Informe Final del
Grupo de Trabajo de Expertos en Servicios de Directorio de gTLD:
Un Servicio de Directorio de Registración (RDS) para la próxima generación

ESTADO DE ESTE DOCUMENTO

Este es el informe final del Grupo de Trabajo de Expertos (EWG) en Servicios de Directorio de gTLD, en el cual se detallan nuestras recomendaciones para la Junta Directiva de la ICANN para que un Servicio de Directorio de Registraciones (RDS) para la próxima generación reemplace el sistema de WHOIS actual.

I. RESUMEN EJECUTIVO

Este es el informe final del Grupo de Trabajo de Expertos (EWG) en Servicios de Directorio de gTLD, en el cual se detallan nuestras recomendaciones para la Junta Directiva y el presidente/director ejecutivo de la ICANN para que un Servicio de Directorio de Registraciones (RDS) para la próxima generación reemplace el sistema de WHOIS actual.

Este informe final representa la culminación de un período de trabajo intenso de más de quince meses durante el cual este grupo diverso de voluntarios dedicó miles de horas a la investigación a fondo, tuvo en cuenta más de 2600 páginas de comentarios públicos, respuestas a encuestas y resultados de investigación, y participó en 19 consultas públicas a la comunidad, 35 días de reuniones de EWG en persona, 42 llamadas de EWG, más de 200 llamadas del subequipo y una infinidad de sesiones con expertos externos y miembros de la comunidad. Todo esto se realizó para responder una pregunta simple:

¿Existe una alternativa al sistema de WHOIS actual para servir mejor a la comunidad global de Internet?

Sí, existe. El EWG recomienda de forma unánime abandonar el modelo actual de WHOIS de darles todos los usuarios el mismo acceso público anónimo a datos (a menudo incorrectos) de registración de gTLD.

En lugar de ello, el EWG recomienda un cambio de paradigma a un RDS para la próxima generación, mediante el cual los datos de registración de gTLD serían recolectados, validados y divulgados únicamente con fines permisibles.

Mientras los datos básicos continuarían estando disponibles públicamente, solo solicitantes acreditados podrían acceder al resto, aquellos que se identifiquen, declaren su propósito y acuerden hacerse responsables de que los usarán de manera adecuada.

En las siguientes más de 150 páginas, se describen los aportes y la investigación que generaron esta recomendación del EWG, una propuesta detallada de un nuevo RDS y las conclusiones siguientes:

- El tema es muy complejo.
- El EWG analizó el tema desde muchas perspectivas y realizó una investigación para garantizar que el RDS pueda implementarse.
- El RDS propuesto, a pesar de no ser perfecto, refleja compromisos cuidadosamente diseñados y equilibrados con elementos independientes que no se deben separar.

- El RDS propuesto está diseñado para afrontar, de lleno, y de manera novedosa los temas siguientes:
    - Problemas de privacidad de datos difíciles;
    - Desafíos de validación que han degradado la calidad y la precisión de los datos; y
    - El equilibrio viable entre el acceso y la responsabilidad.
- El RDS se debe adoptar en su totalidad. La adopción de solamente algunos de los principios recomendados en el presente documento socava los beneficios de todo el ecosistema.

Este informe final, junto con las recomendaciones y los principios propuestos para el RDS para la próxima generación, refleja un consenso. Este apoyo es notable teniendo en cuenta la amplia variedad de partes interesadas y de perspectivas que se reflejan en los miembros del EWG.[1]

El EWG confía en que este informe final cumpla con la directriz de la Junta Directiva de la ICANN para ayudar a redefinir el propósito y la disposición de datos de registración de gTLD, que sirva de base para ayudar a la comunidad de la ICANN (a través de la Organización de Apoyo para Nombres Genéricos, GNSO) a crear una nueva política mundial sobre los servicios de directorio de gTLD.

El EWG está seguro de que el RDS descrito en este informe final brinda una base más sólida que la actual, una base desde la cual la GNSO puede desarrollar una nueva política global para que los datos de registración de gTLD protejan la privacidad personal y garanticen mayor precisión, responsabilidad y transparencia de todo el ecosistema de la ICANN en los años venideros.

En el marco de consideración de este informe final por parte de la Junta Directiva, la GNSO y la comunidad de la ICANN, el EWG recomienda centrarse en las preguntas siguientes:

- ¿Se prefiere el RDS en lugar del WHOIS actual?
- De lo contrario, ¿la comunidad de la ICANN cree que debe continuar el sistema de WHOIS actual y que este cumple con las necesidades de la Internet global en evolución?

[1] Consulte el Anexo J para conocer la conformación del EWG y la experiencia de sus miembros.

Antecedentes

El EWG fue creado por el director ejecutivo de la ICANN, Fadi Chehadé, a pedido de la Junta Directiva de la ICANN, con el fin de ayudar a resolver el atascamiento que ya lleva casi una década en la comunidad de la ICANN respecto de cómo reemplazar el sistema actual de WHOIS.[2]

Para dejar atrás las deficiencias de WHOIS identificadas en numerosos informes y estudios de la comunidad[3], el mandato del EWG es reexaminar y definir el propósito de la recolección y el mantenimiento de datos de registración de gTLD, considerar cómo proteger los datos y proponer una solución para la próxima generación en pos de una mejor atención de las necesidades de la comunidad global de Internet.

Comenzando con una tabla rasa, el EWG cuestionó los supuestos fundamentales acerca de los propósitos, los usos, la recopilación, el mantenimiento y la designación de los datos de registración. El EWG evaluó a cada parte interesada relacionada con los servicios de directorio de gTLD mediante el análisis de sus necesidades de precisión, acceso y privacidad. Consideró posibles enfoques para satisfacer esas necesidades de manera más efectiva.

Para guiar las deliberaciones, el EWG redactó una declaración de propósito de alto nivel para alinear las recomendaciones de este informe con la misión de la ICANN y diseñó un sistema para apoyar la registración de nombres de dominio y mantenimiento, que:

[2] Consulte https://www.icann.org/news/announcement-2-2012-12-14-en

[33] Consulte el Anexo B para obtener una lista de informes que documentan las deficiencias de WHOIS.

- Brinda acceso adecuado a datos de registración precisos, confiables y uniformes;
- Protege la privacidad de la información del registratario;
- Ofrece un mecanismo confiable para identificar, establecer y mantener la posibilidad de contactar registratarios;
- Apoya un marco para afrontar problemas relacionados con registratarios, incluso, pero sin limitarse a ello, para la protección de consumidores, la investigación del delito cibernético y la protección de la propiedad intelectual; y
- Proporciona una infraestructura para satisfacer las necesidades correspondientes de los organismos de seguridad.

Usuarios y propósitos

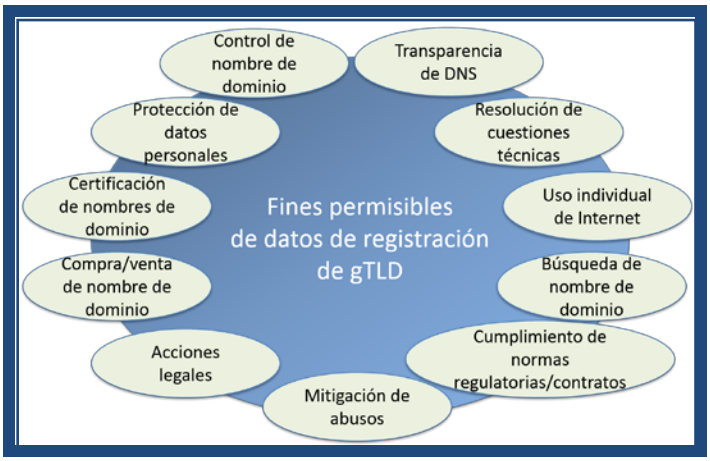
El EWG revisó fines posibles y actuales para recabar, almacenar y proporcionar datos de registración de gTLD a una amplia variedad de usuarios mediante el análisis de un amplio conjunto representativo de casos de uso reales de WHOIS.

El EWG consideró la totalidad de los casos de uso y las lecciones aprendidas de ellos, además del material de referencia y los aportes de la comunidad, para obtener un conjunto consolidado de usuarios y fines permisibles a los cuales se debe ajustar el RDS y posibles usos indebidos que se deben evitar.

Fines que se deben aceptar y fines que se deben prohibir

En consonancia con el mandato del EWG, todos estos usuarios fueron examinados para identificar flujos de trabajo existentes y potenciales, junto con las partes interesadas y los datos involucrados en dichos flujos de trabajo.

Se analizaron las necesidades de información de registro de nombres de dominio con el objetivo de obtener elementos de datos obligatorios, riesgos relacionados e implicaciones de políticas, y se respondieron otras preguntas revisadas en este informe. Los fines permisibles recomendados por el EWG se resumen a la derecha.

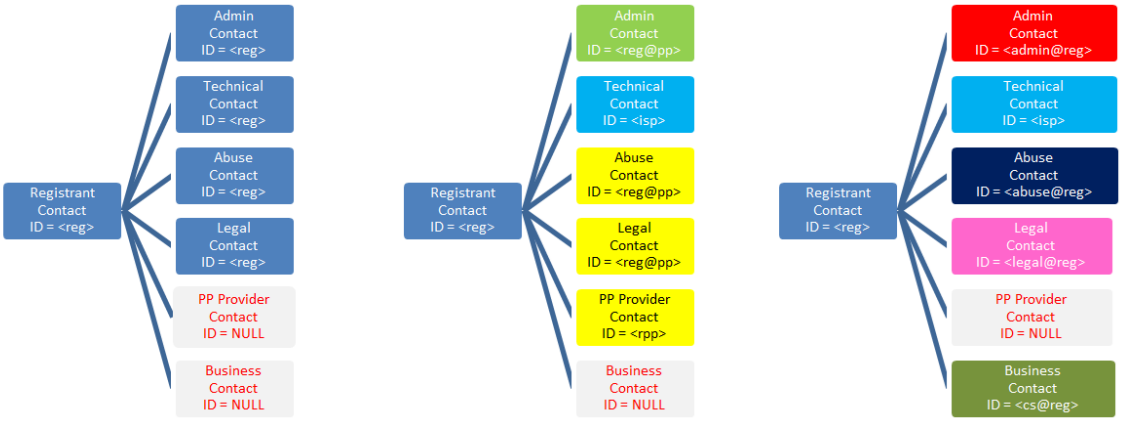


A continuación, se definen los fines permisibles identificados actualmente y las necesidades asociadas de consultas, contacto y datos de registración. Puede encontrar más detalles al respecto en la Sección III.

Propósito	Ejemplos de tareas que incluye
Control de nombre de dominio	La creación, la administración y la supervisión del nombre de dominio (DN) del registratario, incluso la actualización de información relacionada con el DN, la creación, la transferencia, la renovación, la eliminación y el mantenimiento del portfolio de DN, además de la detección del uso fraudulento de la información de contacto del registratario.
Protección de datos personales	La identificación del proveedor acreditado de servicios de privacidad/representación o el aprobador de credenciales con protección de seguridad asociados con un DN por el cual se informa un abuso, se solicita la divulgación de datos relacionados o se contacta al proveedor en cuestión.
Resolución de cuestiones técnicas	El trabajo para resolver cuestiones técnicas asociadas con el uso de nombres de dominio, incluso problemas asociados con el envío de correos electrónicos, fallas de resolución de DNS y problemas técnicos de sitios web, mediante el contacto con personal técnico encargado de resolver estas cuestiones.
Certificación de nombres de dominio	La autoridad de certificación (CA) que emite el certificado X.509 para un sujeto identificado por un nombre de dominio que requiere confirmación de que el DN está registrado con el sujeto de certificación.

Propósito	Ejemplos de tareas que incluye
Uso individual de Internet	La identificación de la organización que utiliza el nombre de dominio para generar confianza en los consumidores o el contacto con la organización para hacerle llegar el reclamo de un cliente o la documentación de un reclamo acerca de esta.
Compra o venta de nombre de dominio comercial	Consultas de compras relacionadas con DN, la adquisición de un DN de otro registratario y la investigación de diligencia debida.
Investigación de DNS de interés público/académico	Estudios de investigación de interés público/académico acerca de nombres de dominio publicados en el RDS, incluso información pública acerca del registratario y los contactos designados, el estado y el historial del nombre de dominio y los DN registrados por un registratario dado.
Acciones legales	La investigación de posibles usos fraudulentos del nombre o la dirección de un registratario por parte de otros nombres de dominio, la investigación de posibles infracciones de marca, el contacto con un representante legal del registratario/licenciatario antes de llevar a cabo acciones legales si la cuestión no se aborda correctamente.
Cumplimiento de normas regulatorias/contratos	La investigación de autoridades tributarias de negocios con presencia en línea, la investigación de UDRP, la investigación de cumplimiento contractual y las auditorías de custodia de datos de registración.
Mitigación de abusos relacionados con DNS e investigación criminal	El informe de abusos a quien pueda investigar y enfrentar dicho abuso o el contacto con entidades asociadas con ese nombre de dominio durante una investigación criminal fuera de línea.
Transparencia de DNS	La consulta de datos de registración publicados por registratarios para cumplir con una variedad de necesidades de informar al público en general.

