecanismos que brindan información pública más detallada sobre presupuestos y gastos relacionados con la SSR en diversos departamentos de la ICANN. Sin embargo, una plantilla para esa información pública no manifiesta actividades o presupuestos de SSR relacionados con el Programa de Nuevos gTLD.
- Resulta evidente que la organización y el presupuesto para cuestiones de SSR relacionadas con el equipo de nuevos gTLD se proporcionaron mediante el equipo de seguridad, pero también se reflejaron en el presupuesto y la organización para el Programa de Nuevos gTLD (por ejemplo, Panel de Estabilidad del Sistema de Nombres de Dominio. EBERO, otros pasos de proceso, etc.). Al parecer, el resultado deseado de la implementación de esta recomendación era mejorar la cantidad y claridad de la información respecto de la organización y el presupuesto para implementar el Marco de IS-SSR y desempeñar funciones relativas a la SSR relacionadas con el Programa de Nuevos gTLD.
- En el Archivo de documentos de IS-SSR, no hay ningún documento que sea específico para el Programa de Nuevos gTLD. En el Marco del 30 de septiembre de 2016, los gTLD son mencionados dos veces, una vez en el Módulo A como una tendencia en el ecosistema de Internet y la segunda vez en el Módulo B como parte del Plan Estratégico general de la ICANN. En el Marco de SSR correspondiente al año fiscal 2014, publicado en marzo de 2013, el Programa de Nuevos gTLD es mencionado nuevamente como una “tendencia”, y como un impulsor de políticas para la GNSO. Las únicas menciones restantes del Programa de Nuevos gTLD se encuentran en la sección que informa sobre la implementación de las recomendaciones del SSR1.

Recomendación 23 del SSR1

“La ICANN debe brindar los recursos adecuados para los Grupos de Trabajo y Comités Asesores relacionados con la SSR, de acuerdo con las exigencias que se les imponen. La ICANN también debe garantizar que las decisiones de los grupos de trabajo y comités asesores se alcancen de manera objetiva y libres de toda presión externa o interna”.

Conclusión del SSR2: esta recomendación sigue siendo relevante y fue implementada en forma parcial. El resultado esperado era permitir que los grupos de trabajo y comités asesores cumpliesen sus mandatos de manera objetiva y libre de toda presión externa o interna, y no es mensurable.

Véase la recomendación 3 del SSR2: Mejorar la transparencia presupuestaria relacionada con la SSR para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- La organización de la ICANN ofrece personal de apoyo técnico de la ICANN al SSAC y RSSAC para ayudarlos a redactar documentos. El presupuesto de la organización de la ICANN incluye algunos fondos para brindar apoyo al SSAC y al RSSAC para realizar reuniones (específicamente, gastos de viajes, alojamiento y comida); la organización de la ICANN le señaló al Equipo de Revisión SSR2 el presupuesto de 2015 como ejemplo.[170] Los fondos de apoyo nunca se vincularon a ningún desempeño, resultado o evaluación de contenido formal, ni fueron condicionados por estos. La ICANN considera que esto permite una adecuada independencia. En la práctica, no resulta claro cómo las prioridades de trabajo del RSSAC o del SSAC son determinadas o evaluadas por la ICANN o la

[170] ICANN, “Plan Operativo y Presupuesto adoptado para el año fiscal 2015”, 1 de diciembre de 2014, 77-78, https://www.icann.org/en/system/files/files/adopted-opplan-budget-fy15-01dec14-en.pdf.

comunidad, lo que crea una brecha en la responsabilidad, además de impedir evaluar si tienen recursos "de acuerdo con las exigencias que se les imponen". El informe original del SSR1 incluyó el siguiente texto asociado con esta recomendación:
"En debates con el SSAC, resultó evidente que, en ocasiones, sentía presión de entregar una respuesta a un problema específico dentro de un plazo muy ajustado. Esto generaba un período más breve para evaluar la cuestión y recomendaciones más orientadas como resultado. Claramente, habrá ocasiones, al observar riesgos inmediatos, que se exige un plazo para el trabajo de investigación. Esto es inevitable. No obstante, sería prudente, para garantizar dicho trabajo con planificación adecuada, que se les otorgase al SSAC y al RSSAC tanto tiempo como sea posible para brindar trabajo de investigación y conclusiones de alta calidad".

Esta observación se hace eco de las circunstancias e inquietudes durante los últimos años, en especial, en el contexto del traspaso de la KSK en octubre de 2018, cuando el SSAC tuvo que lidiar con responder a solicitudes de asesoramiento en plazos breves con datos/investigación inadecuados disponibles para informar el debate.[171] La fracción del presupuesto de la ICANN destinada al SSAC es probablemente inadecuada, debido a las muchas cuestiones prevalecientes y emergentes relacionadas con la SSR, y las expectativas de que el SSAC ofrezca asesoramiento que requiera investigación o síntesis de investigaciones anteriores. Además, la estructura actual del SSAC no es compatible con el "trabajo de investigación de alta calidad", dado que se compone por un grupo de "voluntarios" en su mayoría de la industria y son subsidiados por su empleador por el tiempo que participan, y, por ende, no están "libres de presión externa".

