Revisión de Seguridad, Estabilidad y Flexibilidad (SSR2)

Resumen ejecutivo y reseña

Resumen Ejecutivo

El presente informe es una versión preliminar de las conclusiones y recomendaciones del Equipo de Revisión de la SSR2. Hay varios asuntos sobre los que el SSR2-RT continúa iterando, pero en general el equipo de revisión considera que el informe está en un punto en el que los comentarios públicos proporcionarían un aporte útil y fundamental para incorporar al informe final.

En particular, el SSR2-RT apreciaría recibir comentarios sobre:

- las conclusiones y recomendaciones;
- qué parte de la ICANN (por ejemplo, la Junta Directiva, la organización de la ICANN o la comunidad de la ICANN) debería abordar cada recomendación;
- qué criterios de medición serían los más apropiados para hacer que cada recomendación sea medible y evitar al mismo tiempo la sobreingeniería de la solución;
- qué prioridad debería darse a cada recomendación;
- cualquier informe adicional u otro material que crea que el equipo de revisión debería considerar antes de completar sus recomendaciones (véase el espacio wiki de la SSR2,[1] que incluye "materiales de referencia", "materiales informativos" y "preguntas y respuestas" para el material que el equipo ha revisado).

Según el proceso establecido de revisión de la comunidad, la comunidad también tendrá oportunidades adicionales para proporcionar aportes al informe final de la SSR2.

Reseña

Introducción

[Se agregará en el informe final.]

Información de referencia

[Se agregará en el informe final.]

Objetivos

Conforme a los Estatutos[2] de la organización 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")'.

Específicamente:

[1] Espacio wiki del Equipo de Revisión de la SSR2 de la ICANN, https://community.icann.org/display/SSR/SSR2+Review.

[2] "Estatutos de la Corporación para la Asignación de Nombres y Números en Internet", ICANN, según modificaciones del 28 de noviembre de 2019, https://www.icann.org/resources/pages/governance/bylaws-en.

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

A. *cuestiones de seguridad, estabilidad operativa y flexibilidad, tanto físicas como de red, relacionadas con la coordinación del sistema de identificadores únicos de Internet;*
B. *conformidad con el marco adecuado de planificación de contingencias de seguridad para el sistema de identificadores únicos de Internet;*
C. *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.*

iii. El Equipo de Revisión de SSR también evaluará hasta qué punto 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.

Recomendaciones de la SSR2 - Resumen

El Equipo de Revisión de la SSR2 ha alineado todas las recomendaciones de la SSR2 con el Plan Estratégico[3] de la ICANN para 2021-2025 y sus metas y objetivos. El informe especifica los objetivos pertinentes que las recomendaciones individuales respaldan; el SSR2-RT eliminó de este informe cualquier recomendación que no se alineaba claramente con el plan estratégico.

Todas las recomendaciones del SSR2-RT se alinean con el plan estratégico de la organización de la ICANN y, por lo tanto, se consideran de alta prioridad.

N.°	Recomendación	Titular	Prioridad

3 "Plan Estratégico de la ICANN para los años fiscales 2021 a 2025", ICANN, última actualización: 29 de marzo de 2019, https://www.icann.org/public-comments/strategic-plan-2018-12-20-en.

1	**Completar la implementación de todas las recomendaciones relevantes de la SSR1**		Alta
2	**Recomendación 9 de la SSR1 - Sistemas de gestión de seguridad de la información y certificaciones de seguridad** 2.1. La organización de la ICANN debería establecer una hoja de ruta de sus auditorías de seguridad estándar de la industria y de las actividades de certificación que se están llevando a cabo, incluidas las fechas de los hitos para la obtención de cada certificación y señalar las áreas de mejora continua. 2.2. La organización de la ICANN debería elaborar un plan de certificaciones y requisitos de capacitación para las funciones de la organización, realizar un seguimiento de los índices de finalización, proporcionar una justificación de sus elecciones y documentar cómo se ajustan las certificaciones a las estrategias de gestión de seguridad y riesgos de la organización. 2.3. La organización de la ICANN también debería razonar sus elecciones y demostrar cómo se ajustan a sus estrategias de seguridad y gestión de riesgos. 2.4. La organización de la ICANN debería implementar un Sistema de Gestión de Seguridad de la Información y someterse a una auditoría externa. 2.5. Para poder obtener los beneficios de un régimen de certificaciones y auditorías, la organización de la ICANN debería ser auditada y certificada por un tercero conforme a los estándares de seguridad de la industria y debería evaluar las opciones de certificación con estándares internacionales comúnmente aceptados (por ejemplo, ITIL, ISO 27001, SSAE-18) para sus responsabilidades operativas.		Alta
3	**Recomendaciones 12, 15 y 16 de la SSR1 - Estrategia y marco de RSS, criterios de medición y divulgación de vulnerabilidades** 3.1. La organización de la ICANN debería abordar las cuestiones de seguridad de forma clara y pública (teniendo en cuenta la seguridad operativa, por ejemplo, tras una moratoria establecida y la anonimización de la información, si es necesario) y promover las mejores prácticas de seguridad entre todas las partes contratadas. 3.2. La organización de la ICANN también debería capturar las mejores prácticas relacionadas con la SSR en un documento de consenso, establecer objetivos claros, medibles y trazables, y luego implementar las prácticas en contratos, acuerdos y memorandos de entendimiento. 3.3. La organización de la ICANN debería implementar informes de divulgación coordinada de vulnerabilidades. Las divulgaciones y la información sobre los temas relacionados con la SSR deberían ser comunicadas de forma rápida a las partes relevantes y de confianza (por ejemplo, los afectados o quienes deben solucionar el tema en cuestión), como en los casos de incumplimientos de cualquier parte contratada y en		Alta