Para brindar acceso con un propósito a datos de registración y mejorar la comunicación y la privacidad personal, el EWG elaboró principios para contactos con un propósito (PBC). Los PBC, que se basan en roles y responsabilidades, se asignaron a todos los fines permisibles en los cuales se requiere contacto. A continuación, se muestran tres ejemplos y se pueden encontrar más detalles en la Sección III y en la Sección IV.



El EWG analizó más en detalle todos los elementos de datos de registración —comenzando por aquellos definidos en el RAA 2013— en pos de generar un conjunto de principios rectores para la recopilación y la divulgación de datos, que se complementa con el marco de PBC recomendado y con las recomendaciones formuladas para cumplir con las leyes de protección de datos. El EWG formuló más recomendaciones para identificar nuevos elementos de datos que los registratarios y los contactos pueden publicar para que la comunicación sea más sólida. Estas recomendaciones se detallan en la Sección IV y se brindan ejemplos en el Anexo E.

Acceso con un propósito

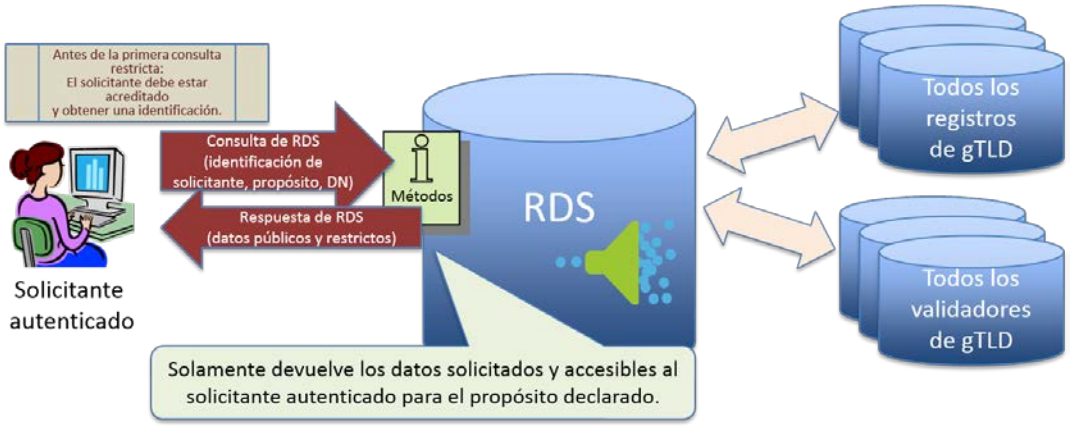
El RDS recomendado utiliza un enfoque de tabla rasa y abandona el sistema de WHOIS de talla única para todos en favor del acceso con un propósito para los datos validados con la esperanza de mejorar la privacidad, la precisión y la responsabilidad. El EWG cree que este nuevo paradigma de acceso puede mejorar la responsabilidad de todas las partes involucradas en la divulgación y el uso de datos de registración de gTLD, ya que:

- Registra todo acceso a datos de registración de gTLD, incluso el acceso no autenticado a elementos de datos públicos, a fin de eliminar y mitigar abusos;
- Restringe el acceso a elementos de datos más confidenciales que solamente estarían disponibles para solicitantes que pidan acceso al RDS y se lo otorguen, en el nivel apropiado para cada usuario y propósito establecido; y
- Audita el acceso a datos restrictos y públicos para minimizar el abuso y aplicar penalidades y otras medidas por uso inadecuado, en virtud de los términos y las condiciones acordadas explícitamente por cada solicitante.

Los principios de acceso a datos del EWG, que sirvieron de base para las recomendaciones detalladas de acceso a datos restrictos y públicos, se explican en la

Sección IV. Como se describe a continuación, todavía cualquiera puede solicitar elementos de datos públicos desde el RDS, con autenticación o sin ella.

Los elementos de datos restrictos también se pueden solicitar por medio del RDS. Para hacerlo, los solicitantes primero deben estar acreditados. Posteriormente, los solicitantes pueden enviar consultas autenticadas para solicitar elementos de datos para un fin establecido.



Consulte el Anexo E para obtener una ilustración más detallada de elementos de datos devueltos para consultas de datos públicos y restrictos, de cómo el acceso restricto depende del usuario y del fin, y de cómo los acreditadores de usuarios de RDS juegan un papel importante en la autorización y la auditoria del acceso restricto.

Privacidad y protección de datos

Es central para el mandato del EWG cómo diseñar un sistema que mejore la precisión de los datos recabados y ofrecer protección para los registratarios que busquen cuidar y mantener la privacidad.

El EWG reconoce que la información personal está resguardada por leyes de protección de datos y que, incluso cuando no rige ninguna ley, existen razones legítimas para que

los individuos busquen la mejor protección para su información personal. Asimismo, algunos negocios y organizaciones pueden buscar protección para su información con propósitos legítimos, por ejemplo, cuando van a lanzar una nueva línea de productos o, en el caso de las pequeñas empresas, cuando la información de contacto incluye datos personales.

En consecuencia, el EWG elaboró un conjunto de recomendaciones para aplicar el cumplimiento de rutinas con leyes de protección de datos y de privacidad, que se detalla en la Sección VI. Estos principios incluyen:

- Mecanismos para facilitar la rutina de recopilación de datos que cumplen con la ley y la transferencia entre actores del ecosistema de RDS;
- Cláusulas contractuales estándares que armonizan con leyes de protección de datos y de privacidad, y que están codificadas en políticas;
- Un "motor de reglas" para aplicar leyes de protección de datos; y
- La manera en que la ubicación del almacenamiento de datos de RDS se relaciona con el acceso a organismos de seguridad.

Además de la privacidad lograda gracias al cumplimiento de las leyes de protección de datos, el RDS también recomendó principios en pos de satisfacer las necesidades de privacidad mediante la inclusión de lo siguiente en el ecosistema de RDS:

- Un servicio acreditado de privacidad/representación para uso general; y
- Un servicio acreditado de credenciales con protección de seguridad para personas en riesgo y en lugares en los cuales no se respete el derecho de libertad de expresión o se persiga a quienes deseen expresarse.

Además, el EWG recomienda que la ICANN investigue el desarrollo de una política de privacidad armonizada que rija las actividades del RDS de manera integral.

Para afrontar las necesidades de servicios de privacidad y representación uniformes y confiables que permitan generar mayor responsabilidad, el EWG incorporó la comunicación de privacidad/representación en los principios de PBC. También recomendó los Principios de privacidad/representación y un marco como aporte para el Grupo de Trabajo sobre Cuestiones de Acreditación de Servicios de Privacidad y Representación de la GNSO.

Para satisfacer las necesidades de los individuos y los grupos que pueden demostrar que estarían en riesgo si se los identificara en datos de registración, el EWG recomienda un marco de credenciales con protección de seguridad en el cual estas partes pueden

solicitar y recibir nombres de dominios registrados usando credenciales seguras, con la ayuda de los responsables de emitir certificaciones y de terceros confiables para ofrecer una protección entre las entidades en riesgo y los registratarios. El EWG recomienda que la ICANN establezca una junta de revisión independiente y confiable que valide los reclamos de individuos u organizaciones en riesgo para aprobar (y rechazar, cuando sea necesario) las credenciales.

Calidad de los datos

El EWG recomienda fijar una validación más sólida de los datos de los registratarios que la del sistema de WHOIS actual o aplicar mejoras que se pueden obtener por medio de una implementación integral del **RAA 2013**. Entre las mejoras básicas para la calidad de los datos, se incluyen las siguientes:

- La designación de contactos con un propósito por parte de los registratarios debería generar mejoras significativas a la accesibilidad de los contactos adecuados para varios propósitos y ofrecer un incentivo para que los registratarios brinden información apropiada para esos roles.
- Con el acceso restricto a elementos de datos confidenciales, los registratarios deben tener menos incentivo de proporcionar datos inexactos, además de más responsabilidad para garantizar la precisión de los datos.

Asimismo, el EWG recomienda dos mejoras relacionadas aunque independientes:

- Una validación estándar de todos los datos de registración de gTLD, usando validación y comprobaciones periódicas en el momento de realizar la recopilación, con la opción de efectuar una validación previa de bloques de datos de contacto para reutilizarlos en varias registraciones de nombres de dominio y se debe permitir que los usuarios de RDS vean cuándo se validaron los datos por última vez y en qué nivel; y
- Un directorio de contacto prevalidado, conceptualmente independiente del directorio de nombres de dominio, para promover la calidad y la reutilización de los elementos de datos usados para contactar a los registratarios de nombres de dominio y a individuos u organizaciones que puedan designar los registratarios como PBC para diversos propósitos asociados con una registración de nombres de dominio y para disuadir el uso fraudulento de datos personales.

Los principios y los procesos que detallan estas recomendaciones se pueden consultar en la Sección V.

Modelos de implementación

Al considerar cómo llevar a la práctica estos principios y recomendaciones, el EWG analizó diversos modelos alternativos en detalle. Todos los modelos se evaluaron por medio de un conjunto de criterios multifacéticos, como se muestra en el Anexo F. Después de realizar análisis rigurosos, el EWG concluyó lo siguiente:

- En la actualidad, los registradores o los afiliados de registradores recopilan y almacenan información de registración de sus propios clientes (registratarios). Este proceso es inherentemente distribuido. Además de que los registradores o los afiliados de registradores continúen recopilando los datos de los registratarios, el EWG propone que validadores recopilen los datos de contacto.
- Existen diversos modelos posibles para el almacenamiento de información de registración en todos los gTLD. El EWG identificó una variedad de modelos posibles y destacó los dos que aparecen como los más prometedores. Recomienda que se seleccione uno por medio del criterio de evaluación.
- Para proteger la privacidad del asunto de los datos, mediante una interfaz centralizada se debe permitir a los solicitantes acceder a información de registración en todos los gTLD, incluso el acceso a datos públicos no autenticados y a datos restrictos autenticados.
- El RDS debe usar RDAP o EPP (según corresponda para cada interfaz) como protocolo subyacente de acceso a directorios a fin de obtener información de registración de las ubicaciones de almacenamiento, donde sea que se encuentren.

El EWG desarrolló y probó varios modelos de sistemas alternativos, que se detallan en el Anexo F, incluso modelos sugeridos por la comunidad de la ICANN. Estos modelos posibles difieren en la manera en que se copia la información de registración o se la consulta por medio del RDS. El EWG analizó todos los modelos con detenimiento a fin de determinar el impacto de estas diferencias. Después de comparar estos modelos posibles, el EWG concluyó que, a excepción del WHOIS actual, todos son capaces de satisfacer en cierta medida los principios de RDS recomendados por el EWG. El EWG se centró en los dos modelos más prometedores para examinarlos con mayor detenimiento: el modelo federado y el modelo sincronizado (antes denominado "modelo agregado").

Para informar el análisis con mayor detalle, el EWG encomendó un análisis de costos de modelo de implementación a un tercero neutral (IBM) con el objetivo de determinar los requerimientos y los posibles costos de ambos modelos. Sobre la base del análisis detallado del EWG, además del informe de análisis de IBM, en el cual se concluyó que el

modelo federado es más costoso para todo el ecosistema del RDS, **el EWG recomendó el RDS sincronizado (SRDS).**

Conclusión

Debido a los detalles exhaustivos, la complejidad y la extensión del informe final, este resumen ejecutivo no constituye una descripción general integral y se recomienda que los lectores consulten el cuerpo del informe final para obtener más información.

El EWG envió este informe final al director ejecutivo y a la Junta Directiva de la ICANN, lo publicó en Internet y llevará a cabo varias consultas públicas en la reunión de junio de 2014 de la ICANN en Londres. También brindará seminarios web y habrá otras oportunidades para analizar el informe y responder preguntas relacionadas con él, con la comunidad de la ICANN. El informe final está destinado a servir de base para el proceso de desarrollo de políticas (PDP) de la GNSO solicitado por la Junta Directiva para la asignación de datos de registración de gTLD y para negociaciones contractuales, según corresponda.

El EWG confía en que este informe final cumpla con la directriz de la Junta Directiva de la ICANN para ayudar a redefinir el propósito y la disposición de datos de registración de gTLD y que sirva de base para ayudar a la comunidad de la ICANN (a través de la GNSO) a crear una nueva política mundial sobre los servicios de directorio de gTLD.

II. Mandato, propósito y resultados del EWG

a. Mandato

El Grupo de Trabajo de Expertos (EWG) en Servicios de Directorio de gTLD fue creado por el director ejecutivo de la ICANN, Fadi Chehadé, a pedido de la Junta Directiva de la ICANN, con el fin de ayudar a resolver el atascamiento que ya lleva casi una década en la comunidad de la ICANN respecto de cómo reemplazar el sistema actual de WHOIS. Diversos estudios e informes de la comunidad[4], publicados durante este período apuntan a deficiencias del sistema actual, que requieren una solución.

