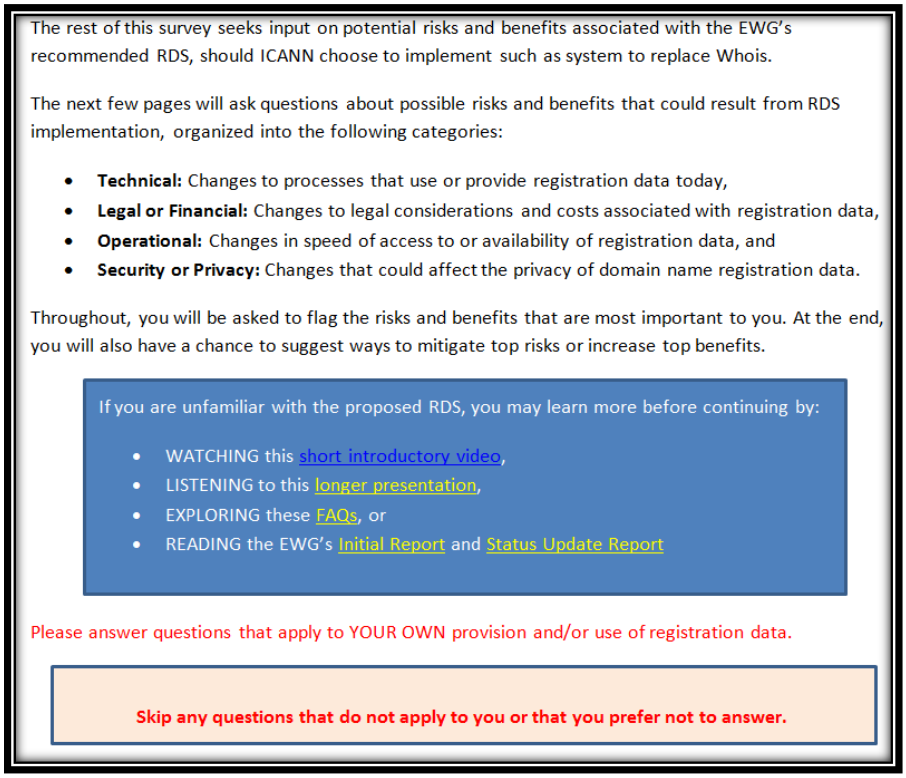
Encuesta sobre Riesgos del RSD - Resumen de Resultados

El 14 de marzo, el Grupo de Trabajo de Expertos sobre Servicios de Directorio de gTLD (EWG) invitó a todas las partes que brindan servicios de datos de registración de nombres de dominio de gTLD a participar en una Encuesta sobre Riesgos del RDS, que incluye a los Registratarios, Registradores, Registros y a una amplia gama de individuos, empresas y otras organizaciones que utilizan datos del Whois en la actualidad. Esta encuesta ofrecía a los encuestados la posibilidad de informar al EWG sobre todos los riesgos y beneficios que el **Servicio de Directorio de Registración para la Próxima Generación (RDS**) podría implicar para ellos.

El presente documento resume los riesgos y beneficios del RDS identificados mediante esta encuesta. El EWG utilizó estas respuestas a la encuesta para identificar y reducir riesgos innecesarios y no anticipados al momento de preparar su Informe Final (publicado el 6 de junio de 2014). El EWG también recomendó que las respuestas se utilicen como aporte para realizar una futura evaluación completa de los riesgos del RDS propuesto.

Diseño de la Encuesta

La introducción presentada a continuación establece el escenario al brindar contexto para quienes no están familiarizados con el RDS y clasifica los riesgos y beneficios en cuatro categorías:



The rest of this survey seeks input on potential risks and benefits associated with the EWG's recommended RDS, should ICANN choose to implement such as system to replace Whois.

The next few pages will ask questions about possible risks and benefits that could result from RDS implementation, organized into the following categories:

- **Technical:** Changes to processes that use or provide registration data today,
- **Legal or Financial:** Changes to legal considerations and costs associated with registration data,
- **Operational:** Changes in speed of access to or availability of registration data, and
- **Security or Privacy:** Changes that could affect the privacy of domain name registration data.

Throughout, you will be asked to flag the risks and benefits that are most important to you. At the end, you will also have a chance to suggest ways to mitigate top risks or increase top benefits.

If you are unfamiliar with the proposed RDS, you may learn more before continuing by:

- WATCHING this short introductory video,
- LISTENING to this longer presentation,
- EXPLORING these FAQs, or
- READING the EWG's Initial Report and Status Update Report

Please answer questions that apply to YOUR OWN provision and/or use of registration data.

Skip any questions that do not apply to you or that you prefer not to answer.

Para cada categoría, se mostraron a los encuestados ejemplos de posibles riesgos y beneficios y se los invitó a:

- *Seleccionar TODOS los Riesgos Técnicos que potencialmente LO afectarían.*
- *Seleccionar DOS (2) riesgos que lo afectarían de manera más significativa.*
- *Seleccionar DOS (2) riesgos con altas probabilidades de ocurrir.*

- *Seleccionar CUALQUIER riesgo en relación al RDS recientemente introducido que no sea un riesgo del Whois ya conocido.*

También se invitó a los encuestados a indicar otros potenciales riesgos y beneficios. El resumen de las respuestas de la encuesta identifica los riesgos y beneficios comúnmente mencionados, además de los que se indicaron de manera adicional.

Generalidades de las Respuestas.

Esta Encuesta Inicial sobre los Riesgos del RDS fue realizada en inglés y recabó 182 respuestas parciales hasta el 12 de junio de 2014. Más de 100 encuestados complementaron la encuesta en su totalidad.