- La falta de mediciones y supervisión de éxito o fracaso del Programa de Nuevos gTLD indica que este enfoque de múltiples partes interesadas no está "libre de presión externa". Es imposible concluir, mediante las mediciones del informe del CCT-RT sobre el uso indebido del DNS en nuevos gTLD, que el Programa de Nuevos gTLD ha sido exitoso desde el punto de vista de CCT. Dicha investigación recae dentro de los roles y responsabilidades del Equipo de Seguridad de la ICANN (véase la recomendación 24 del SSR1). La ICANN no realizó ni financió este tipo de ejercicio, probablemente debido a que prevalecieron presiones externas frente a este tipo de actividad de investigación de SSR.
- El documento de procedimientos operativos del SSAC no menciona nada sobre manejar presiones externas e internas, salvo la sección 2.1.2, Abstenciones y discrepancias, lo que implica que cada miembro, y el mismo comité, autoadministra los conflictos de interés y todas las deliberaciones son confidenciales por razones de seguridad.[172] Lo mismo parece aplicarse para el RSSAC y el RZERC, pero en estos dos casos, los comités están diseñados de manera tal que cada persona representa una parte interesada.
- Constantemente, partes interesadas importantes carecen de estos comités asesores relacionados con la SSR (por ejemplo, víctimas de uso indebido, investigadores del sector académico, organismos de aplicación de la ley, responsables de formulación de políticas).

Recomendación 24 del SSR1

"La ICANN debe definir con claridad la carta orgánica, los roles y las responsabilidades del Equipo de la Oficina del Director de Seguridad".

[171] ICANN, "El primer traspaso de la KSK de la zona raíz se llevó a cabo con éxito", anuncios de la ICANN, 15 de octubre de 2018, https://www.icann.org/news/announcement-2018-10-15-en.
[172] Comité Asesor de Seguridad y Estabilidad de la ICANN, "Procedimientos operativos del SSAC, versión 5.1", 27 de febrero de 2019, 10, https://www.icann.org/en/system/files/files/operational-procedures-27feb18-en.pdf.

Conclusión del SSR2: la recomendación sigue siendo relevante y fue implementada en forma parcial. No logró el resultado esperado de tener una carta orgánica clara, roles definidos y responsabilidades definidas para el Equipo de la Oficina del Director de Seguridad.

Véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- Desde 2018, no hay Oficina del Director de Seguridad. Sin embargo, el equipo de SSR de la OCTO (Oficina del Director de Tecnologías) trabaja en cuestiones de SSR relacionadas con la ICANN centradas en asuntos externos, el CIO y el equipo trabajan en cuestiones de seguridad centradas en asuntos internos y el equipo de investigación de la OCTO observa futuros riesgos relacionados con la SSR y oportunidades dentro del ámbito de competencia y alcance limitado de la ICANN.173 La página web de este equipo describe la misión del equipo en términos generales y brinda un enlace a una página de "actividades" relacionadas con la SSR.174 No hay texto que haga referencia a "carta orgánica", "roles" o "responsabilidades" de este equipo. El Equipo SSR2 supone que las actividades enumeradas en esta página constituyen lo que la ICANN pretende como roles y responsabilidades relacionados con la SSR de la OCTO:
  - Participar activamente con las comunidades dedicadas a la seguridad pública, la seguridad y operaciones a fin de recopilar y procesar datos de inteligencia que indiquen amenazas (inminentes) a las operaciones de servicios de registración de dominios o del DNS ("ecosistema del DNS").
  - Facilitar o participar con estas mismas comunidades en actividades para la preparación ante amenazas a fin de protegerse contra amenazas al ecosistema del DNS, o mitigar dichas amenazas.
  - Realizar estudios o analizar datos para comprender mejor el estado y el bienestar del ecosistema del DNS.
  - Coordinar informes de la divulgación de vulnerabilidades del DNS (https://www.icann.org/vulnerability-disclosure.pdf).
  - Colaborar con expertos en la materia para crear capacidades entre las comunidades de ccTLD y las dedicadas a la seguridad pública en asuntos relevantes al ecosistema del DNS, incluidos las DNSSEC, el uso indebido o el uso incorrecto de operaciones o infraestructuras del DNS.
  - Brindar asistencia a las actividades de gestión de riesgos del ecosistema del DNS.
  - Con el Equipo de Participación Global de Partes Interesadas de la ICANN, participar en un esfuerzo global de múltiples partes interesadas para mejorar la ciberseguridad y mitigar los ciberdelitos.
- La OCTO no parece haber producido mucho en cuanto al análisis de la SSR que está disponible al público. La Iniciativa de Datos Abiertos, los informes de DAAR y el proyecto de mediciones de Internet parecen ser proyectos con datos asociados que son internos de la organización de la ICANN. No resulta claro cuán útil ha sido este trabajo hasta el momento para la comunidad en general que la organización de la ICANN pretende servir.

[173] OCTO de la ICANN, "Oficina del Director de Tecnologías (OCTO)", consultado el 27 de diciembre de 2019, https://www.icann.org/octo..

[174] OCTO de la ICANN, "Seguridad, Estabilidad y Flexibilidad del Sistema de Identificadores de Internet", consultado el 27 de diciembre de 2019, https://www.icann.org/octo-ssr.

Recomendación 25 del SSR1

"La ICANN debería implementar mecanismos para identificar riesgos a corto y mediano plazo y factores estratégicos en su Marco de Gestión de Riesgos".

Conclusión del SSR2: esta recomendación sigue siendo relevante y fue implementada en forma parcial. La implementación no logró el resultado esperado en su totalidad.