El mandato del EWG es reexaminar y definir el propósito de la recopilación y el mantenimiento de servicios de directorio de gTLD, considerar cómo proteger los datos y proponer una solución para la próxima generación en pos de una mejor atención de las necesidades de la comunidad global de Internet. El EWG comenzó con una tabla rasa, analizó y cuestionó los supuestos fundamentales acerca de los propósitos, los usos, la recopilación, el mantenimiento y la designación de los datos de registración. El EWG evaluó a cada parte interesada relacionada con los Servicios de Directorio de gTLD mediante el análisis de sus necesidades de precisión, acceso y privacidad, y los posibles enfoques para satisfacer esas necesidades.

b. Propósito

Con el fin de facilitar las deliberaciones del EWG, el grupo redactó una declaración de propósito de alto nivel como base para evaluar sus conclusiones y recomendaciones, a saber:

> En respaldo de la misión de la ICANN de coordinar el sistema global de identificadores únicos de Internet, y de garantizar la operación estable y segura del sistema de identificadores únicos de Internet, la información sobre los nombre de dominio de gTLD es necesaria para promover la confianza de todas las partes interesadas en Internet.
>
> En consecuencia, es deseable diseñar un sistema que respalde la registración y el mantenimiento de nombres de dominio, que:
>
> - Brinde acceso adecuado a datos de registración precisos, confiables y uniformes;

[44] Consulte el Anexo B para obtener una lista de informes que documentan las deficiencias de WHOIS.

- Proteja la privacidad de la información personal;
- Ofrezca un mecanismo confiable para identificar, establecer y mantener la posibilidad de contactar registratarios;
- Apoye un marco para afrontar problemas relacionados con registratarios, incluso, pero sin limitarse a ello, para la protección de consumidores, la investigación del delito cibernético y la protección de la propiedad intelectual; y
- Proporcione una infraestructura para satisfacer las necesidades correspondientes de aplicación de la ley.

c. Resultados

El 24 de junio de 2013, el EWG publicó su informe inicial, preguntas frecuentes y un cuestionario en línea, y comenzó un amplio proceso de consultas en la comunidad de la ICANN respecto de sus recomendaciones iniciales. En su informe inicial, el EWG concluyó que se debe abandonar el modelo de WHOIS actual, que le da a cada usuario el mismo acceso público anónimo a datos (a menudo inexactos) de registración de gTLD. En su lugar, el EWG recomienda un cambio de paradigma, mediante el cual los datos de registración de gTLD son recolectados, validados y divulgados únicamente con fines permisibles, con ciertos elementos de datos accesibles solamente para solicitantes autenticados y responsables de usarlos apropiadamente.

El EWG llegó a esta recomendación después de un examen completo de los informes anteriores que detallan las deficiencias de WHOIS y las muchas partes interesadas que utilizan el sistema de WHOIS actual. Para cada grupo de usuarios identificado, el EWG analizó los propósitos cumplidos por los datos de registración y los elementos de datos individuales necesarios para hacerlo. Con la información de este análisis, el EWG recomendó principios y características para guiar la creación de un Servicio de Directorio de Registración (RDS) para la próxima generación. Para ilustrar cómo podrían aplicarse estos principios, el EWG también consideró varias alternativas y propuso un modelo para la recopilación y divulgación de los elementos de datos de registración de nombres de dominio precisos para conseguir fines permisibles.

El 11 de noviembre de 2013, después de una cuidadosa consideración de todos los comentarios y aportes recibidos de la comunidad de ICANN, el EWG publicó un Informe de Actualización de Estado, en el que se destaca el pensamiento del EWG respecto de muchos temas clave. El Informe de Actualización de Estado también proporcionó mucho

más detalle del análisis que había detrás del informe inicial, según lo solicitado por la comunidad.

El EWG se ha involucrado en un análisis detallado de comentarios recibidos sobre estos dos informes, usando los amplios y diversos aportes de la comunidad para informar sus trabajos en curso sobre áreas abiertas y para probar y perfeccionar sus recomendaciones. Debido a la complejidad de la tarea por realizar y la importancia de basar cualquier RDS para la próxima generación en una sólida comprensión de los beneficios y los impactos que probablemente derivarían de ello, el EWG realizó una investigación en cinco áreas: prácticas de validación de datos de ccTLD existentes y comerciales, prácticas de proveedores de servicios de privacidad/representación existentes, exploración de organizaciones capaces de acreditar usuarios de RDS y el análisis de riesgos/beneficios y costos de RDS. Los resultados de esta investigación, publicada en marzo de 2014, se utilizaron para perfeccionar las recomendaciones del EWG.

En esta coyuntura, el EWG ha considerado cuidadosamente el trabajo pasado de WHOIS, usuarios actuales y posibles futuros usuarios de los datos de registración de gTLD y sus propósitos, el aporte de las muchas y diversas partes interesadas en el sistema de WHOIS actual, las prácticas existentes asociados con las mejoras de RDS propuestas y el análisis de costos, beneficios y riesgos de RDS. Todos estos aportes han informado las recomendaciones[5] del EWG para elaborar un sistema para la próxima generación, que se detalla en este informe final para la Junta Directiva de la ICANN y

[5] En este informe, los principios del EWG siguen los términos que figuran a continuación, sobre la base de las definiciones dadas en RFC 2119:

- DEBE: Esta palabra, o los términos "OBLIGATORIO" o "DEBERÁ", significa que la definición es un requisito absoluto de este informe.
- NO DEBE: Esta frase, o la frase "NO DEBERÁ", significa que la definición es un requisito absoluto de este informe.
- DEBERÍA: Esta palabra, o la frase "SE RECOMIENDA", significa que pueden existir razones válidas en determinadas circunstancias para ignorar un elemento en particular, pero se deben comprender todas las consecuencias y se las debe sopesar con cuidado antes de elegir un camino diferente.
- NO DEBERÍA: Esta frase, o la frase "NO SE RECOMIENDA", significa que pueden existir razones válidas en determinadas circunstancias cuando el comportamiento es aceptable o incluso útil, pero se deben comprender todas las consecuencias y se las debe sopesar con cuidado antes de tener un comportamiento descrito con esta etiqueta.

están dirigidos a servir de aporte para el proceso de desarrollo de políticas.

III. Usuarios y propósitos

a. Metodología

Se incentivó al EWG, al trabajar en pos de la definición de la próxima generación de servicios de directorio de registración, para que adoptase un enfoque de tabla rasa, en lugar de procurar mejoras al sistema actual de WHOIS, el cual es considerado inexacto en gran medida. En consonancia con las instrucciones de la Junta Directiva, el EWG comenzó su análisis examinando los propósitos existentes y potenciales de la recolección, el almacenamiento y el suministro de datos de registración de gTLD a una amplia gama de usuarios.

Con el fin de lograr dicho propósito, los miembros del EWG confeccionaron un conjunto de casos que involucran al sistema de WHOIS actual, y analizaron cada uno de estos casos para identificar (i) los usuarios que desean acceder a los datos, (ii) sus fundamentos de la necesidad de dicho acceso, (iii) los elementos de datos que necesitan y (iv) los propósitos que sirven dichos datos. Los casos también fueron utilizados para identificar a las partes interesadas involucradas en la recolección, el almacenamiento y el suministro de datos de registración, ayudando al EWG a comprender los flujos de trabajo existentes y potenciales y las maneras en que se podría satisfacer mejor tanto a los usuarios como a sus necesidades mediante el RDS para la próxima generación.

El objeto de los casos de uso no era ser exhaustivos, sino representativos de los múltiples usos del sistema de WHOIS actual, ejemplificando una amplia gama de usuarios, necesidades y flujos de trabajo. El inventario de los casos de uso considerados por el EWG se incluye en el Anexo C.

El EWG consideró la totalidad de los casos de uso y las lecciones aprendidas a partir de ellos, con el fin de extraer un conjunto consolidado de partes interesadas y propósitos deseados que deberían ser tenidos en cuenta en el RDS, así como también un conjunto de posibles usos indebidos que el sistema debería procurar disuadir (presentados en mayor detalle en la próxima sección de este informe). Asimismo, el EWG consultó materiales de referencia surgidos de actividades previas en relación con WHOIS, aportes de la comunidad y casos de uso para examinar las necesidades específicas en cada una de las áreas indicadas en la Figura 1 que se incluye a continuación.

Figura 1: Análisis de necesidades

El EWG continuó con su labor analizando estos propósitos y necesidades de usuarios para extraer un conjunto mínimo de elementos de datos, riesgos relacionados con la accesibilidad de los datos, implicancias en materia de legislación y políticas sobre privacidad, y preguntas adicionales para analizar en mayor detalle en el presente informe.

b. Usuarios y propósitos de RDS

En la Figura 2 incluida a continuación, se presenta un resumen no exhaustivo de usuarios del sistema de WHOIS existente, incluso los que tienen fines constructivos o maliciosos. En consonancia con el mandato del EWG, todos estos usuarios fueron examinados para identificar flujos de trabajo existentes y potenciales, junto con las partes interesadas y los datos involucrados en dichos flujos de trabajo.

Figura 2: Usuarios

En este informe, el término "solicitante" se usa en referencia genérica a cualquiera de estos usuarios que desee obtener datos de registración de gTLD del sistema. Tal como se detalla en este informe, el EWG recomienda abandonar el modelo actual de WHOIS, que le otorga a cada usuario el mismo acceso público y anónimo a datos de registración de gTLD (frecuentemente inexactos). En su lugar, el EWG recomienda un cambio de paradigma, mediante el cual los datos de registración de gTLD son recolectados, validados y divulgados únicamente con fines permisibles, con ciertos elementos de datos accesibles solamente para solicitantes autenticados y responsables de usarlos apropiadamente.

El EWG analizó los casos de uso representativos para desarrollar la tabla que figura a continuación, en la cual se resumen las clases de usuarios que desean acceder a los datos de registración de gTLD, los fundamentos de dicha necesidad y los propósitos generales que se cumplen mediante dichos datos. Se brindan más detalles acerca de los usuarios, los propósitos y las necesidades de datos asociadas en la Sección III (c), Fines que se deben aceptar y que se deben prohibir, y en el Anexo D.

Usuario	Propósito	Casos de uso de ejemplo	Fundamento para acceder a los datos de registración
Todos los registratarios (personas físicas, personas jurídicas, proveedores	Control de nombre de dominio	Creación de cuenta de registración de nombre de dominio	Permitir el registro de nombres de dominio por parte de todo

Usuario	Propósito	Casos de uso de ejemplo	Fundamento para acceder a los datos de registración
acreditados de servicios de privacidad/representación)			registratario mediante la creación de una nueva cuenta con un registrador
		Supervisión de modificación de datos de nombre de dominio	Detectar la modificación accidental, no informada o no autorizada de los datos de registración de un nombre de dominio, actual o histórico (con WhoWas)
		Gestión de portfolio de nombres de dominio	Facilitar la actualización de los datos de registración de todos los nombres de dominio (por ejemplo, contactos designados, direcciones) para mantener un portfolio de nombres de dominio
		Iniciación de transferencia de nombre de dominio	Permitir que un registratario inicie una transferencia de nombre de dominio a otro registrador
		Supresiones de nombres de dominio	Permitir la supresión de un nombre de dominio vencido
		Actualizaciones de DNS de nombres de dominio	Permitir que un registratario inicie un cambio de DNS de un nombre de dominio
		Renovaciones de nombres de dominio	Permitir la renovación de un nombre de dominio registrado por parte del registratario del nombre de dominio
		Validación de contacto del nombre de dominio	Facilitar la validación inicial y continua de los datos de registración (por ejemplo, contactos designados, direcciones) por registratario

Usuario	Propósito	Casos de uso de ejemplo	Fundamento para acceder a los datos de registración
Registratarios protegidos (por ejemplo, clientes de proveedores acreditados de servicios de privacidad/representación que se deben contactar)	Protección de datos personales	Contacto con el proveedor de servicios de privacidad/representación	Permitir el contacto con proveedores acreditados de servicios de privacidad o representación por parte de todo registratario que procure minimizar el acceso público a nombres y direcciones personales
		Contacto con el aprobador de credencial segura	Permitir el contacto con aprobadores acreditados de credenciales seguras que ofrecen servicios de registro usados por individuos o grupos bajo amenaza, usando credenciales seguras enviadas por terceros de confianza
Personal técnico de Internet (por ejemplo, administradores de DNS, de correo electrónico, sitios web y proveedores de servicios de Internet)	Resolución de cuestiones técnicas	Contacto con personal técnico de nombre de dominio	Facilitar el contacto con el personal técnico (individuo, rol o entidad) que pueda ayudar a resolver cuestiones técnicas u operativas relativas a nombres de dominio (por ejemplo, fallas de resolución del DNS, cuestiones de entrega de correos electrónicos, cuestiones funcionales de sitios web)
Autoridad de certificación	Certificación de nombres de dominio	Emisión de certificación de nombres de dominio	Ayudar a una autoridad de certificación (CA) a identificar al registratario de un nombre de dominio ligado a un certificado de SSL/TLS
Usuarios individuales de Internet (por ejemplo, consumidores)	Uso individual de Internet	Contacto con el mundo real	Ayudar a los consumidores a obtener información de contacto del registratario de un nombre de dominio que no figure en Internet (por