Todas las respuestas, a excepción de una, fueron enviadas antes de la publicación del Informe Final del EWG. En ese sentido, estos resultados ofrecen aportes sobre RDS tal como se propone en el Informe de Actualización del EWG (11 de noviembre de 13) presentado en la Reunión ICANN48 celebrada en Buenos Aires. Estos resultados no deben considerarse como aportes en relación a las propuestas finales del RDS detallados en el informe del mes de junio de 2014 del EWG. No obstante, estas respuestas ayudaron al EWG a comprender cuáles son, según los usuarios y proveedores de datos, los riesgos y beneficios potencialmente significativos, de impacto y probables asociados con *cualquier* RDS de próxima generación.

Demografía de los encuestados

- Representación global, que incluye América del Norte (68%), Europa (35%), Asia (20%), América Latina (14%), África 12%) y Oceanía (10%). [1]
- Equitativamente divididas entre quienes USAN y BRINDAN datos de registración:
  - 84% utilizan datos de registración requeridos de Whois
  - 63% ingresan datos y 24% recaban, almacenan o retransmiten datos del Whois.
  - Aquellos que USAN datos incluyen a los Registratarios (45-57%), usuarios individuales de Internet (50%), usuarios de Internet comerciales (50%), personal técnico de Internet (40%), investigadores de Internet (41%), investigadores OpSec (36%), titulares de propiedad intelectual (27%), otros investigadores (14%), agencias de cumplimiento de la ley (5%) y aproximadamente otros 20.
  - Quienes BRINDAN datos incluyen las personas físicas (65%), personas jurídicas (59%), registradores (14%), registros (9%), Proveedores de Servicios de representación (Proxy) (5%), y terceros (5%).

Riesgos Técnicos del RDS

- Posibles **impactos técnicos negativos** citados con mayor frecuencia (104 respuestas):
  1. Quizás ya no tenga acceso público anónimo a todos los datos de registración (69).
  2. La acreditación para el acceso a datos restringidos podría ser onerosa (65).
  3. Puede ser necesario cambiar mis prácticas de acceso a los datos de registración (62).
- Riesgos identificados como de mayor impacto / más probables: 1 y 2 antes mencionados

[1] Nota: Respuestas múltiples permitidas; en total excede el 100%

- Además de los riesgos explícitamente enumerados, se identificaron los siguientes riesgos técnicos:
    - El nuevo RDS podría afectar a las partes que brindan Whois histórico y reverso (8).
    - El acceso automático podría ya no estar disponible (6)
    - No es posible obtener información sobre delincuentes, socios comerciales o Solicitantes (3)
    - El tiempo de respuesta para la obtención de datos de registración podría incrementarse (2)
    - Podrían violarse los derechos de privacidad (2)
    - Única fuente de falla / riesgos técnicos según SAC061 (2)
    - Información a granel para el cumplimiento de la ley y los generadores de correo basura (spammers)-dos grupos susceptibles de cometer abusos.
    - Los datos que se pueden buscar públicamente desaparecerán
    - Puede ser necesario cambiar los [Inicios de sesión] utilizados inicialmente y durante el proceso debido a la rotación.
    - Transferencia/migración
    - Introducción de cuestiones inter-jurisdiccionales
    - Sin escrutinio público de los datos de registración en los registradores conocidos por permitir datos falsos
    - Los cambios en los datos de registración pueden requerir certificados SSL
    - Rompe el modelo de DNS delegado
    - Pierdo la visibilidad de los inicios de sesión respecto de quién tiene acceso a mis datos personales en algunas circunstancias
    - Pierdo la capacidad de controlar o evitar el acceso a la información en forma directa
    - Desarrollo, control de calidad, revisión y actualización de los costos, sin ingresos para compensar

    Nota General: Los encuestados identificaron todos estos como riesgos técnicos, pero muchos se encuentran, en realidad, clasificados como otros tipos de riesgos, considerados otra parte en esta encuesta.

Beneficios Técnicos del RDS

- Posibles **impactos técnicos positivos** citados con mayor frecuencia (89 respuestas):
    1. Los datos de registración a los que accedo podrían ser más precisos (58).
    2. El acceso a los datos de registración puede ser más uniforme y consistente (56).
    3. Podría tener un mejor acceso a los datos restringidos que realmente necesito (41).
- Beneficios identificados como de mayor impacto / más probables: 1 y 2 antes mencionados
- Además de los beneficios explícitamente enumerados, se identificaron los siguientes beneficios técnicos:
    - Mejora de la precisión de los datos (a través de la gestión de contactos y validación) (8)
    - Aquellos con derecho legal podrían acceder a mis datos, en lugar de publicarlos para que todo el mundo los vea.

- Puedo identificar más fácilmente los ciberocupas (cybersquatters) reincidentes y seriales antes de presentar una demanda o reclamo de UDRP, con el consiguiente ahorro de dinero y recursos para mis clientes.
- Siempre voy a tener que proporcionar Whois puerto 43 y no es demasiado problemático
- Los datos de registración a los que se accede son más aplicables, útiles y significativos
- La transferencia de dominios entre los registratarios será más fácil (los datos WHOIS seguirán igual, ya no es necesario el análisis de los resultados del Whois)
- Impacto negativo debido a la minería de datos a gran escala reducido - Ejemplo: menos correo basura

Riegos Financieros y Legales del RDS

- Posibles **impactos legales y financieros negativos** citados con mayor frecuencia (102 respuestas):
  1. La cantidad de datos de registración disponibles gratuitamente para todos podría disminuir (68).
  2. Mi costo total para la obtención de los datos de registración podría aumentar (66).
  3. La conexión de acceso o notificación podría comprometer las investigaciones en curso (51).
- Riesgos identificados como de mayor impacto / más probables: 1 antes mencionado
- Además de los riesgos explícitamente enumerados, se identificaron los siguientes riesgos legales y financieros:
  - Puede dificultar el rastreo de los infractores de marcas registradas o creadores de correo basura *(spammers*). (3)
  - El tiempo para acceder a los datos puede presentar retrasos (3)
  - Sin el acceso público a todos los datos, podrían hacerse menos innovaciones de valor agregado.
  - Demasiados nuevos TLD conducen a un aumento de los costos y muchas registraciones de mala fe.
  - La falta de transparencia de los propietarios de sitios web (en particular de sitios comerciales con transacciones monetarias o ingresos de datos personales) puede ser un riesgo para los consumidores.
  - Puede resultar difícil confirmar la información sobre otros dominios que posee un registratario al momento de confirmar la elegibilidad en el dominio restringido.
  - La falla no sería identificada. Un objetivo para el control de DOS legal y otros "ataques"
  - Podría estar obligado a proporcionar información inexistente (por ejemplo, dirección de correo real; sí, hay personas que no tienen domicilio fijo que tienen los nombres de dominio registrados)
  - La creación de un monopolio sobre los datos del Whois frenará la innovación y centralizará demasiado poder en una "guía telefónica" de Internet en un solo lugar.
  - En algunas situaciones en las que me encuentro dando vueltas no es una información que quisiera compartir, incluso con gente de confianza.