Véase la recomendación 4 del SSR2: Mejorar los procesos y procedimientos de gestión de riesgos para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- La Junta Directiva de la ICANN aprobó un Marco de Gestión de Riesgos en el año 2013, y recibió aportes de la comunidad durante ICANN50 e ICANN51. La organización de la ICANN mantiene un tablero de control de Gestión de Riesgo Empresarial (ERM) que enumera los riesgos a ser monitoreados y abordados, y sigue un marco de gestión de riesgo empresarial. No obstante, si bien hay implementado un mecanismo, falta claridad en cuanto a cómo la identificación de riesgos se incorpora en los procesos y políticas relevantes concernientes a la SSR.

Recomendación 26 del SSR1

"La ICANN debería priorizar la compleción oportuna de un Marco de Gestión de Riesgos".

Conclusión del SSR2: esta recomendación sigue siendo relevante y fue implementada en forma parcial. Dado que el término "oportuna" no brinda ninguna especificidad respecto de lo que se pretendía o era aceptable, no se puede evaluar si se logró el resultado esperado.

Véase la recomendación 4 del SSR2: Mejorar los procesos y procedimientos de gestión de riesgos para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- La Junta Directiva de la ICANN aprobó un Marco de Gestión de Riesgos en el año 2013,175 y recibió aportes de la comunidad durante ICANN50 e ICANN51. Se aborda una respuesta más detallada para esta recomendación en la evaluación de la recomendación 27.

Recomendación 27 del SSR1

"El Marco de Gestión de Riesgos de la ICANN debería ser integral dentro del alcance de su ámbito de competencia y sus misiones limitadas concernientes a la SSR".

Conclusión del SSR2: esta recomendación sigue siendo relevante. Ante la ausencia de una definición de "integral" por parte del SSR1 o de mediciones para su evaluación, el Equipo de Revisión SSR2 no pudo evaluar si esta recomendación fue implementada en su totalidad. La organización de la ICANN no logró el resultado esperado de brindar información integral y fácil de encontrar sobre el marco de gestión de riesgos usado por la ICANN.

[175] ICANN, "Informe del Marco para la Gestión de Riesgos del DNS", modificado por última vez el 4 de octubre de 2013, https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en.

Véase la recomendación 4 del SSR2: Mejorar los procesos y procedimientos de gestión de riesgos para la recomendación del SSR2 que amplía la recomendación original del SSR1.

Fundamentos:

- El Equipo de Revisión SSR2 analizó si la recomendación 27 del SSR1 fue implementada en basa a las referencias formuladas por el personal durante varios intercambios de preguntas y respuestas en relación con la recomendación 25 del SSR1. No obstante, el Equipo de Revisión SSR2 concluyó que esta recomendación, si bien se correlaciona con las recomendaciones 25 y 26 del SSR1, es distinta porque solicita que el marco sea "integral". El Equipo de Revisión SSR2 opinó que, si la recomendación 27 del SSR1 fue implementada en consonancia con lo que pretendía el Equipo de Revisión SSR1, habría abordado las mismas inquietudes que las recomendaciones 25 y 26 del SSR1 probablemente pretendían abordar.
- El SSR1 no brindó ninguna definición respecto a qué elementos del marco serían "integrales" o cómo se debería evaluar este tema. Durante la revisión, se señaló que esta recomendación habría sido implementada por personal de la ICANN que ya no forma parte de la organización de la ICANN. En este respecto, la memoria institucional y un registro histórico completo de cómo evaluó la "integralidad" del Marco de Gestión de Riesgos no estaban disponibles.
- La información públicamente disponible respecto de la forma en que la gestión de riesgos se aborda fue encontrada en ubicaciones fragmentadas. A modo de ejemplo, el personal indicó que el Comité para la Gestión de Riesgos de la Junta estaba conformado por el equipo ejecutivo de la organización de la ICANN, el cual brinda supervisión. Además, que hay coordinadores de enlace de riesgos relacionados con las funciones que son miembros del personal y que representan cada función para implementar el marco de riesgos, y todo el personal de la organización que tiene los riesgos inherentes en sus actividades, se centra en las cuestiones de gestión de riesgos; esto demuestra que la función de riesgos de la organización de la ICANN no ha estado centralizada y coordinada de manera estratégica.

Recomendación 28 del SSR1

"La ICANN debería seguir participando activamente en la detección y mitigación de amenazas, y participando en esfuerzos para distribuir la información de amenazas e incidentes".

Conclusión del SSR2: esta recomendación sigue siendo relevante y no fue implementada en su totalidad. Si bien la organización de la ICANN ha participado en diversos grupos para ayudar a detectar, mitigar y compartir información sobre amenazas e incidentes, el resultado esperado de hacer que esta información esté disponible fuera de estos grupos nombrados no fue logrado.

Véase la recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos, la recomendación 8 del SSR2: Permitir y demostrar la representación del interés público en las negociaciones con las partes contratadas y la recomendación 12 del SSR2: Revisar el análisis del uso indebido del DNS y las iniciativas de presentación de informes para permitir la transparencia y la revisión independiente, y la recomendación 13 del SSR2: Aumentar la transparencia y la responsabilidad en la presentación de reclamos por uso indebido para las recomendaciones de SSR2 que amplían la recomendación original del SSR1.

Fundamentos:

- El Equipo de Revisión SSR2 no encontró datos públicamente disponibles que demostrasen que la organización de la ICANN participa en la detección y mitigación de amenazas. La organización de la ICANN, cuando es factible, difunde las vulnerabilidades informadas a terceros externos responsables. No obstante, es responsabilidad del tercero actuar en consecuencia de la información de amenazas e incidentes difundida.
- No hay evidencia pública de que la organización de la ICANN realice detección continua de amenazas ni de que nadie esté a cargo de esta función. Sin embargo, la comunidad de la ICANN tiene varios grupos (abiertos y cerrados) que realizan activamente detección de amenazas, incluidos el SSAC, el RSSAC, el TLDOPS, el Grupo de Trabajo sobre respuesta ante incidentes de la ccNSO y el PSWG. El Equipo de SSR de la OCTO coordina con estos grupos.