Usuario	Propósito	Casos de uso de ejemplo	Fundamento para acceder a los datos de registración
			ejemplo, el domicilio comercial)
		Protección del consumidor	Costear un mecanismo ligero para que los consumidores se comuniquen con el contacto comercial designado por registratarios de nombres de dominio (por ejemplo, servicio al cliente de minoristas en línea) para resolver cuestiones con rapidez, sin la intervención de LEA/OpSec
Usuarios comerciales de Internet (por ejemplo, titulares de marcas comerciales, intermediarios, agentes)	Compra o venta de nombre de dominio comercial	Venta de nombre de dominio a través de un intermediario	Permitir la averiguación de antecedentes en relación con la compra de un nombre de dominio
		Información y protección (análisis de riesgo) respecto de una marca comercial de un nombre de dominio	Permitir la identificación de registratarios de nombres de dominio para respaldar la información y protección de una marca comercial (análisis de riesgo) al crear nuevas marcas
		Adquisición de nombre de dominio	Facilitar la adquisición de un nombre de dominio previamente registrado permitiendo el contacto con el registratario
		Consulta por compra de nombre de dominio	Permitir la determinación de la disponibilidad de un nombre de dominio y del contacto del administrador o registratario actual (si lo hubiere)
		Historial de registración del nombre de dominio	Proporcionar el historial de la registración de un nombre de dominio para

Usuario	Propósito	Casos de uso de ejemplo	Fundamento para acceder a los datos de registración
			identificar registratarios y fechas anteriores mediante WhoWas
		Nombres de dominio para un registratario especificado	Permitir la determinación de todos los nombres de dominio registrados por una entidad específica (consulta inversa) como parte de una verificación de fusiones/derivaciones de activos
Investigadores de Internet	Investigación de DNS de interés público/académico	Historial de registración del nombre de dominio	Permitir la investigación histórica acerca del registro de nombres de dominio (WhoWas) durante la investigación de DNS de interés público o académico
		Nombres de dominio para un contacto especificado	Permitir la identificación de todos los dominios registrados con un nombre, una dirección, un servidor de nombres, la fecha de registro, etc., (consulta inversa) durante la investigación de DNS de interés público o académico
		Encuesta de registratarios de nombre de dominio o contacto designado	Realizar encuestas de registratarios de nombre de dominio o de sus contactos designados
Titulares de propiedad intelectual (por ejemplo, titulares de marcas comerciales, propietarios de marcas comerciales, titulares de propiedad intelectual)	Acciones legales	Contacto del usuario del nombre de dominio	Contactar a la parte que utiliza un nombre de dominio que está siendo investigado por incumplimiento en materia de marcas comerciales o robo de propiedad intelectual
		Combatir el uso fraudulento de datos de registración	Facilitar la detección del uso fraudulento de datos legítimos (por ejemplo, el domicilio) de nombres de

Usuario	Propósito	Casos de uso de ejemplo	Fundamento para acceder a los datos de registración
			dominio que pertenecen a otro registratario, y la respuesta a dicho uso fraudulento, mediante la consulta inversa de los datos validados de identidad
		Historial de registración del nombre de dominio	Permitir la investigación histórica acerca del registro de nombres de dominio (WhoWas) durante la investigación de infracción de propiedad intelectual
		Nombres de dominio para un registratario especificado	Permitir la identificación de todos los dominios registrados con un nombre o una dirección (consulta inversa) durante la investigación de infracción de propiedad intelectual
Investigadores que no pertenecen a organismos encargados del cumplimiento de la ley (por ejemplo, autoridades impositivas, proveedores de UDRP, cumplimiento contractual de la ICANN)	Cumplimiento de normas regulatorias y contratos	Investigación impositiva en línea	Facilitar la identificación de contactos de nombre de dominio que participa en ventas en línea por parte de autoridades tributarias nacionales, estaduales, provinciales o locales
		Procedimientos de UDRP	Permitir que los proveedores de UDRP confirmen cual es el demandado correcto en relación de un nombre de dominio, realicen verificaciones de cumplimiento, determinen los requisitos de los procesos legales y se protejan contra la transferencia intencional del nombre de dominio por parte del usurpador

Usuario	Propósito	Casos de uso de ejemplo	Fundamento para acceder a los datos de registración
			para evitar ser demandado (*cyberflight*)
		Cumplimiento contractual del ecosistema del RDS	Permitir que la ICANN audite y responda a los reclamos sobre la falta de cumplimiento de las partes contratadas (por ejemplo, inexactitud o falta de disponibilidad de datos, implementación de las decisiones de UDRP, transferencia de reclamos, custodia y retención de datos)
Investigadores de LEA/OpSec (por ejemplo, organismos que se encargan del cumplimiento de la ley, equipos de respuesta ante incidentes)	Mitigación de abusos relacionados con DNS e investigación criminal	Investigar nombres de dominio abusivos	Permitir la investigación efectiva y la recolección de evidencia por parte del personal de LEA/OpSec en respuesta ante un nombre de dominio supuestamente registrado en forma maliciosa, incluido el examen de datos históricos
		Investigación de actividades criminales fuera de línea	Permitir la investigación y la recolección de evidencia por parte del personal de LEA/OpSec en respuesta a actividades criminales fuera de línea mediante el suministro de datos de registración detallados o la búsqueda de nombres de dominio registrados sospechosos (consulta inversa)
		Servicios de reputación de nombres de dominio	Permitir el análisis de listas negras/blancas de nombres de dominio por parte de proveedores de servicios de reputación
		Investigación de actividades criminales en	Ayudar a las víctimas o a sus asesores legales a

Usuario	Propósito	Casos de uso de ejemplo	Fundamento para acceder a los datos de registración
		línea	identificar al registratario de un nombre de dominio involucrado en una actividad potencialmente ilícita para permitir una mayor investigación por parte de LEA/OpSec
		Contacto para informe de abusos de un nombre de dominio afectado	Ayudar a subsanar la situación de nombres de dominio afectados al ayudar al personal de LEA/OpSec a contactar al registratario o al contacto designado para lidiar con el abuso
Público en general (por ejemplo, blogueros, medios, activistas políticos)	Transparencia de DNS	Acceso público a los datos de registración	Identificar la organización "detrás" de un nombre de dominio, como comúnmente lo desea una amplia variedad de usuarios de Internet que no se refleja en casos de uso más específicos
Delincuentes (por ejemplo, los que participan en el envío de correo electrónico no deseado, DDoS, suplantación de identidad, robo de identidad, secuestro de nombre de dominio)	Actividades maliciosas en Internet	Secuestro de nombre de dominio	Recolectar datos de registración de nombres de dominio para obtener acceso ilegítimo a la cuenta de un registratario y secuestrar los nombres de dominio de ese registratario
		Registración maliciosa de un nombre de dominio	Usar la cuenta de registración un nombre de dominio existente/afectado para registrar nuevos nombres en respaldo de actividades ilícitas, fraudulentas o abusivas
		Extracción de datos de registración para usarlos en correos electrónicos	Recolectar datos del registratario de un nombre de dominio para

Usuario	Propósito	Casos de uso de ejemplo	Fundamento para acceder a los datos de registración
		no deseados o engañosos	uso malicioso por parte de quienes envían correos electrónicos no deseados, engañosos y demás delincuentes

Tabla 1: Usuarios y propósitos de RDS

c. Fines que se deben aceptar y que se deben prohibir

El EWG buscó priorizar los fines enumerados anteriormente con el fin de centrarse en el desarrollo de casos de uso y de acotar el rango de fines permisibles. Sin embargo, fue difícil establecer un fundamento para adaptar las necesidades de algunos usuarios que acceden al sistema de WHOIS actual y no las de otros, siempre y cuando sus fines no fuesen maliciosos. Este hallazgo llevó al EWG a recomendar que todos los fines permisibles identificados fuesen incorporados al RDS *de algún modo*, con excepción de actividades maliciosas conocidas en Internet que debieran ser eliminadas. Los fines permisibles recomendados por el EWG se resumen a continuación.

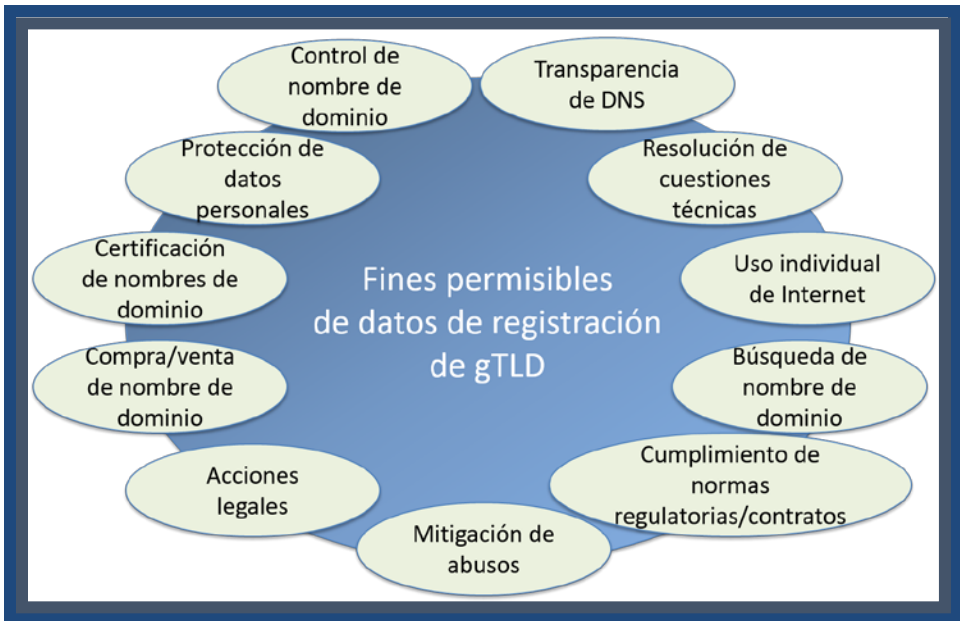


Figura 3: Fines permisibles

Cabe señalar que, dentro de cada fin, hay un número infinito de casos de uso existentes y potenciales. Si bien el EWG no intentó identificar todos los casos de uso posibles, hizo su mayor esfuerzo por analizar una muestra representativa con la esperanza de efectuar una identificación rigurosa de las clases de usuarios y sus propósitos al procurar el

acceso a los datos de registración de gTLD. Sin embargo, el RDS debe ser diseñado con la capacidad de incorporar nuevos usuarios y fines permisibles que probablemente surjan con el transcurso del tiempo.

A medida que el EWG analizó los casos de uso que se detallan en el Anexo C, fue quedando claro que muchos usuarios tienen necesidades de obtener elementos de datos similares, pero con propósitos distintos. Algunas de estas necesidades son comprensibles, por ejemplo:

- La capacidad de determinar si un nombre de dominio se encuentra registrado
- La capacidad de determinar el estado actual de un dominio
- La capacidad de ponerse en contacto con alguien respecto del nombre de dominio

Sin embargo, algunas necesidades son comunes y, aun así, no se ven satisfechas por el sistema de WHOIS actual de manera uniforme. A continuación, se presentan algunos ejemplos:

- La capacidad de determinar todos los dominios registrados por una entidad en particular (comúnmente conocida como "WHOIS inverso")
- La capacidad de determinar la información histórica de registración de nombres de dominio (comúnmente conocida como "WhoWas")

El EWG tuvo en cuenta estas necesidades en común al desarrollar las recomendaciones para RDS detalladas en este informe. Sin embargo, dado que es probable que se identifiquen más necesidades en común con el transcurso del tiempo, el sistema para la próxima generación debe ser diseñado teniendo en cuenta la posibilidad de su ampliación. A continuación, se definen los fines permisibles identificados actualmente y las necesidades asociadas de consultas, contacto y datos de registración del EWG.