- Quiero que mis datos de Whois estén a disposición de todas las partes interesadas, tal como lo están en la actualidad
- Los Registros en la UE y en otros lugares con leyes de protección de datos no podrán exportar datos a los RDS, y se erosionará enormemente su utilidad.
- Carga de los costos y potencial inconveniente legal impuesto sobre los registratarios, registradores y registros con un beneficio mínimo para las partes afectadas, máximo beneficio para otros.

Beneficios Financieros y Legales del RDS

- Posibles **impactos legales y financieros positivos** citados con mayor frecuencia (68 respuestas):
  1. La mejora de la calidad de los datos de registración podría reducir deficiencias costosas (42).
  2. El cumplimiento contractual de las obligaciones relacionadas con los datos podría ser más robusto (35).
  3. Podría resultar más fácil obtener acceso legal a los datos de registración restringidos (35).
- Beneficios identificados como de mayor impacto / más probables: 1 y 2 antes mencionados
- Además de los beneficios explícitamente enumerados, se identificaron los siguientes beneficios legales y financieros:
  - Mi riesgo de tener grandes cantidades de datos personales (que incluyen datos comerciales en relación a individuos) disminuirá de forma drástica.
  - Conectar con facilidad a los titulares de dominios y descubrir las redes
  - Podría culpar al proveedor de la ICANN / RDS por la falta de transparencia y falta de responsabilidad.

Riesgos Operativos del RDS

- Posibles **impactos operativos negativos** citados con mayor frecuencia (87 respuestas):
  1. Mi acceso a los datos de registración podría verse obstaculizado por una falla del RDS (68).
  2. Mi acceso a los datos restringidos podría retrasarse por la acreditación lenta (66).
  3. Mi acceso a los datos de registración podría verse obstaculizado por los cuellos de botella ocasionados en el RDS (65).
  4. Los datos de registración devueltos del RDS podrían no estar sincronizados con las actualizaciones recientes (56).
- Riesgos identificados como de mayor impacto / más probables: 2 y 3 antes mencionados
- Además de los riesgos explícitamente enumerados, se identificaron los siguientes riesgos operativos:
  - Retransmitir y revelar la respuesta de los Servicios Acreditados de Privacidad y Representación (Proxy) podría llevar más tiempo (7)
  - Nuestro negocio podría estar en riesgo sobre la base de las decisiones de política en relación al RDS.

- El acceso restringido al público no permite la transparencia de los consumidores a quienes pagan por servicios o al ingresar datos personales
- Violación de datos
- Puede haber mayor dificultad / retraso en la tramitación de correo basura (spam) /ataques / cuestiones de la red procedente de fuentes externas.
- Los datos de acceso restringidos para el nivel de acreditación pueden no cumplir con el requisito actual.
- Las reglas arbitrarias evitarán las necesidades de acceso válidas.
- Quiero que TODAS las partes tengan acceso a mis datos mediante la tecnología actual establecida.
- Los sitios ilegales que operan a través de programas de red afiliados estarán más protegidos de las agencias de cumplimiento de la ley, los proveedores de servicios y los consumidores que han sido engañados.
- Hay que poner en práctica y mantener un nuevo proceso y sistema cuando no se quiebre el estatus quo.
- Tiempo adicional, ingresos y oportunidades perdidas para un mayor contacto inicial por parte de un asesor de IP sin experiencia que hará un uso indebido o aprovechará el nuevo sistema de manera inapropiada.

Beneficios Operativos del RDS

- Posibles **impactos operativos positivos** citados con mayor frecuencia (61 respuestas):
  1. Retransmitir y revelar la respuesta de los Servicios Acreditados de Representación (Proxy) podría llevar más tiempo (40).
  2. Yo podría tener acceso de alta velocidad más confiable a los datos de registración (40).
  3. El acceso autenticado en tiempo real a los datos restringidos puede ser más rápido que en la actualidad (39).
  4. El tiempo de respuesta del RDS puede ser más uniforme y predecible que Whois (35).
- Beneficios identificados como de mayor impacto / más probables: 2 y 4 antes mencionados
- Además de los beneficios explícitamente enumerados, se identificaron los siguientes beneficios operativos:
  - El RDS agregado puede soportar mejor funciones tales como WhoWas y Whois Reverso (7)

Riesgos en materia de Privacidad y Seguridad del RDS

- Posibles **impactos negativos en materia de seguridad y privacidad** citados con mayor frecuencia (70 respuestas):
  1. Mis datos de registración pueden ser más vulnerables a los ataques externos (40).
  2. Mis datos de registración pueden ser mal utilizados por el operador de RDS (40).
  3. Voy a tener que suministrar una identidad verificable para registrar un dominio de gTLD (24).
- Riesgos identificados como de mayor impacto / más probables: 1 y 2 antes mencionados