	los casos de vulnerabilidades clave detectadas e informadas a la organización de la ICANN. 3.4. La organización de la ICANN debería establecer un plan de comunicación claro para los informes a la comunidad y elaborar informes regulares (al menos de forma anual) y oportunos que contengan mediciones anónimas del proceso de divulgación de vulnerabilidades. Estos comunicados deberían contener una divulgación responsable según lo definido por el proceso acordado por la comunidad e incluir mediciones anonimizadas.		
4	**Recomendación 20 y 22 de la SSR1 - Transparencia presupuestaria y presupuestos de SSR en los nuevos gTLD** 4.1. Cuando sea posible (contractualmente) y razonable en términos de esfuerzo (es decir, más del 10 % de la actividad descrita en la partida presupuestaria), la ICANN debería ser más transparente con el presupuesto para las partes de la organización de la ICANN relacionadas con la implementación del Marco de Seguridad, Estabilidad y Flexibilidad de los Sistemas de Identificadores (IS-SSR) y el desempeño de funciones relacionadas con la SSR, incluidas aquellas asociadas con la introducción de nuevos gTLD.		Media
5	**Recomendación 27 de la SSR1 - Gestión de riesgos** 5.1. El Marco de gestión de riesgos de la ICANN debería estar centralizado y coordinado de forma estratégica. 5.2. La organización de la ICANN debería articular de forma clara su marco de gestión de riesgos y alinear estratégicamente el marco con los requisitos y objetivos de la organización, y describir las medidas de éxito pertinentes y cómo la organización de la ICANN evaluará estas medidas. 5.3. La ICANN debería poner a disposición de la comunidad de forma centralizada la información relativa a la gestión de riesgos. Esta información debería actualizarse de forma periódica para reflejar el panorama actual de amenazas (al menos una vez por año).		Alta
6	**Crear un cargo responsable para la seguridad estratégica y táctica y la gestión de riesgos** 6.1. La organización de la ICANN debería crear un cargo responsable para la seguridad estratégica y táctica y la gestión de riesgos en todo el dominio de seguridad interna de la organización, así como en el sistema de identificación global externo. 6.2. La organización de la ICANN debería contratar a una persona debidamente cualificada para ese puesto y asignar un presupuesto específico suficiente para ejecutar las funciones de este rol. 6.3. Este puesto debería gestionar la función de seguridad de la organización de la ICANN y supervisar las interacciones del		Alta

	personal en todas las áreas relevantes que afectan a la seguridad. 6.4. El cargo también debería proporcionar informes periódicos a la Junta Directiva de la ICANN y a la comunidad. 6.5. Este cargo actuaría como un explorador y solucionador de problemas que elaboraría estrategias y ejecutaría programas multifacéticos para lograr mejoras sustanciales. 6.6. Además, este rol debería participar en todas las negociaciones contractuales relevantes para la seguridad (por ejemplo, cadenas de suministro de hardware y software y acuerdos de nivel de servicio asociados) que lleve a cabo la organización de la ICANN y aprobar todos los términos contractuales relacionados con la seguridad.		
7	**Continuar con el desarrollo de un marco de seguridad de gestión de riesgos** 7.1. La organización de la ICANN debería articular claramente su Marco de Seguridad de Gestión de Riesgos y asegurarse de que se alinea estratégicamente con los requisitos y objetivos de la organización. 7.2. La organización de la ICANN debería describir las medidas de éxito relevantes y cómo se deben evaluar estas medidas. El SSR2-RT describió el fundamento de esta recomendación en detalle en los comentarios adicionales con respecto a la Recomendación 9 de la SSR1 (ver 'Recomendación 9 de la SSR1 - Sistemas de gestión de seguridad de la información y certificaciones de seguridad' mencionada anteriormente en este informe). 7.3. La organización de la ICANN debería: 7.3.1. Adoptar e implementar la norma ISO 31000 "Gestión de riesgos" y validar y certificar su implementación con auditorías independientes apropiadas.[4] Los esfuerzos de gestión de riesgos deberían utilizarse en los planes y disposiciones de continuidad de operaciones y de recuperación ante desastres. 7.3.2. Actualizar de forma periódica un registro de riesgos de seguridad y utilizar ese registro para priorizar y guiar las actividades de la organización de la ICANN. La organización de la ICANN debería informar sobre las actualizaciones de su metodología y las actualizaciones del registro de riesgos de seguridad. Las conclusiones deberían utilizarse en la continuidad de operaciones y la recuperación ante desastres y en el Sistema de Gestión de Seguridad de la Información (ISMS). 7.3.3. Nombrar o designar una persona dedicada y responsable a cargo de la gestión de riesgos de seguridad que estará bajo las órdenes del rol de Seguridad de alta gerencia como se describe en la recomendación "Puesto de seguridad de alta gerencia".		Alta