Propósito	Definición
Control de nombre de dominio	Las tareas incluidas en el alcance de este propósito son la creación, la administración y la supervisión del nombre de dominio (DN) del registratario, incluso la actualización de información relacionada con el DN, la creación, la transferencia, la renovación, la eliminación y el mantenimiento del portfolio de DN, además de la detección del uso fraudulento de la información de contacto del registratario. Esto implica que cada registratario debe ser un usuario autenticado de RDS para este propósito, con la posibilidad de acceder a toda la información pública y restricta en el RDS de su nombre de dominio, incluso los datos de contacto designados publicados en el RDS para este nombre de

Propósito	Definición
	dominio.
Protección de datos personales	Las tareas incluidas en el alcance de este propósito son la identificación del proveedor acreditado de servicios de privacidad/representación asociado con un nombre de dominio por el cual se informa un abuso, se solicita la divulgación de datos relacionados o se contacta al proveedor en cuestión. Para realizar estas tareas, el usuario debe ponerse en contacto de forma confiable y sencilla con el proveedor de servicios de privacidad/representación, por ejemplo, siguiendo la URL con abuso del PBC de un proveedor de servicios de privacidad/representación a una página que describa el proceso de revelación del proveedor o permita al usuario enviar un formulario de solicitud de revelación.
Resolución de cuestiones técnicas	Las tareas incluidas en el alcance de este propósito son el trabajo para resolver cuestiones técnicas asociadas con el uso de nombres de dominio, incluso problemas asociados con el envío de correos electrónicos, fallas de resolución de DNS y problemas técnicos de sitios web. Para realizar estas tareas, el usuario debe tener la posibilidad de ponerse en contacto con el personal técnico responsable del manejo de estos temas. (Nota: Puede resultar útil designar varios puntos de contacto para afrontar diferentes tipos de problemas, por ejemplo, un administrador de correo para problemas relacionados con el correo electrónico).
Certificación de nombres de dominio	Entre las tareas del alcance de este propósito, se incluye que una autoridad de certificación (CA) emita un certificado X.509 para un sujeto identificado por un nombre de dominio. Para realizar esta tarea, el usuario tiene que confirmar que el nombre de dominio esté registrado en el sujeto de verificación. Esto requiere acceso a todos los datos públicos y restrictos del registratario.
Uso individual de Internet	Las tareas incluidas en el alcance de este propósito son la identificación de la organización que utiliza el nombre de dominio para generar confianza en los consumidores o el contacto con la organización para hacerle llegar el reclamo de un cliente o la documentación de un reclamo acerca de esta. Para realizar estas tareas, el usuario necesita el nombre de la organización (preferiblemente, validado por la identidad) y su dirección postal, y puede beneficiarse de seguir una URL de contacto a una página que describa la organización y sus contactos de servicio al cliente o que le permita al usuario enviar una solicitud de servicio al cliente.

Propósito	Definición
Compra o venta de nombre de dominio comercial	Las tareas incluidas en el alcance de este propósito son la realización de consultas de compras relacionadas con nombres de dominio, la adquisición de un nombre de dominio de otro registratario y la investigación de diligencia debida. Para realizar estas tareas, el usuario debe tener acceso a la organización y la dirección de correo electrónico del registratario, y en algunos casos, a los datos restrictos adicionales, por ejemplo, para realizar una consulta inversa respecto del nombre de un registratario o contacto para determinar otros nombres de dominio con los que están asociados.
Investigación de DNS de interés público/académico	Las tareas incluidas en el alcance de este propósito son la realización de estudios de investigación de interés público/académico acerca de nombres de dominio publicados en el RDS, incluso información pública acerca del registratario y los contactos designados, el estado y el historial del nombre de dominio y los nombres de dominio registrados por un registratario dado (consulta inversa). Para realizar estas tareas, el usuario debe poder acceder a todos los datos públicos del RDS y, en algunos casos, es posible que necesite acceso a los datos restrictos para su uso de manera anónima, como compilación.
Acciones legales	Las tareas incluidas en el alcance de este propósito son la investigación de posibles usos fraudulentos del nombre o la dirección de un registratario por parte de otros nombres de dominio, la investigación de posibles infracciones de marca, el contacto con un representante legal del registratario/licenciatario antes de llevar a cabo acciones legales si la cuestión no se aborda correctamente. Para realizar estas tareas, el usuario debe ponerse en contacto con el representante legal del registratario/licenciatario, sin la intermediación de un proveedor de servicios de privacidad/representación.
Cumplimiento de normas regulatorias/contratos	Las tareas incluidas en el alcance de este propósito son la investigación de autoridades tributarias de negocios con presencia en línea, la investigación de UDRP, la investigación de cumplimiento contractual y las auditorías de custodia de datos de registración. Para lograr esto, el usuario necesita tener acceso a algún tipo de contacto restricto del registratario o elementos de datos de nombre de dominio, como la dirección postal y número de teléfono, según sea apropiado para los propósitos indicados. Por ejemplo, la WIPO puede requerir acceso a una resolución de UDRP.
Mitigación de abusos relacionados con DNS e investigación criminal	Las tareas incluidas en el alcance de este propósito son elaborar un informe de abusos a quien pueda investigar y enfrentar dicho abuso o el contacto con entidades asociadas con ese nombre de dominio durante una investigación criminal fuera de línea. Para realizar estas tareas, el usuario acreditado (por ejemplo, un agente del orden público, el primer respondedor) tiene que llegar de forma rápida y confiable al contacto para informe de abusos responsable del nombre de dominio asociado, por ejemplo, siguiendo una URL a una descripción

Propósito	Definición
	del proceso de informes de abuso o un formulario de notificación de incidentes.
Transparencia de DNS	Las tareas incluidas en el alcance de este propósito son la consulta de datos de registración publicados por registratarios para cumplir con una variedad de necesidades de informar al público en general. Para realizar estas tareas, el usuario necesita fácil acceso a los datos públicos (y solamente datos públicos) que puede suministrar el RDS. Los registratarios deben saber que es posible que sus datos públicos de registración de nombre de dominio se utilicen para este propósito abarcativo y dicho propósito debe limitarse a datos públicos (es decir, el propósito NO permite el acceso a datos restrictos).

Tabla 2: Definiciones de propósitos

El alcance de los datos de registración necesarios para el cumplimiento de estos propósitos se resume en la siguiente tabla, que incluye los nombres de dominio en cuestión, los tipos de datos necesarios (datos del registratario, datos de contacto, datos de nombre de dominio) y las consultas adicionales necesarias.

Propósito	Alcance de la consulta	Contactos necesarios	Datos necesarios del registratario	Datos de DN	Otras consultas necesarias
Control de nombre de dominio	DN propio	Todos	Públicos+restrictos	Sí	Inversa (datos propios) WhoWas (DN propio)
Protección de datos personales	DN PP*	PP	Público	Sí	Ninguna
Resolución de cuestiones técnicas	Cualquier DN	Técnicos	Públicos	Sí	Ninguna
Certificación de nombres de dominio	Cualquier DN	Ninguno	Públicos+restrictos	Sí	Ninguna
Uso individual de Internet	DN LP*	Comerciales	Públicos	No	Ninguna
Compra o venta de nombre de dominio comercial	Cualquier DN	Administrativos	Públicos+ restrictos aprobados	Sí	Inversa (datos aprobados) WhoWas (cualquier DN)
Investigación de DNS de interés público/académico	Cualquier DN	Todos	Públicos+ restrictos aprobados	Sí	Inversa (datos aprobados) WhoWas (cualquier DN)
Acciones legales	Cualquier DN	Legales	Públicos+ restrictos aprobados	Sí	Inversa (datos aprobados) WhoWas (cualquier DN)
Cumplimiento de normas regulatorias/contratos	Cualquier DN	Legales	Públicos+restrictos	Sí	Inversa (cualquier dato) WhoWas (cualquier DN)
Mitigación de abusos	Cualquie	Abuso	Públicos+restr	Sí	Inversa (cualquier dato)

relacionados con DNS e investigación criminal	r DN	ictos		WhoWas (cualquier DN)
Transparencia de DNS	Cualquier DN	Públicos	Sí	Ninguna

Tabla 3: Alcance de los datos de registración necesarios para cada propósito

En la Tabla 3, los "datos restrictos aprobados" podrían definirse por los términos del servicio que los usuarios acreditados de RDS pueden solicitar, sujetos a las políticas definidas, que incluyen:

- Quién califica para el acceso restricto
- Motivos legítimos para solicitar esos datos
- Límites en el uso de esos datos
- Supervisión requerida para garantizar el uso adecuado

Estos propósitos que requieren "datos restrictos aprobados" se deben analizar con mayor detenimiento, en consulta con las comunidades de usuarios de RDS, para determinar cómo podrían definirse, implementarse y ejecutarse razonablemente tales políticas, equilibrando las necesidades de responsabilidad y privacidad. Sin embargo, para ilustrar cómo podría funcionar esto, se ofrecen los siguientes ejemplos:

- La **investigación de DNS de interés público/académico** puede incluir a un investigador de una universidad reconocida, dedicado a un estudio específico de DNS, que enumere los elementos de datos restrictos necesarios y cómo se los utilizará, que acuerde publicar los resultados solamente de manera anónima y en una compilación, en virtud de la supervisión de la Junta de Revisión Independiente (IRB). El usuario acreditado de RDS, aprobado para llevar a cabo la "investigación de DNS de interés público", puede acceder a determinados elementos de datos restrictos del registratario o puede consultarlos mediante una consulta inversa.
- La **investigación de compra/venta de DNS** puede incluir al usuario comercial, centrado en una transacción comercial que requiere diligencia debida de los activos de nombres de dominio del vendedor. Con el seguimiento y la supervisión por parte de un organismo de acreditación (que se define en la Sección IV (c), Acreditación de usuarios de RDS), este usuario puede asegurar que no solamente están involucrados en la compra de un nombre de dominio, sino que además se necesitan datos de RDS para permitir la debida diligencia sobre el vendedor X y los resultados se utilizarán únicamente para este propósito

específico. El usuario de RDS acreditado, con la aprobación de utilizar el DNS para realizar este tipo de debida diligencia, puede usar consultas inversas para buscar nombres de dominio con los datos restrictos vinculados al vendedor X, como se describe con más detalles en el Anexo E.

- La investigación de **acciones legales** puede incluir la participando en un abogado que trabaje en investigaciones de infracciones de marca. Con el seguimiento y la supervisión por parte de un organismo de acreditación (que se define en la Sección IV (c), Acreditación de usuarios de RDS), este usuario puede asegurar que no solamente está investigando posibles acciones legales, sino que además se necesitan datos de RDS para permitir la investigación sobre el vendedor Y y los resultados se utilizarán únicamente para este propósito específico. El usuario de RDS acreditado, con la aprobación de utilizar el DNS para realizar este tipo de investigación de infracción de marca, puede usar consultas inversas para buscar nombres de dominio con los datos restrictos vinculados al vendedor Y, como se describe con más detalles en el Anexo E.

Para ilustrar los datos involucrados en estos propósitos, el papel de los datos restrictos aprobados y las garantías que se podrían aplicar para incriminar a los usuarios responsables e impedir el abuso, consulte el Anexo E, Ilustraciones de acceso restricto y no autenticado.

Este análisis de fines permisibles y de usuarios de RDS condujo al EWG a formular los siguientes principios fundamentales para permitir el acceso con un propósito a los datos de registración:

N.º	Principios de fines permisibles
1.	La ICANN debe publicar, en un solo lugar, una política sencilla que describa el propósito y los usos permitidos de los datos de registración, para informar con claridad a los registratarios por qué se están recopilando estos datos y cómo van a ser manipulados y empleados.
2.	Los usos permisibles/no permisibles de RDS deben estar claramente definidos.
3.	El RDS deben admitir fines permisibles definidos, incluidos los usos que implican: • Identificar al registratario y los contactos designados para un propósito dado; • Comunicarse con contactos designados para un propósito dado;

	• Usar los datos publicados por los registros acerca de nombres de dominio; y • Buscar elementos de datos de registración necesarios para un propósito dado.
4.	El RDS debe ser diseñado con la capacidad de incorporar nuevos usuarios y fines permisibles que probablemente surjan con el transcurso del tiempo. • Se debe definir un proceso de solicitudes. • Las solicitudes se deben revisar en virtud de criterios definidos. • Las solicitudes que aprueban la revisión deben ser evaluadas y aprobadas por un comité de revisión de múltiples partes interesadas según lo determinado por el proceso de desarrollo de políticas. • Las solicitudes aprobadas se deben agregar a la política de privacidad de RDS y se las debe programar a fin de implementarlas de manera periódica (por ejemplo, una vez por año o por trimestre) según lo definido en la política. Nota: Consulte la Sección VI, Elementos de datos para conocer el proceso de agregar nuevos elementos de datos.
5.	Todos los fines permisibles identificados se deben incorporar al RDS *de algún modo*, con excepción de actividades maliciosas conocidas en Internet que debieran ser eliminadas. Los fines permisibles recomendados por el EWG se resumen en la Tabla 1, Usuarios y propósitos de RDS, y en la Figura 3, Fines permisibles.
6.	Los datos de registración de gTLD deberían ser recolectados, validados y divulgados únicamente con fines permisibles, con ciertos elementos de datos accesibles únicamente a solicitantes autorizados y responsables usarlos apropiadamente.
7.	Todos los registratarios deben poder acceder a la información pública y restricta que publique el RDS respecto de su nombre de dominio, incluso los datos de contacto designados.

d. Partes interesadas involucradas en el RDS

En la tabla que figura a continuación, se presenta un resumen representativo de la gama de partes interesadas involucradas en la recolección, el almacenamiento, la divulgación y el uso de datos de registración de gTLD, asignados según los propósitos relacionados.