Apéndice E: Datos de investigación sobre informes de tendencias de uso indebido del DNS

Entre algunos ejemplos vinculados al DNS en diversos grados se incluyen:

- Malware: desde 2016 hasta 2018, la cantidad de URL únicos reconocidos como maliciosos por software antivirus se multiplicó más del doble a 554,159,6213[176], y los ataques de malware a dispositivos móviles casi se duplicó de 2017 a 2018 hasta superar los 116 millones[177].
- Fraude de certificado digital: el APWG informa que los suplantadores de identidad (*phishers*) usan cada vez más certificados digitales para hacer que los ataques parezcan legítimos y para derrotar las advertencias de detección de fraude de los navegadores.[178] Debido a la eliminación de acceso de la ICANN al WHOIS, la administración del certificado de SSL ya no tiene acceso a los datos de registración de nombres de dominio y no puede usar los registros de titularidad de nombres de dominio que la organización de la ICANN se encarga de coordinar para validar la titularidad de nombres de dominio. PhishLabs determinó que la mitad de todos los sitios de phishing usan cifrado SSL, lo que puede engañar a los usuarios a pensar que un sitio es seguro de usar, por ejemplo, por medio del símbolo de candado verde que aparece en la barra de direcciones del navegador cuando está activado el cifrado SSL. Parte del aumento proviene de los suplantadores de identidad que agregan cifrado HTTP a sus sitios de phishing, una técnica que hace que una función de seguridad se vuelva en contra de las víctimas.[179]
- Phishing: el APWG informó que los suplantadores de identidad registran nombres de dominio directamente para perpetrar fraude y que los métodos de ataques de phishing se han vuelto más efectivos y más difíciles de detectar.

[176] AMR, "Boletín de Seguridad de Kaspersky 2018: estadísticas", 4 de diciembre de 2018, https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/.
[177] Victor Chebyshev, "Evolución del malware en dispositivos móviles", 5 de marzo de 2019, https://securelist.com/mobile-malware-evolution-2018/89689/.
[178] APWG, "Informe de Tendencias de Actividades de Phishing del APWG, tercer trimestre de 2018", 11 de diciembre de 2018, https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf.
[179] Elliot Volkman, "El 49 % de los sitios de phishing ahora usan HTTPS", blog de PhishLabs, 6 de diciembre de 2018, https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https.

> "*Los suplantadores de identidad usan cada vez más las redirecciones a páginas web como un modo de esconder sus sitios de phishing para no ser detectados. Cuando las víctimas hacen clic en los enlaces contenidos en los correos electrónicos de phishing. las redirecciones llevan al usuario a un recorrido involuntario a través de otros sitios antes de llegar al sitio de phishing. Y, una vez que la víctima presenta sus credenciales, es posible que más redirecciones lleven a la víctima a otro dominio".*[180]

- Correo electrónico corporativo comprometido: el Centro de Quejas de Crímenes en Internet del FBI de EE. UU. informó un aumento del 136 % en pérdidas expuestas globales identificadas de 2016 a 2018 resultantes de correo electrónico corporativo comprometido (BEC), que afectaban a los 50 estados de EE. UU. y a 150 países de todo el mundo. De octubre de 2013 a mayo de 2018, el FBI documentó un crecimiento de varios miles de millones de dólares en BEC, lo que generalmente implica el registro fraudulento de nombres de dominio que son engañosamente similares a uno de las partes afectadas.[181]
- Estafas: ScamWatch de la Comisión Australiana de Competencia y Consumidores (ACCC) informó casi el doble en pérdidas de estafas en aproximadamente los últimos tres años, lo que ascendió a 11,8 millones de dólares australianos en pérdidas en el año 2019.[182] Los nombres de dominio usados para perpetrar estafas en línea infringen, la mayoría de las veces, marcas o nombres comerciales. Los estafadores registran estos nombres con poco o ningún control sobre los volúmenes de nombres similares que el estafador puede registrar y acceso limitado a la información que los investigadores pueden usar para identificar a los delincuentes.
- Botnets: en 2017, Spamhaus DBL enumeró 50 000 nombres de dominio con controladores botnet registrados y configurados por ciberdelincuentes con el único propósito de alojar un controlador botnet. Más del 25 % de estos nombres de dominio botnet registrados han sido registrados por un solo registrador, Namecheap.[183] En 2018, Spamhaus enumeró 103 503 nombres de dominio con controladores botnet, un incremento del 106 %. Namecheap siguió siendo el registrador con más usos indebidos, con una aumento del 220 % en nombres de dominio con controladores botnet.[184]
- Spam: spam es la infraestructura de entrega preferida para phishing, malware y otras amenazas relacionadas con el DNS. El volumen promedio diario de spam fue de 416 040 millones a agosto de 2019.[185]

> *"Independientemente de cuánto cambie el panorama de las amenazas, el correo electrónico malicioso y el spam siguen siendo herramientas vitales para los enemigos a*