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

8	**Establecer un Plan de Continuidad de Operaciones basado en la norma ISO 22301** 8.1. La organización de la ICANN debería establecer un Plan de Continuidad de Operaciones para todos los sistemas que sean propiedad o estén bajo el ámbito de la organización de la ICANN, basado en la norma ISO 22301 "Gestión de la Continuidad de Operaciones".[5] 8.2. La ICANN debería identificar la importancia de plazos funcionales y aceptables para la continuidad de operaciones y la recuperación ante desastres en base a la urgencia de restaurar la plena funcionalidad. 8.3. Para las operaciones de Identificadores Técnicos Públicos (PTI) (funciones de la IANA, incluidos todos los sistemas relevantes que contribuyen a la Seguridad y Estabilidad del DNS y también a la Gestión de la Zona Raíz), la organización de la ICANN debería desarrollar un enfoque compartido para la continuidad del servicio en estrecha cooperación con el Comité Asesor del Sistema de Servidores Raíz (RSSAC) y los operadores de servidores raíz. 8.4. La organización de la ICANN debería publicar evidencia (por ejemplo, un resumen) de sus Planes y Disposiciones de Continuidad de Operaciones. Se debería contratar a un auditor externo para verificar los aspectos de cumplimiento de la implementación de los planes de continuidad de operaciones resultantes.		Alta
9	**Asegurar que el Plan de Recuperación ante Desastres sea apropiado, funcional y documentado correctamente** 9.1. La organización de la ICANN debería garantizar que el Plan de Recuperación ante Desastres para las operaciones de PTI (funciones de la IANA) incluya todos los sistemas relevantes que contribuyen a la seguridad y estabilidad del DNS y que también incluya la Gestión de la Zona Raíz y esté en consonancia con las *Directrices sobre la preparación de las tecnologías de la información y la comunicación para la continuidad de las operaciones* de la norma ISO 27031. La organización de la ICANN debería desarrollar este plan en estrecha colaboración con el RSSAC y los operadores de servidor raíz. 9.2. La organización de la ICANN también debería establecer un Plan de Recuperación ante Desastres para todos los sistemas que son propiedad o están bajo el ámbito de la organización de la ICANN, también en consonancia con las *Directrices sobre la preparación de las tecnologías de la información y la comunicación para la continuidad de las operaciones* de la norma ISO 27031. 9.3. La organización de la ICANN debería tener un plan de recuperación ante desastres que se desarrolle en un plazo de		Alta

[5] "ISO 22301:2019 Seguridad y flexibilidad — Sistemas de gestión de la continuidad de operaciones — Requisitos", https://www.iso.org/standard/75106.html.

	doce meses a partir de la adopción de estas recomendaciones por parte de la Junta Directiva de la ICANN en torno al establecimiento de al menos un tercer sitio para la recuperación ante desastres (además de Los Ángeles y Culpeper), específicamente fuera de Estados Unidos y sus territorios y la región de América del Norte, incluido un plan de implementación. 9.4. La organización de la ICANN debería publicar un resumen de sus planes y disposiciones generales de recuperación ante desastres. La organización de la ICANN debería contratar a un auditor externo para verificar los aspectos de cumplimiento de la implementación de estos planes de recuperación ante desastres.		
10	**Mejorar el marco para definir y medir el cumplimiento de registradores y registros** 10.1. Establecer un marco de métricas de desempeño para guiar el nivel de cumplimiento por parte de los registradores y registros para las obligaciones de WHOIS (incluida la inexactitud), así como otros elementos que afectan el uso indebido, la seguridad y la capacidad de recuperación, como se describe en la Revisión RDS/WHOIS2 y la Revisión de CCT.[6,7] 10.2. Asignar una partida presupuestaria específica para un equipo de funcionarios de cumplimiento con la tarea de llevar a cabo activamente o encargar el trabajo de pruebas/evaluaciones de gestión del desempeño de las métricas acordadas de SLA. 10.3. Enmendar la cláusula de renovación de SLA de 'renovación automática' a una renovación cíclica de cuatro años que incluya una cláusula de revisión (este período de revisión consideraría el nivel de cumplimiento de las métricas de desempeño por parte del Registrador y el Registro y recomendaría la inclusión de requisitos para fortalecer la seguridad y la flexibilidad cuando el incumplimiento fuera evidente). 10.4. Además, la Junta Directiva de la ICANN debería asumir la responsabilidad de cerrar el EPDP[8] y aprobar e implementar una política de WHOIS en el año posterior a la publicación de este informe.		Alta

6 Equipo de Revisión de RDS-WHOIS de la ICANN, "Revisión de Servicios de Directorio de Registración (RDS)-WHOIS2: Informe Final", 3 de septiembre de 2019, https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf.

7 "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.

8 Organización de Apoyo para Nombres Genéricos de la ICANN, "Proceso Expeditivo de Desarrollo de Políticas (EPDP) de la GNSO sobre la Especificación Temporaria para los Datos de Registración de los gTLD para consideración de la Junta Directiva de la ICANN", 1 de mayo de 2019, https://www.icann.org/public-comments/epdp-recs-2019-03-04-en.

11	**Dirigir los esfuerzos para desarrollar las definiciones en torno al uso indebido y permitir la presentación de informes en contra de esas definiciones** 11.1. La Junta Directiva de la ICANN debería impulsar los esfuerzos que minimicen el lenguaje ambiguo y lleguen a un acuerdo universalmente aceptable sobre el uso indebido, SSR y las amenazas a la seguridad en sus contratos con las partes contratadas y en los planes de implementación. 11.2. La organización de la ICANN y la Junta Directiva deberían implementar sin demora los compromisos relevantes para la SSR (junto con las recomendaciones de las Revisiones de CCT y RDS/WHOIS2) en base a las definiciones actuales de uso indebido, aprobadas por la comunidad[9]. 11.3. La Junta Directiva de la ICANN, en paralelo, debería alentar la atención de la comunidad a la evolución de la definición (y aplicación) de uso indebido del DNS y adoptar el término adicional y la definición externa en evolución de "amenaza a la seguridad", un término utilizado por el proyecto de Informes de Actividades de Uso Indebido de Dominios (DAAR) de la ICANN, y el GAC (en su Comunicado de Pekín[10] y para la Especificación 11[11]), y que se aborda en convenciones internacionales como la Convención sobre ciberdelito y sus "Notas Explicativas"[12] relacionadas, para utilizarlas junto con la definición de Uso indebido del DNS de la organización de la ICANN[13]. 11.4. La Junta Directiva de la ICANN debería encomendar al SSAC y al PSWG que trabajen con expertos en ciberdelito y uso indebido para elaborar la definición de Uso indebido del DNS, teniendo en cuenta los procesos y las definiciones que figuran en la Convención sobre ciberdelito.		Alta
12	**Crear mecanismos legales y adecuados de acceso a los datos de WHOIS**		Alta