Algunas partes interesadas suministran datos (por ejemplo, los registratarios), mientras que otras recolectan/almacenan datos (por ejemplo, los validadores, registradores, registros) o los divulgan (por ejemplo, el proveedor de RDS, proveedores acreditados de servicios de privacidad/representación). Sin embargo, la mayoría de las partes interesadas son partes involucradas en el inicio de solicitudes de datos (por ejemplo, propietarios de marcas comerciales o sus agentes) o partes identificadas, contactadas o impactadas de algún otro modo por la divulgación de datos (por ejemplo, contactos designados para informe de abusos de nombres de dominio). El presente resumen tiene por objeto ilustrar la amplia gama de partes interesadas más probablemente afectadas por el RDS. Sin embargo, en toda transacción que implique datos de registración, puede haber partes interesadas adicionales que no se enumeren a continuación.

Partes interesadas	Propósitos
Contacto designado en caso de abuso del nombre de dominio	Mitigación de abusos e investigación criminal
Compañía/sociedad compradora	Compra o venta de nombre de dominio comercial
Agentes/letrados de la compañía/sociedad compradora	Compra o venta de nombre de dominio comercial
Servicio de validación de direcciones	Control de nombre de dominio
Agentes/mandatarios del registratario	Control de nombre de dominio
Propietario de marca comercial	Cumplimiento efectivo de normas regulatorias/contratos
Proveedor de servicio de gestión de marca comercial	Control de nombre de dominio
Propietario de marca comercial	Compra o venta de nombre de dominio comercial
Autoridad de certificación	Certificación de nombres de dominio
Reclamante/demandante	Cumplimiento efectivo de normas regulatorias/contratos
Consumidores que adquieren productos mediante sitios web	Uso individual de Internet
Usuarios de Internet que visitan sitios web	Uso individual de Internet
Corredor de dominios	Compra o venta de nombre de dominio comercial
Comprador de dominio	Compra o venta de nombre de dominio comercial
Víctima de fraude	Acciones legales
Agente/mandatario de víctima de fraude	Acciones legales
Personal de organismo gubernamental	Cumplimiento efectivo de normas regulatorias/contratos
Cumplimiento de la ICANN	Cumplimiento efectivo de normas regulatorias/contratos
Junta de revisión independiente (IRB)	Investigación de DNS de interés público/académico
Proveedores de Servicios de Internet	Resolución de cuestiones técnicas Mitigación de abusos e investigación criminal
Investigador	Uso individual de Internet
Personal de organismos encargados del cumplimiento de la ley	Mitigación de abusos e investigación criminal Acciones legales
Contacto de proveedor de servicios de privacidad/representación listado	Protección de datos personales Control de nombres de dominio Investigación de DNS de interés público/académico

Contactos técnicos listados	Resolución de cuestiones técnicas Control de nombre de dominio Investigación de DNS de interés público/académico
Contactos administrativos listados	Cumplimiento efectivo de normas regulatorias/contratos Compra o venta de nombre de dominio Control de nombre de dominio Investigación de DNS de interés público/académico
Contactos legales listados	Acciones legales Cumplimiento efectivo de normas regulatorias/contratos Investigación de DNS de interés público/académico
Contactos comerciales listados	Uso individual de Internet Control de nombre de dominio Investigación de DNS de interés público/académico
Contactos relacionados con abuso listados	Mitigación de abusos e investigación criminal Control de nombre de dominio Investigación de DNS de interés público/académico
Proveedor de servicios en línea	Resolución de cuestiones técnicas
Proveedores de servicios de seguridad operativa	Mitigación de abusos e investigación criminal
Organismo que patrocina un estudio	Investigación de nombre de DNS de interés público
Persona/entidad que está siendo investigada	Cumplimiento efectivo de normas regulatorias/contratos
Cliente de servicios de privacidad/representación	Compra o venta de nombre de dominio comercial Control de nombre de dominio Resolución de cuestiones técnicas Cumplim normas regulatorias/contratos Pr personales
Proveedor de servicios de privacidad/representación	Mitigación de abusos e investigación criminal o venta de nombre de dominio comercial C nombre de dominio de interés público R Acciones legales Protección de datos personales Cumplimiento efectivo de normas regulatorias/contratos Reso técnicas
Proveedor de RDS	Todos los propósitos
Registratario	Todos los propósitos
Contacto legal del registratario	Acciones legales Cumplimiento efectivo de normas regulatorias/contratos
Registrador	Compra o venta de nombre de dominio comercial Control de nombre de dominio Investigación de nombre de DNS de interés público U Internet Accion personales Cumplim regulatorias/contratos Reso técnicas Mitigación de abusos e investigación criminal
Registro	Todos los propósitos

Informante de un problema	Resolución de cuestiones técnicas
Investigador	Investigación de DNS de interés público/académico
Revendedor	Control de nombre de dominio Mitigación de abusos e investigación criminal
Resolutor de un problema	Resolución de cuestiones técnicas
Destinatario de acciones legales/civiles	Uso individual de Internet
Terceros que buscan contacto	Acciones legales Protección de datos personales
Aprobador de credencial segura	Protección de datos personales
Destinatario de credencial segura	Protección de datos personales
Panelistas de UDRP	Cumplimiento efectivo de normas regulatorias/contratos
Proveedor de UDRP	Cumplimiento efectivo de normas regulatorias/contratos
Validador	Todos los propósitos
Víctima de abuso	Mitigación de abusos e investigación criminal
Proveedor de servicios de alojamiento en la Web	Resolución de cuestiones técnicas

Tabla 4: Resumen representativo de las partes interesadas

e. Principios de contactos con un propósito

La existencia y el uso de nombres de dominio de Internet en zonas públicas crean potenciales efectos externos en terceros en todo el mundo. Desde conductas de abuso hasta problemas técnicos e incumplimiento de derechos y problemas de nombres de dominio grandes y pequeños, hay miles de razones por las cuales un tercero de cualquier lugar del mundo puede tener una necesidad legítima de ponerse en contacto con una persona o una organización asociada con un nombre de dominio en particular.

Al mismo tiempo, los registratarios de nombres de dominio pueden desear privacidad y tener derecho a ella (dependiendo de su jurisdicción local). Probablemente no deseen que sus detalles de contacto sean públicos. Además, los registratarios a menudo no son la mejor persona o entidad para resolver cualquier asunto que pueda plantear un tercero, como problemas relacionados con la configuración de DNS de un nombre de dominio o responder a una disputa de marca. Por lo tanto, solo suministrar información del registratario probablemente sea insatisfactorio para terceros que buscan resolver problemas asociados con un nombre de dominio.

La naturaleza diversa de los posibles problemas requerirá respuestas diferentes —tanto en el contenido como en el tiempo— a situaciones que a menudo son lógicamente resueltas por diferentes personas u organizaciones asociadas a un dominio particular. Sin embargo, como mínimo, cualquier nombre de dominio debe tener uno o más contactos públicos, publicados, precisos y disponibles que respondan a consultas externas y sirvan de punto de referencia para fines permisibles de actores externos, que se vean afectados por la existencia de un nombre de dominio o por sus operaciones.

La puntualidad a la hora de responder puede ser un objetivo deseado para la elaboración de políticas para algunos tipos de contacto en particular. No obstante, el objetivo debe ser el equilibrio respecto de las cargas que puedan imponer los requisitos de respuesta en las entidades que cumplan esas funciones. El provecho indebido, las solicitudes inadecuadas o la sobrecarga intencional de contactos no deben generar penalidades para esos contactos. Es aconsejable que los solicitantes tengan un proceso para escalar toda comunicación insatisfactoria con un contacto que no responda para ciertos propósitos (por ejemplo, que se ocupe de cuestiones de abuso, que responda a presentaciones de UDRP). La falta de respuesta a un proceso de este tipo podría dar lugar a la suspensión o la cancelación de ese contacto y de los nombres de dominio que puedan resultar afectados en un proceso codificado. Sin embargo, en este informe no se abarcan los objetivos específicos de las políticas de puntualidad de respuesta.

N.º	Principios de contactos con un propósito
8.	Se debe proporcionar al menos un contacto con un propósito (PBC) por cada nombre de dominio registrado, lo que hace pública la unión de todos los elementos de datos obligatorios de todos los PBC obligatorios. Este PBC debe ser sintácticamente preciso y se lo debe poder contactar para satisfacer las necesidades de todos los fines permisibles codificados.
9.	En el proceso de registración del nombre de dominio, el ID de contacto del registratario[6] se debe utilizar como ID de PBC predeterminado para cada propósito. El registratario deberá ser informado de todos los fines permisibles y debe poder publicar otros ID de PBC para cada propósito, incluso el reemplazo del ID de contacto del registratario para todos los propósitos.
10.	El contacto con un propósito no tiene por qué ser registratario y el acceso a la información del registratario puede estar altamente restringida según otras políticas. Tenga en cuenta que un PBC no es necesariamente una persona, sino más bien un punto de contacto designado para diversos propósitos.
11.	No se debe activar (colocar en el DNS global) un nombre de dominio hasta que se proporcione un ID de PBC válido para cada propósito aplicable. Si un PBC no es válido para el propósito establecido, debe comenzar un proceso que le

[6] Los ID de contacto son identificadores asociados con bloques de datos de contacto para permitir la recuperación y la actualización; se presentan en la Sección IV (a), Elementos de datos, y se los define en la Sección V (d), Marco operativo para ID de contacto.

N.º	Principios de contactos con un propósito
	permita al registratario especificar un nuevo contacto válido, que posibilite enviar una notificación en un plazo razonable para actualizar el ID de PBC. En virtud del Principio 9 mencionado anteriormente, el ID de contacto del registratario se debe utilizar como ID de PBC predeterminado para cada propósito. Si no se proporciona un ID de PBC válido pasado ese tiempo, se podría generar la suspensión o cancelación del nombre de dominio en un proceso codificado. (Consulte la Sección V para conocer los requisitos de validación).
12.	Los ID de PBC se pueden proporcionar opcionalmente para cada fin permisible, con distintos requisitos definidos para los elementos de datos que se deben recopilar y publicar para cada tipo de PBC con el fin de satisfacer las necesidades de los fines permisibles asociados.
13.	Se debe desarrollar un proceso y políticas que permitan que los contactos designados por el registratario puedan aceptar o rechazar que se publiquen sus ID de contacto como ID de PBC para nombres de dominio, a fin de respetar los derechos de las personas y las entidades a aceptar o rechazar la responsabilidad de servir en funciones específicas para registraciones de dominios particulares.
14.	Cualquier sistema para proporcionar "contactos con un propósito" debe ser flexible y permitir la creación y la publicación de nuevos propósitos y tipos de contacto en el RDS. (Consulte la Sección III (c) para conocer más detalles sobre la incorporación de nuevos propósitos).

f. Roles y responsabilidades de contactos con un propósito

Como se resume en la Figura 4 y se detalla en la Tabla 1, el EWG analizó casos de uso representativos para identificar los tipos de usuarios que desean acceder a los datos de registración de gTLD y los fines permisibles que actualmente permiten esos datos. Para brindar acceso con un propósito a datos de registración, se asignaron a PBC todos los fines permisibles. Por ejemplo:

- Se puede designar un contacto legal para manejar las disputas en materia de marcas comerciales u otros reclamos legales relacionados con nombres de dominio. Para permitir el contacto por propósitos asociados, este PBC solamente tiene una dirección física para recibir avisos legales, una dirección de correo electrónico activa para recibir solicitudes de información y un número de teléfono o de fax laboral para recibir consultas.

- Puede designarse un contacto para cuestiones relacionadas con abuso a fin de manejar todas las consultas en materia de comportamiento abusivo por parte de un dominio y que se manifiesten en tráfico u otras actividades maliciosas de Internet muy sensibles al tiempo. Para permitir el contacto por propósitos asociados, este PBC solamente tiene una dirección de correo electrónico activa para recibir y responder reclamos válidos, y un número de teléfono para recibir consultas. El PBC también puede incluir redes sociales y direcciones de mensajería instantánea para facilitar la interacción en tiempo real, una dirección física o un número de fax para recibir consultas y una URL publicada que facilite la denuncia de abusos.

También se recomiendan los PBC para designar contactos comerciales, administrativos, técnicos y proveedores acreditados de servicios de privacidad/representación. En la Tabla 5, se proporciona una lista completa de las responsabilidades y los tipos de PBC. Asimismo, puede consultar el Principio 20 de la Sección IV, Recopilación de datos, para conocer las necesidades de elementos de datos de cada tipo de PBC.

Como se muestra en la siguiente figura, el EWG recomienda que se utilice el ID propio del registratario si no se proporcionan PBC más específicos para un nombre de dominio determinado. Por ejemplo, si no se ha especificado un contacto legal para un nombre de dominio, se debe informar al registratario que las partes pueden tener que contactarlo respecto de este fin permisible y se le dará la oportunidad de designar un PBC para recibir dichas solicitudes para este nombre de dominio.