[180] Informe de Tendencias de Actividades de Phishing del APWG, https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf.
[181] "Correo electrónico corporativo comprometido: la estafa de 12 mil millones de dólares", anuncio del servicio público de la Agencia Federal de Investigaciones, 12 de julio de 2018, https://www.ic3.gov/media/2018/180712.aspx.
[182] ScamWatch, Comisión Australiana de Competencia y Consumidores, https://www.scamwatch.gov.au/about-scamwatch/scam-statistics.
[183] "Informe de amenazas de botnets de Spamhaus de 2017", Spamhaus Malware Labs, modificado por última vez el 8 de enero de 2018, https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017.
[184] "Informe de amenazas de botnets de Spamhaus de 2019", Spamhaus Malware Labs, sin fecha, https://www.spamhaustech.com/botnet-threat-report-2019/
[185] "Datos de correo electrónico y spam", Cisco Talos Intelligence Group, https://www.talosintelligence.com/reputation_center/email_rep.

fin de distribuir malware porque llevan las amenazas directamente al extremo. Mediante la aplicación de la combinación correcta de técnicas de ingeniería social, como phishing, y adjuntos y enlaces maliciosos, los adversarios solo necesitan sentarse a esperar que usuarios ingenuos activen sus ataques".[186]

- Ataques de DDoS: los ataques de Denegación de Servicio Distribuido (DDoS) aumentaron un 40 % desde mediados de 2017 hasta mediados de 2018.[187] El tamaño máximo de ataques de DDoS aumentó a nivel mundial un 174 % en el primer semestre de 2018 con respecto al mismo período de 2017 y el ataque más grande nunca antes registrado (1.7 Tbps) golpeó a un importante proveedor de servicios de Norteamérica en febrero de 2018.[188] Dado que todo, desde empresas a organismos gubernamentales hasta infraestructuras físicas de trabajos públicos, depende de los servicios ininterrumpidos relacionados con el DNS, los ataques no mitigados de DDoS causan cada vez más perjuicio. Los ataques de DDoS también se han vuelto más complejos y los ataques multivectoriales son ahora los más comúnmente empleados. Verisign informó que el 52 % de sus ataques registrados en el segundo trimestre de 2018 fueron ataques multivectoriales.[189] Además, la Internet de las cosas (IoT) es una creciente preocupación para los ataques de DDoS porque estos dispositivos conectados son objetivos fáciles, y continúan proliferando. La cantidad de dispositivos conectados fue de 27 000 millones en 2017 y se prevé que alcance los 125 000 millones para el año 2020.[190]

[186] "Informe anual sobre ciberseguridad de Cisco de 2018", Cisco Systems, febrero de 2018, https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.
[187] "Informe de tendencias de DDoS del primer semestre de 2018", Corero Network Security, sin fecha, https://info.corero.com/report-2018-half-year-ddos-trends-report-download.html.
[188] Kevin Whalen, "Entrando a la era del terabit: Preparación para ataques de DDoS más grandes", 5 de septiembre de 2018, https://www.netscout.com/blog/entering-terabit-era-get-ready-bigger-ddos-attacks.
[189] "Informe de tendencias de DDoS del segundo trimestre de 2018: el 52 % de los ataques empleó tipos de ataques múltiples", blog de Verisign, modificado por última vez el 27 de septiembre de 2018, https://blog.verisign.com/security/ddos-protection/q2-2018-ddos-trends-report-52-percent-of-attacks-employed-multiple-attack-types/.
[190] John English, "Preparando la red para cumplir con las expectativas de IoT", blog de NETSCOUT, modificado por última vez el 28 de febrero de 2018, https://www.netscout.com/blog/getting-network-ready-meet-iot-expectations.

Apéndice F: Datos de investigación sobre criptografía

Criptografía de curva elíptica

La criptografía de curva elíptica (ECC) ofrece una alternativa a la criptografía de clave pública de RSA que se usa actualmente para las DNSSEC. La técnica se basa en una teoría de curva elíptica que se puede usar para crear claves criptográficas más rápidas, más pequeñas y más eficientes.[191]

La declaración de prácticas de DNSSEC (DPS) de la KSK de la zona raíz brinda pautas sobre la longitud y el traspaso de las claves. No obstante, la DPS no dice nada sobre los procedimientos para cambios al algoritmo de firma digital. Pautas recientes de la Agencia Nacional de Seguridad de EE. UU. recomiendan usar 3072 bits para RSA. El algoritmo de seguridad digital de curva Edwards (EdDSA) parece ofrecer una mejor alternativa que las claves de RSA muy grandes.[192]

Criptografía poscuántica

La mayoría de la gente no había escuchado sobre cómputo cuántico hace una década, pero ha captado la imaginación del público en los años recientes. Parte de este interés proviene de la potencia informática única de una computadora cuántica. La Academia Nacional de Ciencias de EE. UU. recientemente publicó un informe sobre “Cómputo cuántico: progreso y previsiones”, con la conclusión general de que ahora es el momento de comenzar a prepararse para un futuro con seguridad cuántica.[193]

DigiCert ha estimado que demora varios cuatrillones de años fabricar una clave de RSA de 9048 bits mediante la tecnología informática clásica.[194] En el futuro, si se inventa una computadora cuántica a gran escala, puede descodificar la misma clave mucho más rápidamente, quizá en solo unos meses. Aún existen muchos desafíos técnicos que se deben superar antes de que sea posible crear una computadora cuántica que amenace a RSA y ECC, los dos algoritmos criptográficos asimétricos principales usados para proteger la Internet.