Encuesta sobre Riesgos del RSD - Resumen de Resultados

- Además de los riesgos explícitamente enumerados, se identificaron los siguientes riesgos en materia de seguridad y privacidad.
    - "Los usuarios individuales de Internet" son, a menudo, los titulares de derechos y deben tener la capacidad de acceder a la registración pertinente para investigar infracciones en línea (5)
    - Preocupa el hecho de que los usuarios individuales que deben tener acceso puedan quedar excluidos.
    - El suministro de un número de teléfono o correo electrónico válidos son esenciales para que los titulares de derecho investiguen la infracción.
    - Mis consultas sobre datos de registración pueden ser mal utilizadas por el operador de RDS.
    - Voy a tener que poner en peligro los derechos que tengo, tanto como persona jurídica y persona física, al tener que elegir uno u otro - cuando mi registración del nombre de dominio claramente admite ambos. Por lo tanto, se me pediría renunciar a derechos en virtud de una categoría de derechos, a pesar de tener legalmente derecho a ambos beneficios.
    - Riesgo en relación a la privacidad personal de que mis datos se tornen más disponibles como administrador de nombres de dominio.
    - Pérdida de registraciones a causa de los requisitos adicionales; las empresas en formación pueden no tener identificadores comerciales, etc., pero aun así necesitar un dominio.
    - Los atacantes externos tendrán ahora un importante blanco intermitente.
    - Mi identidad personal puede estar asociada forzosamente a un dominio que pertenece a una entidad corporativa y que está controlado por ella, no por mí en persona
    - Personas y organizaciones con intenciones maliciosas se aprovechan de la capacidad de ocultar información en los datos restringidos, lo que dificulta la tarea de investigación del personal de seguridad y cumplimiento.
    - No puedo registrar un nombre de dominio en forma anónima
    - Revelación de mis motivos para acceder a los datos. Son legítimos, pero es asunto mío, no de la ICANN.
    - Los datos de registración podrían ser menos accesibles por parte de sectores de seguridad, marcas y otros actores en relación al cumplimiento en el sector privado.
    - Mis datos de registro serán más vulnerables a terceros, incluidos los que manejan las funciones de seguridad privada para empresas privadas y que va a querer más acceso a la información personal y sensible a través de múltiples gTLD.
    - Posibilidad de aparecer mencionado en una demanda como consecuencia de la disponibilidad de mi nombre para la empresa
    - El ofrecer acceso por niveles para la aplicación de ley es una manera de concederles un acceso extra, y es una forma de evitar las órdenes judiciales y citaciones. Ese no es el tipo de oportunidad o proceso en el que la ICANN debe participar.
    - Las decisiones de política futuras en relación a los datos de registración podrían ser realizadas por una sola entidad.

-- Publicado el 28 de julio de 2014 --

- El acceso de terceros podría contravenir las leyes locales, la retención de datos o la vida privada, o exponer legalmente al cliente sin mi conocimiento.
- El acceso de terceros o compromiso de datos almacenados podrían crear herramientas masivas para el uso indebido de mis datos o los de mi cliente.
- El nuevo sistema podría ser un nuevo vector de ataque.

Beneficios en materia de Privacidad y Seguridad del RDS

- Posibles **impactos positivos en materia de seguridad y privacidad** citados con mayor frecuencia (55 respuestas):
  1. Mis datos de registración pueden estar mejor protegidos del uso indebido (37).
  2. Mis datos de registración pueden asegurarse de manera más uniforme (31).
  3. Yo podría publicar un ID de Contacto re utilizable en lugar de mi nombre (29).
  4. Menos datos de registración podrían ser públicos y estar disponibles de manera anónima (27).
- Beneficios identificados como de mayor impacto / más probables: 2 y 3 antes mencionados
- Además de los beneficios explícitamente enumerados, se identificaron los siguientes beneficios en materia de seguridad y privacidad:
  - Las Reglas de Validación, Autenticación y Autorización se aplicarán sistemáticamente y se pueden auditar con facilidad (7)
  - Me inclinaría más por actualizar mi información de contacto para que sea precisa, dado que el acosador no tendría acceso a la misma
  - Se requiere proporcionar certificación legal versus natural
  - Mejor acceso abierto a una entidad legal

Nuevas Perspectivas

Los encuestados brindaron 30 comentarios en relación a los **Riesgos Inevitables**, teniendo en cuenta los riesgos anteriormente enunciados:

1. El acceso a los datos de registración que se encuentran actualmente disponibles de forma gratuita disminuirá.
2. Los riesgos 5a, 5b, 9b (cambio en las prácticas, reducción del acceso público disponible en forma gratuita) son inherentes al RDS.
3. Cualquier entidad que controla un punto de acceso central singular para recuperar datos de registración siempre tendrá mucho poder sobre un bien público.
4. La cuestión del acceso ilimitado a los datos, incluso por aquellos que tienen credenciales, es un tema que la comunidad necesita comprender mejor. El hecho de que sea poco probable que el RDS verifique búsquedas muy amplias por parte de los actores estatales y terceros constituye un gran riesgo.
5. Si la arquitectura falla, no vamos a tener fácil acceso a la información O el acceso de acreditación lleva demasiado tiempo.
6. Capacidad para obtener información de manera oportuna y eficiente (para apoyar a clientes que llevan a cabo investigaciones sobre sitios web ilegales)
7. Capacidad para proteger a los consumidores de compras y / o la introducción de datos personales en sitios web ilegales (debido a la falta de transparencia en relación a la titularidad del sitio)
8. Almacenamiento centralizado y suministro de Whois para todas las registraciones en cualquier tipo de base de datos (en lugar de los registradores y registros) incrementa la exposición a la violación de datos.