9 El informe de CCT define tanto el Uso indebido del DNS como el Abuso a la seguridad del DNS y cita con aprobación en la pág. 8, nota 11, definiciones contenidas en un documento del personal de la ICANN titulado "Medidas de protección contra el uso indebido del DNS, 18 de junio de 2016". El Grupo de Trabajo sobre Políticas de Uso Indebido de Registraciones (RAP) de la comunidad en 2010 'desarrolló una definición consensuada de uso indebido' que dice lo siguiente: “El uso indebido es 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”. (Esta definición se cita con aprobación en la página 88, nota 287 del informe final de CCT)

10 Comité Asesor Gubernamental de la ICANN, “Asesoramiento del GAC: Comunicado pronunciado en Pekín, ICANN46”, última modificación: 11 de abril de 2013, https://gac.icann.org/contentMigrated/icann46-beijing-communique.

11 ICANN, “Acuerdo de Registro”, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm.

12 Consejo de Europa, “Convención sobre ciberdelito”, ETS N.º 185, p. 7, 23 de noviembre de 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

13 Véase la nota 50

	12.1. La Junta Directiva de la ICANN debería crear mecanismos legales y adecuados de acceso a los datos de WHOIS por parte de las partes autorizadas, como organismos de cumplimiento de la ley. 12.2. La Junta Directiva de la ICANN debería asumir la responsabilidad y asegurar que la organización de la ICANN concluya de inmediato la implementación de la Especificación Temporaria para los Datos de Registración de los gTLD.		
13	**Mejorar la exhaustividad y utilidad del programa de Informes de Actividades de Uso Indebido de Dominios** 13.1. La Junta Directiva de la ICANN y la organización de la ICANN deberían trabajar con entidades dentro y fuera de la comunidad de la ICANN que estén mitigando el uso indebido para mejorar la exhaustividad y la utilidad del programa de DAAR, con el fin de mejorar tanto la medición como los informes de uso indebido de dominios. 13.1.1. La organización de la ICANN debería publicar informes DAAR que identifiquen los registros y registradores cuyos dominios contribuyan en mayor medida al uso indebido de acuerdo con la metodología DAAR. 13.1.2. La organización de la ICANN debería poner a disposición los datos de origen para DAAR a través de la Iniciativa de Datos Abiertos de la ICANN y priorizar los elementos "daar" y "daar-resumido" del Inventario de Activos de Datos de ODI[14] para el acceso inmediato de la comunidad. 13.1.3. La organización de la ICANN debería publicar informes que incluyan formatos legibles por computadoras de los datos, además de los datos gráficos de los informes actuales. 13.1.4. La organización de la ICANN debería proporcionar asistencia a la Junta Directiva y a todas las unidades constitutivas, grupos de partes interesadas y comités asesores en la interpretación de DAAR, incluida la asistencia en la identificación de actividades en materia de política y asesoramiento que mejoren la prevención y mitigación del uso indebido de los nombres de dominio.		Alta
14	**Permitir un análisis cuantitativo riguroso de la relación entre los pagos de las registraciones de dominios y la evidencia de amenazas a la seguridad y uso indebido** 14.1. La organización de la ICANN debería recopilar, analizar y publicar datos de precios para permitir la realización de más estudios independientes y el seguimiento de la relación entre los precios y el uso indebido.		Alta

[14] Ver: https://www.icann.org/en/system/files/files/odi-data-asset-inventory-spreadsheet-11jun18-en.csv según publicación de la Oficina del Director de Tecnologías, disponible aquí: https://www.icann.org/public-comments/odi-datasets-metadata-2018-06-11-en.

15	**Mejorar los contratos con los Registradores y Registros para incentivar la mitigación del uso indebido del DNS** 15.1. La organización de la ICANN debería hacer obligatorios los requisitos de SSR en la renovación del contrato o del acuerdo base en los acuerdos con partes contratadas, incluidos los Acuerdos de Registro (base e individual) y el RAA. Estos requisitos contractuales deberían incluir disposiciones que establezcan umbrales de uso indebido (por ejemplo, el 3 % de todas las registraciones) que activen automáticamente consultas de cumplimiento, con un umbral más alto (por ejemplo, el 10 % de todas las registraciones) en el que la organización de la ICANN considere que los registradores y los registros se encuentran en incumplimiento de sus acuerdos. La Revisión de CCT también recomendó este enfoque.[15] 15.2. La organización de la ICANN debería introducir una cláusula contractual que apoye la rescisión del contrato en el caso de "un patrón y práctica" de uso indebido (como en la sección 5.5.2.4 "PLAZO, RESCISIÓN Y RESOLUCIÓN DE DISPUTAS" del Acuerdo de Acreditación de Registradores de 2013)[16]. 15.3. Con el fin de apoyar la revisión de estos cambios en los contratos, la organización de la ICANN debería: 15.3.1. Asegurar el acceso a los datos de registración a las partes con fines legítimos a través de obligaciones contractuales y con mecanismos de cumplimiento rigurosos. 15.3.2. Establecer y exigir el cumplimiento de los requisitos uniformes del Servicio de Datos de Zona Centralizado para asegurar el acceso continuo para fines de investigación de SSR. 15.3.3. Atraer y colaborar con los ccTLD y la ccNSO para ayudar a abordar el uso indebido del DNS y las amenazas a la seguridad en los ccTLD. 15.3.4. La Junta Directiva, la comunidad y la organización de la ICANN deberían trabajar con la ccNSO para avanzar en el seguimiento y la presentación de informes de datos, evaluar el uso indebido del DNS y las amenazas a la seguridad en los ccTLD, y desarrollar un plan de la ccNSO para ayudar a los ccTLD a mitigar aún más el uso indebido del DNS y las amenazas a la seguridad. 15.3.5. Instaurar de inmediato un requisito para los servicios de RDAP de las partes contratadas para registrar en lista blanca el espacio de direcciones de la organización de la ICANN y establecer un proceso de investigación de otras entidades que los servicios de RDAP de las partes contratadas incluirán en la lista blanca para el acceso no limitado. 15.4. A más largo plazo, la Junta Directiva de la ICANN debería solicitar que la GNSO inicie el proceso para adoptar nuevas políticas y acuerdos con las partes contratadas que mejoren de manera mensurable la mitigación del uso indebido del DNS y		Alta