El avance hacia una computadora cuántica a gran escala debe rastrear la tasa de escalamiento del número de bits cuánticos físicos o “cúbits” que las computadoras tienen y los índices de

---

[191] Véase las siguientes RFC para obtener más información sobre posibles algoritmos nuevos para las firmas con DNSSEC: Hoffman, P. y W. Wijngaards, "Algoritmo de firma digital con curvas elípticas (DSA) para las DNSSEC", RFC 6605, DOI 10.17487/RFC6605, abril de 2012, <https://www.rfc-editor.org/info/rfc6605>, Sury, O. y R. Edmonds, "Algoritmo de seguridad digital de curva Edwards (EdDSA) para las DNSSEC", RFC 8080, DOI 10.17487/RFC8080, febrero de 2017, <https://www.rfc-editor.org/info/rfc8080>, y Wouters, P. y O. Sury, "Requisitos para la implementación de algoritmos y guía de uso para las DNSSEC", RFC 8624, DOI 10.17487/RFC8624, junio de 2019, <https://www.rfc-editor.org/info/rfc8624>.

[192] Wouters y Sury, RFC 8624, https://www.rfc-editor.org/info/rfc8624.

[193] Academias Nacionales de Ciencias, Ingeniería y Medicina. 2019. Cómputo cuántico: progreso y previsiones. Washington, DC: Prensa de las Academias Nacionales. https://doi.org/10.17226/25196.

[194] Hollebeek, Timothy, “DigiCert sobre sistema cuántico: Informe de la Academia Nacional de Ciencias”, blog de DigiCert, 9 de enero de 2019, https://www.digicert.com/blog/digicert-on-quantum-national-academy-of-sciences-report/.

errores. Los índices de errores son importantes porque afectan considerablemente la cantidad de cúbits físicos que se requieren para hacer un cúbit lógico. Los cúbits físicos son los sistemas cuánticos individuales que representan un cero o un uno; no obstante, los cúbits físicos son propensos a errores a través de interacciones inevitables con su entorno, incluso a temperaturas que se acerca a cero absoluto. Muchos cúbits físicos se pueden combinar en un único cúbit lógico y los cúbits adicionales se usan para detectar y corregir estos errores. Los investigadores aún deben elaborar incluso un único cúbit lógico, aunque se está avanzando rápidamente para lograr esa meta. Una vez disponibles los cúbits lógicos, el rastreo de la cantidad de cúbits lógicos será la medición a rastrear.

Los grupos de estándares de la industria también se están preparando para un futuro poscuántico. La actividad más conocida es el proyecto de criptografía poscuántica NIST, que trabaja con investigadores de todo el mundo para desarrollar nuevos elementos básicos criptográficos que no sean susceptibles de ser atacados por computadoras cuánticas.[195] Se puede esperar que el proyecto demore varios años más antes de que los algoritmos resultantes estén listos para su normalización.

Mientras tanto, los investigadores acuerdan que las firmas basadas en hash son seguras para la tecnología poscuántica. El Equipo de Investigación sobre Internet (IRTF) ha especificado estos algoritmos de firmas en su Grupo de Investigación del Foro de Criptografía (CFRG), mediante el uso de claves públicas y privadas pequeñas con un bajo costo informático.[196] Sin embargo, las firmas son bastante grandes y una clave privada solo puede producir una cantidad finita de firmas. Si bien estos algoritmos están disponibles hoy en día, estas últimas dos propiedades hacen que las firmas basadas en hash no sean aconsejables en el entorno de las DNSSEC.

[195] Instituto Nacional de Normas y Tecnología (NIST), Laboratorio de Tecnología de la Información, Recursos de Seguridad Informática, Centro, “Criptografía poscuántica”, elaborado el 3 de enero de 2017, actualizado el 23 de noviembre de 2020, https://csrc.nist.gov/projects/post-quantum-cryptography.
[196] IRTF, Grupo de Investigación del Foro de Criptografía, https://irtf.org/cfrg.

Apéndice G: Mapeo de las recomendaciones del SSR2 al Plan Estratégico 2021 a 2025 de la ICANN y los Estatutos de la ICANN

Estatutos relevantes de la ICANN

Sección 1.2.(a)(i) y 1.2 (a) (ii) de los Estatutos y sección 27.1(c)(i)(B) respecto de preservar y mejorar "la administración del DNS y la estabilidad operativa, la confiabilidad, la seguridad, la interoperabilidad mundial, la flexibilidad y la apertura del DNS e Internet".

Sección 3.6(a) de los Estatutos: asistir a la Junta Directiva en considerar e informar respecto de los "posibles efectos significativos, si los hubiere, de su decisión sobre el interés público global, incluido un debate de los impactos significativos a la seguridad, estabilidad y flexibilidad del DNS".

Sección 12.2(b) y 12.2(c) de los Estatutos: trabajar estrechamente con el Comité Asesor de Seguridad y Estabilidad y el Comité Asesor del Sistema de Servidores Raíz en particular, y garantizar que la Junta y la organización de la ICANN estén ejecutando completamente respecto de su asesoramiento aceptado.

Anexo G-1 de los Estatutos: los temas, cuestiones, políticas, procedimientos y principios referidos en la sección 1.1(a)(i) con respecto a registros y registradores de gTLD son los siguientes: "temas para los cuales se hace razonablemente necesario contar con una resolución uniforme o coordinada a fin de facilitar la interoperabilidad, la seguridad o la estabilidad de Internet, los servicios de registrador, los servicios de registro o el DNS" y "la seguridad y estabilidad de la base de datos de registros para un TLD".

Metas y objetivos relevantes del Plan Estratégico

Del Plan Estratégico de la ICANN para los años fiscales 2021 a 2025.[197]

1. fortalecer la seguridad del Sistema de Nombres de Dominio y el Sistema de Servidores Raíz del DNS.