-- Publicado el 28 de julio de 2014 --

9. Un sistema como este será un imán para aquellos que deseen *hackear* bases de datos, lo que podría resultar en un servicio lento y con cortes repetidos.
10. Yo creo que puede ser posible que alguien brinde alguna información correcta al momento de la registración, pero ¿cómo se mantendrá?
11. El cumplimiento de las normativas de la ICANN no es la única razón para proporcionar acceso al WHOIS. En la práctica, el registro siempre tendrá que proporcionar acceso al WHOIS mediante el puerto 43 y puerto 80, lo que incrementa el riesgo y el costo.
12. El RDS viola un principio fundamental de Internet - la devolución del poder y el control. Lo hace mediante la introducción de muchas nuevas cuestiones inter-jurisdiccionales de una manera técnicamente deficiente.
13. Ignora estos problemas: 1) ¿Cómo puedo encontrar un servidor de Whois para una zona; 2) dominios "privados" que están abiertos para su registración "pública"; 3) la base instalada, herramientas y prácticas existentes.
14. El nuevo mecanismo dicta que hay muchos datos ocultos. Esto conducirá a un aumento del riesgo para el público dado que no se tomarán medidas sobre los dominios [problemáticos] ni serán escalados. Las pruebas también se perderían para el cumplimiento de la ley
15. El sistema actual requiere que se brinde una gran cantidad de datos. Estos datos son vulnerables a la captura en la presentación o en el almacenamiento por parte de personas con una postura ética dudosa y con intención delictiva.
16. Los seres humanos están involucrados - la falla está integrada en el sistema.
17. La centralización del control sobre quién puede acceder a los datos de registración de nombres de dominio y el requisito de cierto tipo de validación de la persona o entidad que tiene acceso a dichos datos, crea un riesgo inevitable de monopolio y la disminución de la capacidad para hacer cumplir la ley y para que los investigadores en materia de seguridad puedan identificar de manera efectiva el comportamiento abusivo en Internet. Estos riesgos parecen inevitables [en cualquiera de los modelos].
18. Será inevitable una ralentización global del proceso de registración de dominios, si ahora es necesario validar los datos de registración.
19. El RDS propone ampliar el acceso restringido para las agencias de cumplimiento de la ley de la mayoría /todos los países. Por lo tanto, su propósito es exponer a los registratarios individuales a una investigación por parte de las agencias extranjeras, a las que no tienen el deber de obedecer o una razón legítima para someterse a ellas. De este modo el RDS está viciado de manera inherente
20. Todo mecanismo para registraciones anónimas será usado indebidamente. Al menos, el obligar a los infractores a que se registren en una DBA y con una dirección postal constituye una pequeña barrera de entrada para la registración de dominios con fines delictivos.
21. Tanto el acceso abierto como el hecho de impedir la replicación masiva de datos de registración se oponen a los intereses de la especulación en la registración de dominios, por lo que es inevitable que cualquier nuevo RDS establecido por la ICANN "corrija" esos "problemas" con el Whois actual.
22. Está claro que los autores del informe están muy centrados en la protección de la privacidad de un número relativamente pequeño de registratarios de dominios con necesidades especiales de privacidad. Sin embargo, los casos legítimos de esa clase son muy pocos... Los cambios propuestos dificultarán, en gran medida, la tarea de "quienes trabajan bien intencionadamente", y dará lugar a un ecosistema de dominios que es más propenso al abuso, y con más probabilidades de ser poblados con datos inútiles e imprecisos.
23. Poseer grandes datos es, obviamente, un riesgo mayor que no se puede evitar por completo.
24. Toda centralización de los datos plantea el riesgo inevitable de un único punto de falla: hackers, delincuentes cibernéticos y entidades con malas intenciones, tales como los gobiernos deshonestos o gobiernos que hacen abuso de los derechos civiles y humanos necesitan buscar en un solo lugar para obtener información privada.
25. Cualquier restricción del acceso público a la información sobre la identidad del propietario de un dominio dificulta la investigación contra el correo basura (*spam*) y software malicioso.
26. El terrible historial de la ICANN en cuanto a las operaciones y el cumplimiento hace totalmente inverosímil que esto funcione
27. Mis datos de registración se encuentran en otro país, en cuya jurisdicción no confío.

28. Parece que el nuevo sistema de RDS mejorará en gran medida la privacidad de los datos de registración, por lo tanto promoverá la libertad de expresión que, en mi opinión, es el fundamento y la belleza de la Internet. Mi única preocupación, en cuanto a los riesgos inevitables, es en lo que respecta a los operadores y empleados, así como las personas y organizaciones que podrán o podrían tener acceso ilimitado y / o no regulado a todos los datos de registración.
29. El servicio centralizado es arriesgado e innecesario y expone a la ICANN a cuestiones legales engorrosas que pueden evitarse. Veamos algunas de las soluciones potenciales.
30. No importa el tipo o estructura de teatro kabuki que pudiera acompañar el origen del RDS o lo que podría finalmente ofrecer a alguien que no sea una agencia de cumplimiento de la ley o intereses de marcas registradas como beneficio, este RDS se percibiría como una fuente de datos que los Gobiernos utilizarán indebidamente.

13 encuestados proporcionaron respuestas detalladas y fundamentos en relación a los **Riesgos Aceptables**:

1. El riesgo es aceptable sobre la base de los recursos técnicos existentes en la actualidad (informática de alto rendimiento, distribución basada en nube y la tecnología de recuperación ante fallos para incrementar la disponibilidad, etc. (5)
2. En tanto se desarrolle con el diseño técnico generalmente aceptado destinado a asegurar la disponibilidad de toda seguridad, se deben mitigar las inquietudes.
3. Los sitios no comerciales (que no tienen requisitos de funcionalidad de comercio electrónico o de entrada de datos) presentan menos riesgo para los consumidores y los que se esfuerzan por protegerlos (empresas, agencias de cumplimiento de la ley, etc.). Menos transparencia en estos sitios sería aceptable.
4. La capacidad para hacer frente a diversas leyes de privacidad es un riesgo aceptable que afecta potencialmente a las empresas.
5. El riesgo de violación de la seguridad de los datos de acceso restringidos es aceptable, ya que el riesgo es aún menor que el que existen en la actualidad con la actual base de datos pública del Whois.
6. El riesgo que representan los grandes datos puede ser aceptable mediante una cuidadosa supervisión operativa y de diseño. La falta de acceso a la información requerida según el nivel de acceso restringido se puede mejorar mediante un cuidadoso análisis de los requisitos de las partes interesadas.
7. La ICANN recibiría menos "Honorarios" como resultado de la implementación del RDS. El RDS propuesto reducirá el volumen de registración del que el mercado goza actualmente, debido a la manera onerosa en la que el cliente debe suministrar grandes cantidades de datos antes de poder hacer una compra inicial.