[15] Ver recomendaciones 14, 15 y 16 en el documento "Competencia, Confianza y Elección de los Consumidores: Informe Final", https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

[16] "Acuerdo de Acreditación de Registradores de 2013", ICANN, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

	las amenazas a la seguridad, incluidos los cambios en el RDAP y en la información de los registratarios, incentivos para las partes contratadas para la mitigación del uso indebido/amenazas a la seguridad, establecimiento de un marco de medición del desempeño e institucionalización de la capacitación y las certificaciones para las partes contratadas y las principales partes interesadas.		
16	**Crear incentivos de precios para las partes contratadas para mitigar el uso indebido y las amenazas a la seguridad** 16.1. La organización de la ICANN debería incentivar la mitigación del uso indebido y de las amenazas a la seguridad mediante los siguientes cambios en los contratos: 16.1.1. Las partes contratadas que tengan carteras con menos de un porcentaje específico (por ejemplo, el 1 %) de nombres de dominio abusivos (según lo identifiquen los proveedores comerciales o el DAAR) deberían recibir una reducción de las tarifas (por ejemplo, una reducción de las tarifas actuales o un aumento de la tarifa actual por transacción de nombre de dominio y ofrecer un descuento a un Registrador). 16.1.2. Los registradores deberían recibir una reducción de las tarifas por cada nombre de dominio registrado a un registratario verificado hasta un umbral apropiado. 16.1.3. Renunciar a las tarifas de RSEP cuando las presentaciones de RSEP indiquen claramente cómo la parte contratada tiene la intención de mitigar el uso indebido del DNS, y que cualquier RSEP del Registro reciba una aprobación previa si permite que un campo de EPP a nivel de Registro designe esos nombres de dominio como bajo la gestión de un Registratario verificado. 16.1.4. Reembolsar las tarifas que se cobran a los registradores y registros por los dominios identificados como de uso indebido y amenazas a la seguridad que se retiran dentro de un período apropiado después de la registración (por ejemplo, 30 días después de que se registra el dominio). 16.2. Dado que todas las partes (la organización de la ICANN, las partes contratadas y otras partes interesadas críticas como Registros, Registradores, Proveedores de Servicios de Privacidad/Proxy y Proveedores de Servicios de Internet) deben entender cómo medir, rastrear, detectar e identificar con precisión el uso indebido del DNS, la organización de la ICANN debería institucionalizar la capacitación y las certificaciones de todas las partes en las áreas identificadas por DAAR y otras fuentes sobre los métodos comunes de uso indebido **[agregar cita]** y cómo establecer los esfuerzos de mitigación apropiados. La capacitación debería incluir lo siguiente como punto de partida: seguimiento automático de la cantidad de reclamos y del tratamiento de los mismos; informes públicos trimestrales/anuales sobre reclamos y acciones; y análisis.		Alta
17	**Establecer un portal central de informes de uso indebido**		Alta

	17.1. La organización de la ICANN debería establecer y mantener un portal central de reclamos de uso indebido del DNS que dirija automáticamente todos los informes de uso indebido a las partes pertinentes. El sistema actuaría exclusivamente como una entrada, solo con un flujo ascendente del resumen y los metadatos. El uso del sistema debería ser obligatorio para todos los gTLD; se debería invitar a los ccTLD a participar. Las respuestas deberían poder buscarse públicamente e incluirse en los informes anuales (en forma completa o por referencia). Además, los informes deberían estar disponibles (por ejemplo, por correo electrónico) para los ccTLD que no participen.		
18	**Garantizar que las actividades de cumplimiento de la ICANN sean neutrales y efectivas** 18.1. La organización de la ICANN debería encargar una auditoría externa de las actividades de cumplimiento y mantenerlas a un alto nivel. 18.2. La Junta Directiva de la ICANN debería facultar a la Oficina de Cumplimiento para reaccionar ante los reclamos y exigir a Cumplimiento que inicie investigaciones y exija el cumplimiento de las obligaciones contractuales contra aquellos que ayuden e instiguen al uso indebido sistemático, tal como se define en el SLA. Esta autoridad adicional podría incluir el apoyo a las acciones por etapas en torno a la intervención progresiva de las medidas de cumplimiento y las acciones apropiadas implementables que la organización de la ICANN puede utilizar en respuesta a cualquier caso que no se subsane infracciones de cumplimiento dentro de los plazos especificados. 18.3. La Oficina de Cumplimiento de la ICANN debería, de forma predeterminada, involucrar a los SLA en el cumplimiento y la presentación de informes, procesos claros y eficientes, una parte reclamante cabalmente informada, satisfacción medible y máxima divulgación pública.		Alta
19	**Actualizar el manejo de nombres que incurran en uso indebido** 19.1. La organización de la ICANN debería basarse en las actividades actuales para investigar las típicas denominaciones engañosas, en cooperación con los investigadores y las partes interesadas, siempre que sea posible. 19.2. Cuando un nombre engañoso se eleva al nivel de nombre abusivo, la organización de la ICANN debería incluir este tipo de uso indebido en sus informes DAAR y desarrollar políticas y mejores prácticas para la mitigación. 19.3. La organización de la ICANN debería publicar la cantidad de reclamos de nombres abusivos que se realizan en el portal de forma que permita a terceros independientes analizar, mitigar y prevenir los daños y perjuicios derivados del uso de dichos nombres de dominio. 19.4. La organización de la ICANN debería actualizar las actuales "Directrices para la implementación de los IDN" **[agregar cita]**		Alta