Si el registratario opta por no designar un PBC, se le enviarán dichas solicitudes utilizando los datos necesarios para este propósito asociados con el ID de contacto del registratario. Si el registratario prefiere no publicar esos elementos de datos, el nombre de dominio se puede registrar por medio del proveedor acreditado de servicios de privacidad/representación. Consulte la Sección IV para leer más acerca del debate sobre PBC y principios de elementos de datos.

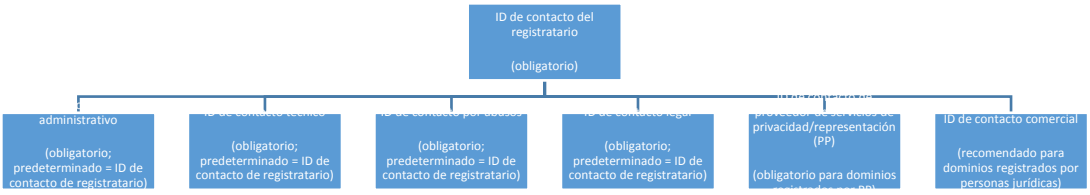


Figura 4: Tipos de contacto de RDS

Los creadores de políticas deben codificar todos los propósitos/contactos por medio de un proceso definido para agregar, cambiar o eliminar propósitos.

Este enfoque de PBC conserva la sencillez de los registratarios con necesidades básicas de contacto y ofrece granularidad adicional para los registratarios con necesidades de contacto más amplias. Para ilustrar este concepto, a continuación se presentan tres ejemplos ficticios, pero típicos:

1. Un registratario puede designar explícitamente su ID de contacto como único punto de contacto del nombre de dominio. En este caso, las consultas de RDS para todo fin permisible devolverán elementos de datos autorizados, públicos o restrictos, asociados con el ID de contacto del registratario según sea necesario para cada propósito.

Ejemplo de registro de nombre de dominio:

```
ID de contacto de registratario = <reg>
ID de contacto técnico = <reg>
ID de contacto administrativo = <reg>
ID de contacto para informe de abusos = <reg>
ID de contacto legal = <reg>
```

2. Un registratario que utilice un servicio acreditado de **privacidad** (definido en la Sección VII) puede designar varios ID de contacto únicos para su nombre de dominio, incluso un ID de contacto de proveedor de servicios de privacidad/representación (es decir, el proveedor de servicios de privacidad), un ID de contacto técnico (por ejemplo, el proveedor de alojamiento o de servicios de Internet) y también ID de contacto legal, administrativo y por abusos suministrados por el proveedor. En este ejemplo, el contacto técnico designado es responsable de resolver todas las cuestiones técnicas relacionadas con el nombre de dominio y el contacto de proveedor acreditado de servicios de privacidad/representación es responsable por todos los servicios de privacidad asociados con el nombre de dominio (incluido el reenvío de mensajes de administración, abuso y legales al registratario).

Ejemplo de registro de nombre de dominio:

```
ID de contacto de registratario = <reg>
ID de contacto de PP = <pp>
ID de contacto técnico = <isp>
ID de contacto administrativo = <reg@pp>
ID de contacto por abusos = <reg@pp>
ID de contacto legal = <reg@pp>
```

3. Un registratario que optó por autoidentificarse como persona jurídica puede proporcionar varios ID de contacto únicos para un nombre de dominio dado, incluso ID de PBC legal, comercial y por abusos, específicamente asociados con este nombre de dominio. En este ejemplo, las consultas de RDS para cada uno de estos propósitos devolverán elementos de datos asociados con un ID de PBC especializado correspondiente, lo que facilita el contacto directo con la persona o la entidad que haya asumido la responsabilidad del rol designado. Con el paso del tiempo, este escenario puede volverse más común a medida que las organizaciones aprovechen esta granularidad para mejorar la capacidad de contacto y para reducir la falta de comunicación y el redireccionamiento.

Ejemplo de registro de nombre de dominio:

```
ID de contacto de registratario = <reg>
ID de contacto técnico = <isp>
ID de contacto administrativo = <admin@reg>
ID de contacto para informe de abusos = <abuse@reg>
ID de contacto legal = <legal@reg>
ID de contacto comercial = <cs@reg>
```

Estos ejemplos se ilustran gráficamente en la siguiente figura:

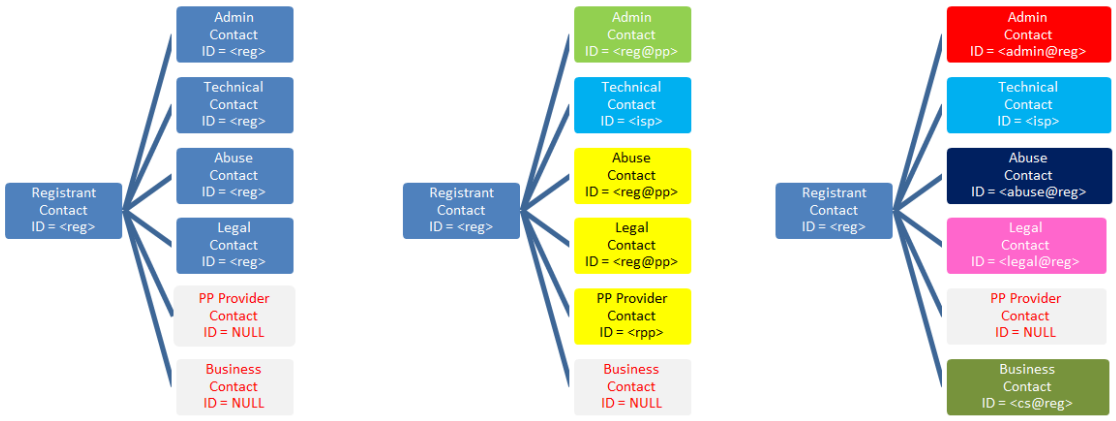


Figura 5: Ejemplo de registraciones de nombre de dominio usando contactos con un propósito

Consulte la Sección IV para obtener una lista de PBC recomendados y el Anexo D para obtener una lista completa de los elementos de datos asociados a cada fin permisible y PBC asociado.

Entre las responsabilidades del PBC, se incluye la recepción de solicitudes relacionadas con el nombre de dominio, la evaluación de dichas solicitudes y el acuse de recibo de la solicitud o la notificación al registratario/licenciatario, en virtud del acuerdo contractual entre el registratario y el PBC.

Las posibles responsabilidades de los PBC se pueden resumir de la siguiente manera:

Tipo de PBC	Posibles responsabilidades
Administrativo	Encargarse de solicitudes relacionadas con la adquisición o la venta de nombres de dominio, como preguntas sobre compra y transferencias de nombres de dominio.
Legal	Encargarse de solicitudes relacionadas con un nombre de dominio por parte de autoridades tributarias, investigadores de UDRP, investigadores de cumplimiento contractual y representantes legales.
Técnico	Encargarse de solicitudes relacionadas con un nombre de dominio respecto de problemas de baja de sitios web, problemas de DNS, problemas de entrega de correo, etc.
Abuso	Encargarse de informes de abuso de DNS en relación con un nombre de dominio, incluso casos de phishing, correo no deseado y otras actividades dañinas de Internet.
Privacidad/representación	Encargarse de solicitudes de retransmisión y revelación, presentación de reclamos por abusos de nombres de dominio por parte del registratario/licenciatario, cumplimiento con investigaciones de LEA de actividades criminales.
Comercial	Encargarse de solicitudes de información por parte de consumidores respecto de un negocio e información para contactar a la empresa a fin de obtener más detalles o para resolver quejas de clientes.

Tabla 5: Posibles responsabilidades de los contactos con un propósito

Para su futura consideración: Se pueden especificar varios PBC para cada tipo de PBC, lo que permite tener contacto directo con individuos específicos con responsabilidades críticas. Por ejemplo, para tener una gran presencia en Internet, se aconseja dividir las cuestiones técnicas entre el administrador de correo, el operador de DNS, el administrador de web, etc. Las funciones ejercidas por esos contactos especializados serían etiquetadas en un campo que se publicaría en los datos públicos para identificar el propósito específico del PBC según lo designado por el registratario. Por el momento, no puede garantizarse esta complejidad, pero no se la debe descartar para el futuro.

g. Autorización de uso de contacto de RDS

Como se describió anteriormente, las registraciones de nombres de dominio deben designar al menos los PBC mínimos y necesarios. Esos contactos deben conocer los roles designados y acordar cumplirlos para cada nombre de dominio registrado. Los principios asociados con este concepto se detallan a continuación.

N.º	Principios de autorización de uso de contactos con un propósito
15.	Debe ser posible obtener la aprobación de cada PBC en tiempo real o casi en tiempo real, de manera escalable a fin de no retrasar la registración de nombres de dominio o los cambios de nombres de dominio.
16.	Las políticas y los procesos deben evitar el uso no autorizado de PBC.
17.	El PBC o el registratario debe poder rescindir la aprobación más tarde. (Consulte la Sección V, Validación de detalles).
18.	Los registratarios deben estar facultados para designarse fácilmente como PBC para sus nombres de dominio sin la aprobación de un tercero o una parte externa.

Por ejemplo, un registratario suministra un ID de contacto de PBC y una credencial de seguridad de un solo uso que el validador responsable de ese ID de contacto puede verificar de forma instantánea y automática. De forma alternativa, se puede implementar un sistema de verificación por correo electrónico o SMS en un proceso para obtener la autorización de contacto.

IV. Mejora de la responsabilidad

El RDS recomendado utiliza un enfoque de tabla rasa y abandona el sistema de WHOIS de talla única para todos en favor del acceso con un propósito para los datos validados con la esperanza de mejorar la privacidad, la precisión y la responsabilidad.

El EWG cree que este paradigma de acceso restricto puede mejorar la responsabilidad de todas las partes involucradas en la divulgación y el uso de datos de registración de gTLD. En primer lugar, el RDS registra todo acceso a los datos de registración de gTLD, incluso el acceso no autenticado a los elementos de datos públicos y las restricciones de acceso para impedir la recolección masiva de datos. Además, el acceso restricto a elementos de datos más confidenciales estaría disponible únicamente para los solicitantes que hayan solicitado y recibido credenciales para ser utilizadas en la autenticación de consultas al RDS. Por último, el RDS audita el acceso a datos restrictos y públicos para minimizar el abuso y aplicar penalidades y otras medidas por uso inadecuado. Podrán aplicarse distintos términos y condiciones a los distintos propósitos.

Se deberían aplicar penalidades ante un incumplimiento de los términos y las condiciones por parte de los solicitantes.

Muchos miembros de la comunidad de la ICANN han expresado su preocupación por el abandono del WHOIS público totalmente anónimo en favor del paradigma de acceso restricto recomendado por el EWG. Hay quienes sugirieron que todos los datos de registración deben seguir siendo públicos para solicitantes totalmente anónimos, mientras que otros sugirieron que muy pocos datos (o ninguno) deberían ser públicos. Algunos apoyaron el concepto de acreditación de usuarios que solicitan acceso para fines permisibles, pero pidieron detalles adicionales de los elementos de datos disponibles, de los procesos de acreditación y de cómo se establecerían y se perfeccionarían con el tiempo las políticas relacionadas con los fines permisibles. Aunque no hay una respuesta fácil para satisfacer estos diversos puntos de vista, en esta sección se detallan las recomendaciones del EWG en estas áreas.

a. Principios de elementos de datos

El EWG recomienda los siguientes principios para clasificar los elementos de datos.

N.º	Principios de elementos de datos
19.	El RDS debe incorporar la divulgación de elementos de datos con un propósito. (Consulte la Sección III para obtener una lista de fines permisibles y contactos con un propósito asociados [PBC]).
20.	No todos los datos recolectados han de ser públicos; la divulgación debe depender del solicitante y el propósito.
21.	Debe estar disponible el acceso público a un conjunto mínimo de datos identificados, incluso los datos de PBC publicados expresamente a fin de facilitar la comunicación para este propósito.
22.	Los elementos de datos considerados de alta sensibilidad (una vez efectuado el análisis de riesgo e impacto) deben estar protegidos mediante acceso restricto, sobre la base de lo siguiente: • Identificación de un fin permisible • Divulgación del solicitante/el propósito • Auditoría/cumplimiento contractual para garantizar que no se haga uso abusivo del acceso restricto
23.	Solamente deben ser divulgados los elementos de datos permitidos para el propósito declarado (es decir, aquellos devueltos en respuestas o buscados mediante consultas inversas o WhoWas).

N.º	Principios de elementos de datos
24.	Los únicos elementos de datos que deberían ser recolectados son los que tienen al menos un fin permisible.
25.	Cada elemento de datos debe estar asociado con un conjunto de fines permisibles. • En este informe (consulte la Sección III y el Anexo D), se identifica un conjunto inicial de usos aceptables, fines permisibles y elementos de datos. • Cada fin permisible debe estar asociado con políticas de uso y el acceso a elementos de datos claramente definido. • Como se especifica en la Sección III, se debe definir un proceso de revisión continua para considerar nuevos fines permisibles y se deben actualizar fines permisibles de manera periódica para reflejar las incorporaciones aprobadas y asignarlas a elementos de datos existentes. • Se debe definir un proceso de definición de políticas para considerar nuevos elementos de datos propuestos y, cuando sea necesario, actualizar los elementos de datos definidos y asignarlos a fines permisibles existentes.
26.	La lista de elementos de datos mínimos que se deben recopilar, almacenar y divulgar debe basarse en casos de uso conocidos (reflejados en este documento) y en una evaluación del riesgo (por completar antes de la implementación de RDS).
27.	Todos los registros y los validadores deben almacenar todo el conjunto de elementos de datos que recopilen/proporcionen al RDS. (Consulte también la Sección VIII, Posibles modelos de RDS).