Los encuestados sugirieron 24 formas de **Reducir o Cambiar los Riesgos:**

1. Medidas adoptadas para mejorar la exactitud
2. Los riesgos de falla / cuello de botella en el RDS se deben administrar mediante una sólida supervisión del operador de RDS.
3. Las capacidades del Whois Reverso/ WhoWas se podrían incorporar en el RDS.
4. Se podría mejorar la reducción de los datos disponibles de manera gratuita a través de un análisis riguroso de los elementos de datos actualmente públicos, y sólo mediante la supresión al acceso público de aquellos para quienes es posible establecer objetivamente la necesidad de dicha supresión.
5. Diseño de un proceso de acreditación sencillo que lleve a una credencial persistente.
6. La identificación de la utilización de un nombre tiene que estar justificada. La respuesta sólo debe basarse en un reclamo. Si la solicitud es válida, entonces es posible dar una respuesta.
7. ¿Recibe el registratario un aviso de que la información ha sido solicitada y, en tal caso, identifica a la parte solicitante?
8. Los principales riesgos del RDS se pueden evitar sólo mediante la implementación de los aspectos de validación en el paradigma actual. Si se desea que todos los datos de registración cumplan con un formato específico, esto se podría lograr mediante la política de la ICANN, en lugar de implementar un nuevo RDS.

9. Quizás una manera de delimitar los sitios comerciales de los no comerciales para proporcionar una mayor transparencia en los sitios comerciales reduciría el riesgo.
10. Al menos, algunos de los riesgos se pueden reducir mediante el uso de un enfoque federado con cada registro que almacena su propia información.
11. Re-pensar el cronograma completo y recabar datos de contacto mínimos. Aplicar los principios estándares de proporcionalidad, privacidad mediante el diseño y privacidad por defecto.
12. Requerir plazos razonables para las respuestas a los contactos luego de los cuales los dominios pueden suspenderse a la espera de una respuesta.
13. Almacenar menos datos.
14. El acceso al Whois puede y debe permanecer anónimo y abierto a todos los usuarios de Internet.
15. Es necesario reducir los tiempos de procesamiento para la validación de los datos de registración tanto como sea posible para que los administradores de dominios puedan ejecutar, de manera eficiente y eficaz, sus dominios con el mínimo tiempo de espera debido a los procedimientos de validación.
16. Sería prudente permitir la elección del consumidor en la selección de un proveedor de validación, por lo que se recomienda a los proveedores mantener los costos y tiempos de procesamiento a fin de que sean competitivos.
17. La centralización de la validación en un grupo pequeño o forzar la validación a través de un proveedor específico disminuirá el incentivo para mantener un proceso rápido y rentable.
18. Permitir la registración de dominios por parte de cualquier persona (no sólo las personas que se considera necesitan la protección de alguna organización) de forma totalmente anónima, sin proporcionar ningún dato de registración. Si casi no hay datos de registración, entonces no hay problema con el acceso público a todos estos datos.
19. Eliminar el anonimato en la registración.
20. Algunos riesgos pueden amortiguarse mediante un enfoque por etapas para la implementación del RDS, por ejemplo, al hacer que cualquier requerimiento de información adicional sea opcional durante un tiempo, en tanto que los datos se ponen a disposición en la infraestructura del WHOIS existente. Esto significará que el sistema de RDS se puede desarrollar y cualquier error / cuestión puede ser fácilmente resuelto sin afectar el sistema existente; entonces, una vez que está establecido y los problemas de integración han sido resueltos con el tiempo suficiente, los registradores / registros pueden hacer el cambio. Sugeriría que el período adecuado para que los datos adicionales sean opcionales y para que los servicios se superpongan fuese de ~ 3 años, esto daría tiempo suficiente para cambiar los sistemas y brindar la capacitación adecuada a los clientes.
21. Eliminar toda registración por representación ("proxy"), exigir la exactitud de los datos de registración, solicitar a los registros restringir el acceso a granel, exigir el acceso Whois abierto pero a velocidad limitada a todos los datos de registración y prohibir la venta de los datos de registración a granel por parte de los registros y registradores.
22. Eliminar el incentivo financiero para que los registradores u otras personas vendan servicios de privacidad en la registración. Actualmente es una fuente de ingresos, tanto como lo eran los números telefónicos no enumerados para las compañías telefónicas. Garantizar que los registradores no perciban * nada * al ofrecer servicios de registración de representación (proxy) o privacidad. Garantizar que los registratarios que tienen una necesidad legítima de registratarios privados o por representación (proxy) abonen una cuota que se suficiente para demostrar que realmente necesitan este tipo de servicio, y que todos los ingresos provenientes de dichos honorarios se destinen a una entidad de bien público (lo que garantiza que la ICANN tampoco tiene ningún motivo para incentivar la registraciones por representación o privacidad)
23. Mejora de la consulta de los datos requeridos en comparación con el nivel de datos restringidos.
24. Con el fin de reducir el riesgo de abuso en el acceso a los datos de registración privados, dicho acceso debe ser aprobado mediante documentos jurídicos firmados por un juez u otra autoridad legal.
25. Superar las percepciones de Snowden / Kafka / Orwell en relación al abuso generalizado de estos intereses excesivos al hacer que todos los accesos y solicitudes al sistema sean 100% transparentes a la visión pública.

26. Para superar la resistencia a los cambios generales, implementar un método para incrementar los beneficios y reducir las desventajas para los Registratarios, Registradores y Registros, como por ejemplo el uso del Registro como sistema centralizado de validación.