	para incluir una sección sobre nombres que contengan marcas comerciales, encadenamiento de TLD y el uso de errores tipográficos (difíciles de detectar). Además, la ICANN debería exigir contractualmente el cumplimiento de las "Directrices para la implementación de IDN" para los gTLD y recomendar que los ccTLD hagan lo mismo.		
20	**Desarrollo completo de una prueba de regresión del DNS** 20.1. La organización de la ICANN debería completar el desarrollo de un conjunto de pruebas de regresión del DNS.[17] 20.2. La organización de la ICANN debería garantizar la implementación y el mantenimiento de la capacidad de realizar pruebas funcionales de diferentes configuraciones y versiones de software.		Alta
21	**Implementar las recomendaciones de SAC063 y SAC073 y establecer procedimientos formales para los traspasos de claves** 21.1. La organización de la ICANN debería implementar las recomendaciones de SAC063 y SAC073 para garantizar la SSR del proceso de traspaso de la KSK. 21.2. La organización de la ICANN debería establecer un procedimiento formal, respaldado por un lenguaje y una herramienta formales de modelado de procesos[18] para especificar los detalles de futuros traspasos de claves, incluidos los puntos de decisión, tramos de excepción, el flujo de control completo, etc. La verificación del proceso de traspaso de clave debería incluir la publicación del procedimiento programático (por ejemplo, el programa, FSM) para comentario público y se deberían 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 debería ser reevaluado al menos con la misma frecuencia que el propio traspaso (es decir, con la misma periodicidad) para que se puedan utilizar las lecciones aprendidas para ajustar el proceso. 21.3. La organización de la ICANN debería crear un grupo de partes interesadas que involucre al personal relevante (de la organización de la ICANN o de la comunidad) para realizar periódicamente ejercicios de simulación que sigan el proceso de traspaso de la clave para la firma de la llave de la zona raíz.		Alta

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

18 Análisis iterativo para mejorar las propiedades clave de los procesos críticos que requieren un empleo intensivo de personal: Un ejemplo de la seguridad en las elecciones, Leon J. Osterweil, Matt Bishop, Heather Conboy, Huong Phan, Borislava I. Simidchieva, George Avrunin, Lori A. Clarke, Sean Peisert, ACM Transactions on Privacy and Security (TOPS), Vol. 20, N.º 2, Mayo 2017, págs. 5:1-31. (UM-CS-2016-012)

22	**Establecer prácticas de seguridad básicas para operaciones y operadores de servidores raíz** 22.1. La organización de la ICANN, en estrecha colaboración con el RSSAC y otras partes interesadas pertinentes, debería garantizar que el modelo de gobernanza del RSS, tal como lo propone el RSSAC037, incluya las mejores prácticas de seguridad básicas para las operaciones y los operadores de servidores raíz con el fin de minimizar los riesgos de SSR asociados con la operación del servidor raíz. Estas mejores prácticas deberían incluir la gestión de cambios, procedimientos de verificación y procedimientos de verificación de sanidad. 22.2. La organización de la ICANN también debería desarrollar KPI relevantes para medir la implementación de estas mejores prácticas y requisitos y asegurar la presentación de informes públicos anuales sobre cómo los Operadores de Servidores Raíz (RSO) y otras partes relevantes, incluida la organización de la ICANN, pueden cumplir con estos KPI. 22.3. La organización de la ICANN debería documentar las estrategias de fortalecimiento del Servidor Raíz Gestionado por la ICANN, comúnmente conocidas como Raíz L, y debería alentar a otros RSO para que hagan lo mismo. 22.4. La organización de la ICANN debería asegurarse de que el IMRS utilice un proceso de divulgación de vulnerabilidades (no necesariamente público), informes de seguridad e inteligencia y comunicación con investigadores y asesoramiento o recomendaciones del RSSAC, según corresponda.		Alta
23	**Acelerar la implementación del RZMS de nueva generación** 23.1. Las operaciones de la ICANN y PTI deberían acelerar la implementación de nuevas medidas de seguridad del RZMS con respecto a la autenticación y autorización de los cambios solicitados. 23.2. La organización de la ICANN debería iniciar un período de comentario público tan pronto como sea posible sobre los cambios relacionados con las revisiones de las políticas del RZMS.		Alta
24	**Crear una lista de estadísticas y métricas sobre el estado operativo de los sistemas de identificadores únicos** 24.1. 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 cada tipo de información de identificador único, como el servicio relacionado con la zona raíz, los registros de la IANA y cualquier servicio de gTLD sobre el cual la organización de la ICANN tenga autoridad. 24.2. La organización de la ICANN debería publicar un directorio de estos servicios, conjuntos de datos y métricas en una sola		Media