1.1 Mejorar la responsabilidad común de respaldar la seguridad y estabilidad del DNS mediante el fortalecimiento de la coordinación de este sistema en asociación con partes interesadas relevantes.
1.2 Fortalecer la gobernanza de las operaciones de los servidores raíz del DNS en coordinación con los operadores de los servidores raíz del DNS.
1.3 Identificar y mitigar las amenazas a la seguridad del DNS mediante una mayor interacción con proveedores de hardware, software y servicios relevantes.
1.4 Aumentar la solidez de los servicios y procesos de distribución y firma de claves de la zona raíz del DNS.

[197] Plan Estratégico de la ICANN para los años fiscales 2021 a 2025, https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf.

2. Objetivo estratégico: mejorar la eficacia del modelo de gobernanza de múltiples partes interesadas de la ICANN.

2.1. Fortalecer el proceso ascendente de toma de decisiones de múltiples partes interesadas de la ICANN y garantizar que se realice el trabajo y se elaboren políticas de manera eficaz y oportuna.
2.2 Apoyar y desarrollar una participación activa, informada y efectiva de las partes interesadas.
2.3 Sostener y mejorar la apertura, inclusión, responsabilidad y transparencia.

3. Objetivo estratégico: evolucionar los sistemas de identificadores únicos en coordinación y colaboración con partes relevantes para continuar atendiendo a las necesidades de la base global de usuarios de Internet.

3.1 Fomentar la competencia, la elección de los consumidores y la innovación en el espacio de Internet al aumentar la concientización e incentivar la preparación para la aceptación universal, la implementación de los IDN y el IPv6.
3.2 Mejorar la evaluación de las nuevas tecnologías que afectan la seguridad, estabilidad y flexibilidad de los sistemas de identificadores únicos de Internet, junto con la capacidad de respuesta ante dichas tecnologías, mediante una mayor interacción con las partes relevantes.
3.3 Continuar desempeñando y mejorando las funciones de la IANA mediante la excelencia operativa.
3.4 Respaldar la evolución continua de los sistemas de identificadores únicos de Internet mediante una nueva ronda de gTLD financiada, gestionada y evaluada en materia de riesgos de manera responsable, y alineada a los procesos de la ICANN.

4. Objetivo estratégico: abordar las cuestiones geopolíticas que afectan la misión de la ICANN para garantizar una Internet única e interoperable a nivel mundial.

4.1 Identificar y abordar tanto desafíos como oportunidades globales dentro de su ámbito de incumbencia mediante un mayor desarrollo de sistemas de alerta temprana, tales como los informes de la organización de la ICANN sobre novedades legislativas y normativas.
4.2 Continuar generando alianzas dentro y fuera del ecosistema de Internet para aumentar la concientización sobre la misión de la ICANN y sus procesos de desarrollo de políticas, como también interactuar con partes interesadas globales al respecto.

5. Objetivo estratégico: garantizar la sostenibilidad financiera de la ICANN a largo plazo.

5.1 Implementar un plan financiero quinquenal que respalde el plan operativo quinquenal.
5.2 Desarrollar proyecciones de fondos confiables y predecibles.
5.3 Gestionar operaciones y costos para optimizar la eficacia y eficiencia de las actividades de la ICANN.
5.4 Garantizar que el nivel de las reservas de la ICANN se fije, alcance y mantenga continuamente en consonancia con la complejidad y los riesgos del entorno de la ICANN.

N.°	Recomendación	Meta y objetivo estratégicos
1	Completar la implementación de todas las recomendaciones relevantes del SSR1.	Objetivos estratégicos 1, 2 y 3
2	Recomendación 2 del SSR2: Crear un cargo de alta gerencia responsable de la seguridad estratégica y táctica y de la gestión de riesgos	Objetivos estratégicos 1, 3 y 4
3	Recomendación 3 del SSR2: Mejorar la transparencia presupuestaria relacionada con la SSR	Objetivos estratégicos 1, 2, 3 y 5; y metas estratégicas 2.1 y 3.4
4	Recomendación 4 del SSR2: Mejorar los procesos y procedimientos de gestión de riesgos	Objetivos estratégicos 1, 2, 3, 4 y 5
5	Recomendación 5 del SSR2: Cumplir con los sistemas de gestión de seguridad de la información apropiados y las certificaciones de seguridad	Objetivo estratégico 1
6	Recomendación 6 del SSR2: Divulgación y transparencia sobre vulnerabilidades de SSR	Objetivos estratégicos 1, 2, 3 y 4; y metas estratégicas 1.1, 1.2, 1.3 y 4.1
7	Recomendación 7 del SSR2: Mejorar la continuidad de las operaciones y los procesos y procedimientos de recuperación ante desastres	Objetivos estratégicos 1, 3 y 4; y también metas estratégicas 1.1, 1.4 y 3.3
8	Recomendación 8 del SSR2: Permitir y demostrar la representación del interés público en las negociaciones con las partes contratadas	Objetivos estratégicos 1 y 3; y metas estratégicas 1.1, 1.2, 1.3 y 1.4
9	Recomendación 9 del SSR2: Supervisar y exigir el cumplimiento	Objetivos estratégicos 1, 2 y 3; y meta estratégica 2.1
10	Recomendación 10 del SSR2: Aclarar las definiciones de los términos relacionados con el uso indebido	Objetivo estratégico 1
11	Recomendación 11 del SSR2: Resolver los problemas de acceso a los datos del CZDS	Objetivo estratégico 3 y meta estratégica 3.2
12	Recomendación 12 del SSR2: Revisar el análisis del uso indebido del DNS y las iniciativas de presentación de informes para permitir la transparencia y la revisión independiente	Objetivos estratégicos 1, 2, 3, 4 y 5
13	Recomendación 13 del SSR2: Aumentar la transparencia y la responsabilidad en la presentación de reclamos por uso indebido	Objetivos estratégicos 1 y 3; y meta estratégica 2.1