13 encuestados sugirieron maneras en las cuales los **Riesgos resultaban una Buena Compensación de los Beneficios:**

1. Los potenciales beneficios dependen de cómo se implementen (2)
2. Los riesgos asociados con la reducción del acceso a los datos (actualmente gratuito y público) podrían reducirse si la comunidad garantizase una mayor precisión de datos para aquellos datos que requieren un acceso restringido. Reducir el acceso sin mayor precisión sería un defecto importante en cualquier nuevo sistema propuesto (2).
3. En tanto que una base de datos agregada podría aumentar los riesgos de seguridad, estos se pueden mejorar mediante el diseño y supervisión adecuados, y un servicio disponible en todas partes que muestre resultados en un formato coherente podría justificar estos riesgos.
4. Acceso diferenciado a cambio de mejores datos (es decir, más completos y precisos) podría ser una posible forma de compensar.
5. El RDS propuesto presenta una serie de ventajas que superan los riesgos. Un acceso fácil a los datos del registratario es fundamental para la exigibilidad de los derechos de propiedad intelectual en línea. Un sistema de RDS que permite mejorar el acceso y la exactitud de estos datos sería muy beneficioso para los titulares de derecho de propiedad intelectual y su asesoramiento para hacer frente a la infracción en materia de propiedad intelectual y otros abusos relacionados con los registratarios de nombres de dominio y otros usuarios de Internet.
6. Si los costos de validación y los plazos pudieran controlarse y minimizarse, los beneficios del sistema propuesto podrían ser algo justo para los beneficios propuestos del sistema. Si no se controlan los costos, éstos superarán seriamente los beneficios.
7. Mejorar la calidad de los datos en la base de datos del Whois es muy importante y vale la pena. La vinculación de los registratarios de manera coherente a la totalidad de su cartera de dominios también es muy importante y vale la pena, lo que garantiza que cuando se identifica y se corrige una inexactitud en el dato de punto de contacto de un dominio, se corrige en todas partes donde existe.
8. El acceso programático mejorado (sin límites de frecuencias arbitrarias o mal concebidas, etc.) también sería de gran ayuda.
9. Acceso uniforme / fiable / utilizable a los datos correctos es una clara ventaja ya que los riesgos se pueden minimizar mediante un cuidadoso diseño y consulta.

Al finalizar la encuesta, 25 encuestados hicieron **Más Comentarios**, que se detallan a continuación.

1. La propuesta carece de características concretas para mejorar la precisión práctica de los datos (la capacidad de contacto de los registratarios) significativamente por encima del nivel de la línea de base planteada en el RAA 2013 y (para los nuevos gTLDs) los PIC. Estos deben ser explicados. Del mismo modo, una base de datos más rica que proporcione servicios mejorados como datos históricos podría ayudar a justificar la reducción del acceso público a este recurso.
2. Uno de los beneficios es que nos permite identificar registratarios que intentan ocultar su identidad para que puedan continuar con las actividades maliciosas y con la distribución de software malicioso.
3. La capacidad de los usuarios y herramientas de terceros para utilizar el actual sistema de Whois a fin de acceder y guardar la información del WHOIS para fines históricos es crítica. Cualquier sistema de RDS propuesto debe garantizar esta capacidad. Esto puede ocurrir, ya sea directamente a través del propio RDS, o indirectamente, al continuar permitiendo que los clientes / herramientas de terceros lo hagan.
4. Otorgar el control monopólico de este bien público a una entidad singular resulta en una pérdida para el mundo con poco beneficio que no se podría lograr a través de otro medio menos centralizado.
5. ¿Por qué hay tantos nuevos gTLD? Esta decisión es desastrosa para los propietarios de marcas, ya que conduce al aumento de los costos en materia de protección de propiedad intelectual. Ya en la actualidad,

nos enfrentamos a una gran cantidad de registraciones de mala fe a pesar de que los períodos de prerregistro (*sunrise*) para los lotes de nuevos gTLD aún no han comenzado. Como empresa más pequeña, es posible que no tenga el presupuesto para registrarse para todos a fin de evitar las registraciones de mala fe. Por otra parte los costos de los recursos legales son altos.

6. El hecho de tener un Whois verificado es de suma importancia debido al anonimato de Internet. Buscamos infractores y los datos inexactos ya no son aceptables.
7. Apoyo plenamente el esfuerzo para hacer que los datos de WHOIS sean más precisos. Sería un cambio positivo SI una base de datos centralizada, cerrada no dificultara la obtención de información, ralentizara el proceso de obtención de información, tuviese un límite en la cantidad de información que se puede obtener, crease procesos largos para que las empresas obtengan acreditación a fin de que puedan acceder a los datos, o crease cuestiones de transparencia para los usuarios de Internet. Gran parte de mi preocupación recae sobre la comunidad de la seguridad cibernética respecto de si es capaz de proteger eficazmente a los consumidores de los sitios web ilegales que pueden sacar ventaja de una base de datos cerrada.
8. El acceso público versus el acceso restringido propuesto para ciertos elementos de datos es bueno. Sería de gran ayuda conocer más detalles en torno a los propósitos de divulgación aceptables, la evaluación de los solicitantes y cómo los usuarios con acceso restringido rinden cuentas, etc. para comentar al respecto.
9. En general, cualquier movimiento para centralizar los datos incrementa, en gran medida, los riesgos de hackeo abierto o encubierto y el espionaje no responsable por parte de gobiernos, los modos de falla a gran escala y la interferencia política. Si bien algunos de los objetivos del RDS son valiosos, no superan en su totalidad a los riesgos predecibles. Los mayores riesgos del RDS son la posibilidad de tener que pagar por el acceso a la información pública del WHOIS y / o la pérdida de acceso público a la información básica de gestión de red, que incluye la asignación de bloques de direcciones de IP, localización física y uso indebido de casillas de correo. Cualquier propuesta que no proteja el acceso público libre y la continua disponibilidad de estos elementos de información debe ser eliminado lo más rápido posible y de forma definitiva.
10. Todavía no estoy seguro de cómo puedo garantizar la "exactitud" de los datos de registración, los datos del primer día (de registración) son una cosa, y otra cosa es la "revisión periódica", que creo es lo más importante. IMO, es posible que tengamos que terciarizar esto a una "agencia" en cada localidad (país, o tal vez, ciudad) para realizar la revisión, pero esto puede conducir a algunas dudas en relación a la exactitud y al estándar nuevamente.
11. Los dos grupos de individuos que el registro promedio desearía evitar que tuvieran acceso masivo a los datos Whois son los creadores de correo basura (*spammers*) y las agencias de cumplimiento de la ley. Brindar información a granel a cualquiera de estos grupos dañaría irreparablemente la reputación del Registro. Un sistema de RDS centralizado requiere que el registro ponga su reputación en manos de un tercero.
12. Es necesario aceptar que no todas las partes tienen la misma protección según las leyes locales y que las solicitudes transfronterizas de datos pueden no proseguir debido a cuestiones de política externa. Con el RDS se perderá un recurso vital en la lucha contra el ciberdelito organizado.
13. Como registratario individual, actualmente uso una función de privacidad / representación (proxy) disponible que brinda mi registrador para proteger mi identidad individual del acceso innecesario e informal por parte del público en general, lo que me parece útil como medida de precaución contra el acoso personal anónimo. Me gustaría ver que las funciones de privacidad exigidas estén regularmente disponibles siempre que utilice cualquier registrador, con el fin de garantizar un mercado de registración totalmente competitivo a nivel de todos los registradores, y no sólo en un subconjunto de registradores voluntarios.
14. El riesgo mayor que me inquieta es el costo para la validación de los datos de registración y la autenticación para tener acceso a los datos restringidos. También me preocupan los tiempos de procesamiento y la desaceleración general que estos procedimientos causan.
15. El RDS es una gran idea. Esto ayudaría a resolver muchos problemas si se aplicara adecuadamente. Espero poder tener algún aporte. Sin embargo, esta encuesta en particular no está bien interpretada.