	página del sitio web de la organización de la ICANN, como por ejemplo en la plataforma de datos abiertos. 24.3. La ICANN debería publicar resúmenes anuales y longitudinales de estos datos, solicitar comentarios públicos sobre los resúmenes e incorporar los comentarios para mejorar los informes futuros. 24.4. Para ambos conjuntos de KPI, la organización de la ICANN debería elaborar resúmenes tanto del año anterior como en forma longitudinal, solicitar y publicar un resumen de los comentarios de la comunidad sobre cada informe e incorporar estos comentarios para mejorar los informes de seguimiento.		
25	**Garantizar que el acceso centralizado a los datos de los archivos de zona esté disponible de forma constante** 25.1. La comunidad de la ICANN y la organización de la ICANN deberían tomar medidas para garantizar que el acceso al CZDS, así como a otros datos, esté disponible de manera oportuna y sin obstáculos innecesarios para los solicitantes. 25.2. La organización de la ICANN debería implementar las cuatro recomendaciones del SSAC 97:[19] *"Recomendación 1: El SSAC recomienda que la Junta Directiva de la ICANN sugiera al personal de la ICANN que considere la posibilidad de revisar el CZDS para abordar el problema de las suscripciones que finalizan automáticamente de forma predeterminada, por ejemplo, permitiendo que las suscripciones se renueven automáticamente de forma predeterminada. Esto podría incluir una opción que permitiera al operador de registro apartarse del valor predeterminado por cada suscriptor, obligando así al suscriptor elegido a volver a presentar la solicitud al final del plazo actual. El CZDS debería continuar proporcionando a los operadores de registro la capacidad de interrumpir explícitamente el acceso de un suscriptor problemático en cualquier momento.* *Recomendación 2: El SSAC recomienda que la Junta Directiva de la ICANN sugiera al personal de la ICANN que se asegure de que en las siguientes rondas de nuevos gTLD, el acuerdo de suscripción del CZDS se ajuste a los cambios ejecutados como resultado de la implementación de la Recomendación 1.* *Recomendación 3: El SSAC recomienda que la Junta Directiva de la ICANN sugiera al personal de la ICANN que procure formas de reducir la cantidad de reclamos de acceso a*		Alta

[19] 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 de actividad mensuales de los operadores de registro", 12 de junio de 2017, https://www.icann.org/en/system/files/files/sac-097-en.pdf.

	archivos de zona y que procure maneras de resolver los reclamos de manera oportuna. *Recomendación 4: El SSAC recomienda que la Junta Directiva de la ICANN sugiera al personal de la ICANN que se asegure de que el acceso a archivos de zona y las estadísticas de consultas de WHOIS basadas en la web se informen de manera precisa y pública, de acuerdo con estándares bien definidos que todos los operadores de registro de gTLD puedan cumplir uniformemente. La métrica del acceso a archivos de zona (ZFA) debería aclararse tan pronto como sea posible.*		
26	**Documentar, mejorar y probar los procesos de EBERO** 26.1. La organización de la ICANN debería documentar públicamente los procesos de ERERO, incluidos los puntos de decisión, acciones y excepciones. El documento debería describir las dependencias para cada decisión, acción y excepción. 26.2. Siempre que sea posible, la organización de la ICANN debería automatizar estos procesos y probarlos anualmente. 26.3. La organización de la ICANN debería realizar públicamente pruebas de verificación de EBERO a intervalos predeterminados utilizando un plan de pruebas coordinado con las partes contratadas por la ICANN con antelación para garantizar que se ejerciten todos los tramos de excepción y publicar los resultados. 26.4. La organización de la ICANN debería mejorar el proceso permitiendo que el Agente de Custodia de Datos del gTLD envíe el depósito de custodia de datos directamente al proveedor de EBERO.		Alta
27	**Actualizar la DPS y crear un consenso en torno a los futuros traspasos del algoritmo DNSKEY** 27.1. Las operaciones de PTI deberían actualizar el DPS para facilitar la transición de un algoritmo de firma digital a otro, incluida una transición anticipada del algoritmo de firma digital RSA al ECDSA o a futuros algoritmos postcuánticos, que creará un DNS más resiliente y al mismo tiempo proporcionará el mismo o un mayor nivel de seguridad. 27.2. Dado que el traspaso del algoritmo DNSKEY raíz es un proceso muy complejo y delicado, las operaciones de PTI deberían trabajar con otros socios de la zona raíz y con la comunidad global para desarrollar un plan de consenso para futuros traspasos del algoritmo DNSKEY raíz, que tenga en cuenta las lecciones aprendidas del primer traspaso de la KSK en 2018.		Media