14	Recomendación 14 del SSR2: Crear una especificación temporaria para las mejoras de seguridad basadas en pruebas	Objetivo estratégico 1 y meta estratégica 1.1
15	Recomendación 15 del SSR2: Iniciar un EPDP para las mejoras de seguridad basadas en pruebas	Objetivo estratégico 1 y meta estratégica 1.1
16	Recomendación 16 del SSR2: Requisitos de privacidad y RDS	Objetivos estratégicos 1, 3 y 5
17	Recomendación 17 del SSR2: Medición de colisiones de nombres	Objetivos estratégicos 1, 3 y 4; y meta estratégica 3.4
18	Recomendación 18 del SSR2: Informar los debates de políticas	Objetivos estratégicos 1, 3 y 4; y meta estratégica 3.2
19	Recomendación 19 del SSR2: Desarrollo completo de la serie de pruebas de regresión del DNS	Objetivo estratégico 1; y metas estratégicas 1.2, 1.3 y 1.4
20	Recomendación 20 del SSR2: Procedimientos formales para el traspaso de claves	Objetivos estratégicos 1, 2 y 4; y meta estratégica 1.4
21	Recomendación 21 del SSR2: Mejorar la seguridad de las comunicaciones con los operadores de TLD	Objetivo estratégico 1 y meta estratégica 3.3
22	Recomendación 22 del SSR2: Medidas de servicio	Objetivos estratégicos 1, 2, 3, 4 y 5; y metas estratégicas 1.1, 1.2, 2.1, 3.2, 3.4 y 4.1
23	Recomendación 23 del SSR2: Traspaso de algoritmos	Objetivos estratégicos 1 y 3
24	Recomendación 24 del SSR2: Mejorar la transparencia y las pruebas de extremo a extremo del proceso EBERO	Objetivo estratégico 1 y meta estratégica 1.2

Apéndice H: Análisis de comentarios públicos

El Equipo de Revisión SSR2 creó una hoja de cálculo para registrar su respuesta a los comentarios públicos y los cambios resultantes de los comentarios públicos. El archivo está disponible en la página Documentos y borradores del Equipo de Revisión del espacio wiki del SSR2 o se puede descargar directamente desde los enlaces siguientes.

Excel:
https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/155191048/Public%20Comment%20Feedback%20-%20March%202020.xlsx

PDF:
https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/155191042/Public%20Comment%20Feedback%20-%20March%202020.pdf

Apéndice I: Hojas informativas

La organización de la ICANN publica hojas informativas y de gastos de forma trimestral, así como actualizaciones mensuales de participación e hitos. Estos documentos aportan transparencia y responsabilidad a la comunidad sobre cómo se están utilizando los recursos y el tiempo del equipo de revisión.

La hoja informativa captura la asistencia de los miembros del equipo de revisión, los costos asociados con los servicios profesionales y los viajes para asistir a las reuniones presenciales, los hitos y la participación.

Las definiciones son las siguientes:

Servicios profesionales: presupuesto aprobado para que el equipo de revisión lo utilice para los servicios de expertos independientes, como se indica en la sección 4.6(a)(iv) de los Estatutos. Los equipos de revisión también podrán solicitar y seleccionar a expertos independientes para que presten el asesoramiento que solicite el equipo de revisión. La ICANN pagará los honorarios y gastos razonables de dichos expertos por cada revisión contemplada en esta sección 4.6 en la medida en que dichos honorarios y costos sean coherentes con el presupuesto asignado para dicha revisión. Las directrices sobre cómo los equipos de revisión deben considerar y trabajar con el asesoramiento de expertos independientes se especifican en los estándares operativos.

Viajes: importe aprobado para viajes del equipo de revisión para reuniones presenciales. Los ejemplos de gastos de viaje incluyen, aunque no taxativamente, cargos por pasajes aéreos, gastos de hotel, reembolso de viáticos, costos de reuniones en el lugar de la reunión, apoyo audiovisual/técnico y catering. Estos gastos incluyen apoyo para viajes de la organización de la ICANN y el Equipo de Revisión.

Apoyo de la organización de la ICANN: importe aprobado en el presupuesto para que la organización de la ICANN contrate servicios externos para apoyar el trabajo del equipo de revisión.

Gastado a la fecha: los importes incluyen los estados financieros trimestrales desde el inicio del trabajo por parte del equipo de revisión hasta el final del trimestre más reciente.

Servicios comprometidos:
1. Viajes: gastos estimados para las reuniones presenciales aprobadas.
2. Servicios profesionales: servicios incluidos de los contratos firmados para ser prestados o facturados.

Estos son generalmente para servicios de apoyo que prestan contratistas y no están relacionados con los empleados. Total

Gastado y comprometido a la fecha: esta es la suma de los montos “Gastado a la fecha” y “Servicios
comprometidos” hasta el fin del trimestre más reciente. El importe de Servicios comprometidos no incluye los importes de Gastado a la fecha. Presupuesto restante: Esta es la diferencia entre los importes de "Presupuesto aprobado" y "Total gastado y comprometido a la fecha".

Los archivos de las hojas informativas pueden consultarse en: https://community.icann.org/x/S7zRAw.