16. Francamente, este sistema parece ser tan irreflexivo como los servicios de "privacidad del WHOIS" que existen en la actualidad. El mero uso daña la transparencia de una organización y, por lo tanto, su reputación en línea. Gracias por escuchar.
17. Veo que no hay beneficios, sino muchos riesgos en relación al uso indebido o robo de datos. Idealmente, la necesidad de proporcionar los datos de registración al registrador sería eliminada - si no hay datos de registración, entonces no hay riesgo de abuso o robo.
18. Mi preocupación es poder hacer frente a diversos tipos de ataques / correo basura (*spam*) / intrusiones / inundación de datos, etc. en la red. Resulta ABSOLUTAMENTE esencial que exista un contacto válido y que ese contacto, de hecho, resuelva los problemas de red que se le comuniquen. Esto significa que el contacto debe tener la autoridad y la capacidad técnica para garantizar que su dominio no sea fuente de abusos. El sistema actual, en particular aquellos dominios que se ocultan detrás de las representaciones (proxies), NO asegura que el registrador / representante (proxy) podrá (o pueda) abordar las cuestiones de manera oportuna. Si se van a permitir los representantes (proxies), entonces debe quedar ABSOLUTAMENTE claro que quien sea que aparezca en las búsquedas / consultas accesibles públicamente se responsabiliza por el comportamiento del dominio que están protegiendo, lo que incluye la capacidad total para desactivar el dominio en caso de un abuso significativo a la red.
19. El mayor riesgo es cómo se gestionará el acceso a la información "restringida", como por ejemplo, si esto implicará honorarios y cuán oneroso se tornará el proceso de acreditación para obtener acceso. Si esto es costoso u oneroso, entonces se dificultan seriamente las operaciones comerciales básicas, el contacto con los propietarios de dominios, la investigación y muchos otros ámbitos en relación a la gestión e investigación de dominios.
20. Creo que este proceso propuesto es una solución en busca de un problema y está alimentado por argumentos preliminares de personas movidas por ideas políticas dogmáticas.
21. Yo no creo que se hayan considerado cuidadosamente los requisitos de privacidad de las entidades naturales versus legales corporativas / comerciales. Los registratarios individuales / naturales deber poder ser localizados a fin de permitir la resolución de los problemas que afectan a otros, sin embargo, siempre se debe permitir el derecho de guardar el anonimato, salvo en el caso de solicitud legal adecuada. En contraste, las personas jurídicas con sólo restricciones acotadas (como refugios para mujeres, ciertas organizaciones políticas en situación de riesgo), NO DEBEN tener anonimato. Es absolutamente inapropiado, especialmente con las empresas comerciales, que funcionen de forma anónima y los datos DEBEN ser de acceso público / anónimo. En segundo lugar, debe existir un proceso mediante el cual sea posible quitar el anonimato a aquellas entidades que demuestran no calificar para el mismo.
22. Padecemos mucho la actividad de los generadores de correo basura (*spammers*) y botnets que utilizan datos falsos para ocultar la titularidad de los dominios. La información del Whois puede, y debe, ser clara y estar bien definida. No es una penalización excesiva obtener servicios de alojamiento (hosting) de otras entidades, pero debe quedar en claro quién es responsable de los servidores de DNS para un dominio determinado que es operativamente útil.
23. En mi opinión, la privacidad es mucho más importante que el acceso público a los datos de registración.
24. Puesto que no hay beneficios, por favor dejen de hacer lo que están haciendo. Si funciona - no lo arreglen. No hay que olvidar que un número de registratarios SI DESEAN que sus datos de Whois sean accesibles de la misma manera que lo son ahora, y los que no son de uso libre que utilicen POB o protección de privacidad ofrecida al registrador.
25. El RDS es demasiado y una mala idea. Crea costos para aquellos que son menos beneficiados, sin un costoso real para quienes obtienen el mayor beneficio.

Por último, aproximadamente 5 de 182 encuestados completaron la mayoría o totalidad de los campos de texto con formato libre con respuestas que no abordan directamente las preguntas, sino que declararon que el RDS era una mala idea o que no presentaba beneficios.