28	**Elaborar un informe sobre la frecuencia de la medición de colisiones de nombres y proponer una solución** 28.1. La organización de la ICANN debería producir conclusiones que caractericen la naturaleza y frecuencia de las colisiones de nombres y las preocupaciones consiguientes. La comunidad de la ICANN debería implementar una solución antes de la próxima ronda de gTLD. 28.2. La organización de la ICANN debería facilitar este proceso mediante el inicio de un estudio independiente de las colisiones de nombres hasta su eventual finalización y adoptar o justificar la implementación o no adopción de cualquier recomendación resultante. Por "independiente", el SSR2-RT refiere a que la organización de la ICANN debería garantizar que los resultados del equipo de evaluación del informe y la investigación del grupo de trabajo del Proyecto de Análisis de Colisiones de Nombres (NCAP) del SSAC sean examinados por las partes que no tengan ningún interés financiero en la expansión de TLD. 28.3. La organización de la ICANN debería permitir que la comunidad informe sobre instancias de colisión de nombres. Estos informes deberían permitir el manejo apropiado de datos sensibles y amenazas a la seguridad y deberían ser incluidos en las métricas de los informes de la comunidad.		Media
29	**Enfoque en las mediciones de privacidad y RSS y mejora de las políticas basadas en esas mediciones** 29.1. La organización de la ICANN debería monitorear e informar de manera periódica sobre el impacto en la privacidad de las tecnologías como DoT (DNS sobre TLS) y DoH (DNS sobre HTTPS). 29.2. Por lo tanto, los acuerdos y políticas de consenso de la organización de la ICANN con operadores de registro y registradores deberían tener cláusulas que reflejen el cumplimiento de los mismos y al mismo tiempo deberían garantizar que el DNS no se fragmente debido a la necesidad de mantener/implementar los requisitos mínimos que rigen la recopilación, retención, custodia, transferencia y presentación de los datos de registración, que incluyen la información de contacto del registratario, los contactos administrativos y técnicos, así como la información técnica asociada a un nombre de dominio. 29.3. La organización de la ICANN debería: 29.3.1. Crear unidades especializadas dentro de la función de cumplimiento contractual que se centren en 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 RDAP en evolución. 29.3.2. Supervisar la legislación de privacidad pertinente y en evolución (por ejemplo, la CCPA y la legislación que protege la información de identificación personal [PII]) y garantizar que		Alta

	las políticas y procedimientos de la organización de la ICANN estén alineados y cumplan con los requisitos de privacidad y la protección de la información de identificación personal según lo exijan la legislación y las reglamentaciones pertinentes.[20] 29.3.3. Desarrollar y mantener actualizada una política de protección de la información de identificación personal. La política debería comunicarse a todas las personas involucradas en el procesamiento de la información de identificación personal. Deberían implementarse medidas técnicas y organizacionales para proteger adecuadamente la PII. 29.3.4. Llevar a cabo auditorías periódicas de la adhesión a las políticas de privacidad que implementan los registradores para asegurar que, como mínimo, tienen procedimientos disponibles para abordar las infracciones a la privacidad. 29.4. El DPO de la organización de la ICANN también debería ser responsable de la PII externa del DNS. El DPO debería orientar a los gerentes y a las partes interesadas en lo que respecta a las responsabilidades y los procedimientos, y supervisar e informar sobre los avances técnicos pertinentes.		
30	**Mantenerse informado sobre la investigación académica en materia de cuestiones de RSS y utilizar esa información para apoyar los debates sobre políticas** 30.1. La organización de la ICANN debería hacer un seguimiento de los avances en la comunidad de investigación de revisión por pares, centrándose en las conferencias de investigación sobre redes y seguridad, incluidas al menos la ACM CCS, la Conferencia sobre la Medición de Internet de ACM, Usenix Security, CCR, SIGCOMM, IEEE S&P, así como las conferencias de seguridad operativa APWG, M3AAWG y FIRST, y 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. 30.1.1. Estos informes deberían incluir recomendaciones de acciones, incluidos los cambios en los contratos con registros y registradores, que puedan mitigar, prevenir o remediar los daños y perjuicios a los consumidores y a la infraestructura en materia de SSR identificados en la literatura revisada por pares. 30.1.2. Estos informes también deberían incluir recomendaciones de estudios adicionales para confirmar las conclusiones revisadas por pares, una descripción de los datos que se necesitarían para ejecutar los estudios adicionales recomendados y la forma en que la ICANN puede ofrecer ayuda a los agentes para acceder a dichos datos, por ejemplo, el CZDS.		Media

[20] El Equipo de Revisión tiene conocimiento de que la Carta Orgánica de la organización de la ICANN estipula un enfoque para la participación gubernamental https://www.icann.org/en/system/files/files/proposed-org-engagement-govt-standards-charter-25feb19-en.pdf y el Informe legislativo (el Seguimiento) https://www.icann.org/legislative-report-2019. Sin embargo, nos gustaría un enfoque más específico sobre la privacidad y la protección de datos.

31	**Aclarar las implicancias de SSR del DNS sobre HTTP** 31.1. La organización de la ICANN debería encargar una o varias investigaciones independientes sobre las implicancias relacionadas con la SSR de las tendencias de despliegue de DoH, así como las implicancias para el futuro rol de la IANA en el ecosistema de Internet. El resultado que se pretende conseguir es garantizar que todas las partes interesadas tengan la oportunidad de comprender las implicancias en materia de SSR de estos avances y las diversas alternativas (o la falta de ellas) que tienen las distintas partes interesadas para influir en el futuro.		Alta

Guía para los futuros equipos de revisión de SSR: conclusiones

Con el fin de permitir evaluaciones más directas por parte de los futuros equipos de revisión de SSR, el SSR2-RT se esforzará por formular sus propias recomendaciones de acuerdo con los criterios SMART: siempre que sea posible, las recomendaciones serán *específicas, medibles, asignables, relevantes y trazables*. El SSR2-RT considera que recomendaciones más claras y orientadas a la acción simplificarán la implementación, el seguimiento y el proceso de evaluación que se llevará a cabo en la próxima revisión de SSR. El SSR2-RT ha incluido información adicional sobre el proceso y la metodología que utilizó el SSR2-RT para cumplir su mandato en el 'Apéndice C: Proceso y metodología'.