Paso 1: Recopilación de datos

Los datos se deben recopilar antes de que se los pueda divulgar de forma selectiva para los fines permitidos. Se recomiendan los siguientes principios para guiar la recopilación en el momento de la registración:

N.º	Principios de recopilación de datos
28.	Para apoyar los principios jurídicos generales mencionados en la Sección VI, los registradores y los validadores deben permitirles a los contactos con un propósito y a los registratarios de nombres de dominio, en el momento de la recopilación de datos, aceptar el uso de sus datos para fines permisibles ya divulgados, en virtud de las leyes de protección de datos de su jurisdicción. Al formular la política, este

N.º	Principios de recopilación de datos
	principio se debe abordar en el contexto más amplio de estos principios jurídicos generales.[7]
29.	Para satisfacer las necesidades básicas de control de dominios, debe ser obligatorio para los registros y los registradores recopilar los siguientes datos, y suministrarlos para los registratarios, cuando se registre un nombre de dominio: a. Nombre del dominio b. Servidores de DNS c. Nombre del registratario d. Tipo de registratario Indica el tipo de entidad identificada por el nombre de registratario para su uso en la aplicación de requisitos de datos de registración, de la siguiente manera: **Sin declarar**: se aplica de manera predeterminada si no se selecciona ninguna de las opciones siguientes y el RDS la debe tratar de manera similar a las personas físicas. **Proveedor de servicios de privacidad/representación**: se debe seleccionar para nombres de dominio registrados por medio de un proveedor acreditado de servicios de privacidad/representación. Cuando se la selecciona, también se debe suministrar el ID de contacto de un proveedor acreditado de servicios de privacidad/representación para permitir la escala de solicitud de retransmisión y revelación al PBC de PP. **Persona jurídica**: se debe seleccionar para nombres de dominio registrados para entidades que NO sean personas físicas NI proveedores de servicios de representación. Cuando se la selecciona, también se debe proporcionar el ID de contacto de un PBC comercial designado a fin de facilitar los reclamos y las consultas de los consumidores. (Consulte la nota que se encuentra debajo de esta tabla). **Persona física**: se puede seleccionar para nombres de dominio registrados para personas físicas. Cuando se la selecciona, no se deben definir PBC de proveedor de servicios de privacidad/representación ni PBC comerciales, y el nombre y la dirección del registratario se deben tratar como información personal en virtud de las leyes de protección de datos aplicables a la jurisdicción del asunto de los datos.

[7] Hubo un apoyo casi unánime para este texto, con un solo miembro disidente del EWG.

N.º	Principios de recopilación de datos
	e. ID de contacto de registratario Un ID único asignado a cada contacto de registratario [nombre+dirección] durante la validación (consulte la Sección V para obtener una definición más detallada del ID de contacto y de cómo se crea a través de un validador y se utiliza para la registración de nombres de dominio) f. Dirección postal del registratario Incluye los siguientes elementos de datos: Calle, ciudad, estado/provincia, código postal, país (según corresponda) g. Dirección de correo electrónico del registratario h. Número de teléfono del registratario Incluye los siguientes elementos de datos: Número y extensión (si corresponde)
30.	a. Para mejorar tanto la privacidad como la capacidad de contactar al registratario, los registradores deben recopilar y los registratarios deben proporcionar contactos con un propósito (PBC) por cada nombre de dominio registrado. b. Opcionalmente, los registratarios pueden designar PBC proporcionados por proveedores de servicios de privacidad/representación o PBC de terceros autorizados para fines permisibles especificados (consulte la Sección III). c. Para satisfacer las necesidades de comunicación asociadas con cada fin permisible, los PBC creados a través de un validador y posteriormente asociados con un nombre de dominio deben cumplir los siguientes requisitos mínimos de elementos de datos obligatorios: Contacto técnico dirección de correo electrónico Contacto administrativo: organización, dirección de correo electrónico Contacto legal: organización, dirección de correo electrónico, teléfono, dirección postal Contacto para informe de abusos: dirección de correo electrónico, número de teléfono Contacto comercial[8]: organización, dirección postal Contacto de proveedor de servicios de privacidad/representación[9]: organización, dirección de correo electrónico, URL de contacto, URL para informe de abusos

[8] El contacto es obligatorio solamente si el tipo de registratario es una persona jurídica.

[9] El contacto es obligatorio solamente si el tipo de registratario es un proveedor de servicios de privacidad/representación.

N.º	Principios de recopilación de datos
	d. Si un registratario no designa un PBC para cada fin permisible obligatorio, de manera predeterminada se debe usar el ID de contacto propio del registratario para los PBC. (Tenga en cuenta que el registratario puede evitar esto usando un proveedor acreditado de servicios de privacidad/representación o designando PBC). Cuando se utiliza el ID de contacto de un registratario como ID de PBC, es posible que aumenten los requisitos de recopilación y divulgación de datos del registratario a fin de satisfacer las necesidades de elementos de datos obligatorios de PBC establecidos anteriormente.
31.	Para evitar la recopilación de más datos de los necesarios, el resto de los datos suministrados por el registratario no enumerados en los Principios 29 o 30 y utilizados para al menos *un* fin permisible se pueden recopilar opcionalmente a discreción del registratario. Los validadores, los registros y los registradores deben permitir que estos datos se recopilen y se almacenen si así lo decide el registratario.
32.	Para maximizar la estabilidad de Internet, los siguientes elementos de datos obligatorios deben ser proporcionados al RDS por los registros y los registradores: a. Estado de registración b. Estado del cliente (fijado por el registrador) c. Estado del servidor (fijado por el registro) d. Registrador e. Jurisdicción del registrador f. Jurisdicción del registro g. Idioma del acuerdo de registro h. Fecha de creación i. Fecha de vencimiento del registrador j. Fecha de actualización k. URL del registrador l. Número de IANA del registrador m. Número de teléfono de contacto para informe de abusos del registrador n. Dirección de correo electrónico para informe de abusos del registrador o. URL de sitio de reclamos de InterNIC
33.	Para los elementos de datos específicos de TLD, el registro de TLD debe establecer y publicar una política de recopilación de datos (en consonancia con estos

N.º	Principios de recopilación de datos
	principios generales) y es responsable de toda validación de elementos de datos específicos de TLD.
34.	Los validadores, los registros y los registradores pueden recopilar, almacenar y divulgar elementos de datos adicionales para uso interno que nunca se comparta con el RDS.[10]

Nota: Después de un importante debate, el EWG no recomienda agregar el **propósito de nombre de dominio** como elemento de datos. En cambio, el EWG ha recomendado principios para lograr los objetivos asociados y un **PBC comercial** explícito para su publicación por parte de los registratarios, que se identifican a sí mismos como **personas jurídicas** que ejercen actividades comerciales. Esto podría dar lugar a que muchos usuarios comerciales de Internet publiquen de manera más uniforme los elementos de datos para impulsar la confianza de los consumidores, si bien reconocerían que los registratarios están, en última instancia, eligiendo ellos mismos esta clasificación y que sería casi imposible aplicar un cumplimiento riguroso a nivel mundial de propósitos de nombres de dominio con la diferencia entre comercial y no comercial.

Paso 2: Divulgación de datos

Después de recopilar los datos, se los puede divulgar de forma selectiva para los fines permitidos. Se recomiendan los siguientes principios para guiar la divulgación cuando se reciben consultas:

N.º	Principios de divulgación de datos
35.	Para maximizar la privacidad de los registratarios, los datos suministrados por el registratario se deben restringir de manera predeterminada, excepto cuando haya una necesidad imperiosa de acceso público que exceda el riesgo resultante. • Los registratarios pueden optar por publicar cualquier dato restricto

[10] Entre los ejemplos, se incluye la dirección IP utilizada por el cliente cuando se registró, un enlace para solicitar la generación de una clave de transferencia EPP para un nombre de dominio y los datos de pagos asociados con la cuenta del cliente. El RDS no estandariza los datos de uso interno, sino que los registros y los registradores los definen de manera privada.

N.º	Principios de divulgación de datos
	suministrado por el registratario con el consentimiento informado.
36.	Para maximizar la estabilidad de Internet, todos los datos de registración suministrados por registradores o registros deben ser siempre públicos, excepto cuando esto genere un riesgo inaceptable. • Los registratarios pueden optar por publicar los datos públicos restrictos suministrados por registratarios/registros, con la excepción que se explica a continuación para permitir el control de dominio básico.
37.	Para maximizar la capacidad de acceso, todos los PBC deben ser públicos por defecto. • Los titulares de contactos[11] pueden optar por restringir elementos de datos de PBC, a excepción de los necesarios para cumplir con el propósito designado (puede encontrar más detalles en la Tabla 5).
38.	Para satisfacer las necesidades de control de dominio básico, se deben incluir los siguientes datos suministrados por el registratario, lo cual es obligatorio para recopilar y divulgar con bajo riesgo, en el conjunto mínimo de datos públicos: a. Nombre del dominio b. Servidores de DNS c. Tipo de registratario d. ID de contacto de registratario (más detalles en la Sección V) e. Dirección de correo electrónico del registratario f. ID de contacto técnico g. ID de contacto administrativo h. ID de contacto legal i. ID de contacto para informe de abusos

[11] Según la Sección III (g), Autorización de uso de contacto de RDS, los PBC designados deben autorizar el uso de un ID de contacto en una registración de nombre de dominio. Al hacerlo, los titulares de contactos también acuerdan el uso público/restricto de sus datos para ese propósito. Sin embargo, si un PBC prevalidado no contiene los elementos de datos obligatorios/públicos para cumplir con un propósito determinado, no se puede designar el PBC para ese propósito en una registración de nombre de dominio.

N.º	Principios de divulgación de datos
	j. ID de contacto de proveedor de servicios de privacidad/representación (obligatorio solamente si el tipo de registratario es un proveedor de servicios de privacidad/representación) k. ID de contacto comercial (obligatorio solamente si el tipo de registratario es una persona jurídica)
39.	Para equilibrar la simplicidad y la accesibilidad, si un registratario no proporciona un PBC obligatorio, el registratario deberá ser informado de que su ID de contacto será utilizado como PBC y los elementos de datos del registratario serán publicados como contacto técnico, contacto administrativo, contacto legal y contacto para informe de abusos del nombre de dominio. El registratario puede evitar esta divulgación si especifica uno o más PBC de terceros o si utiliza un proveedor acreditado de servicios de privacidad/representación (en cuyo caso esas direcciones serán suministradas por el proveedor de servicios).
40.	Para los elementos de datos específicos de TLD, el registro de TLD debe establecer y publicar una política de divulgación de datos (en consonancia con estos principios generales) y es responsable de identificar fines permisibles para los elementos de datos restrictos específicos de TLD.

Clasificaciones de elementos de datos resultantes

Sobre la base de estos principios, en la tabla siguiente, se detalla la clasificación resultante de cada elemento de datos de RDS recomendado por el EWG, utilizando la siguiente notación:

- Si es (Oblig)atorio u (Op)cional recopilar cada elemento: Esto significa:

  [1] Para datos recopilados por registratarios,
  (Oblig)atorio significa que los registradores/validadores deben solicitar los datos y los registratarios deben suministrarlos, mientras que
  (Op)cional significa que el registrador/validador debe solicitar los datos, pero el registratario decide si los suministra o no, según corresponda.

  [2] Para datos recopilados por titulares de contactos con un propósito,
  (Oblig)atorio significa que los registradores/validadores deben solicitar los datos y los titulares de contactos deben suministrarlos, mientras que
  (Op)cional significa que el registrador/validador debe solicitar los datos, pero el titular de contacto decide si los suministra o no, según corresponda; y

(R)ecomendado significa que el registrador/validador debe solicitar los datos, pero el titular de contacto decide si los suministra, según corresponda, para reflejar las recomendaciones de "mejores" y "buenas" prácticas.[12]

[3] Para los datos suministrados por registros o registradores al RDS,
(Oblig)atorio significa que el registro/registrador debe suministrar los datos, mientras que
(Op)cional significa que los datos se pueden suministrar o no, según corresponda.

- Un elemento es (P)úblico (accesible para cualquiera, con autenticación o sin ella) o (R)estricto (accesible para usuarios autenticados solamente, para fines permisibles únicamente), y los registratarios pueden cambiar esa configuración predeterminada de divulgación (S/N). Esto significa:

[4] Para los datos recopilados de los registratarios:
P/N significa que los datos recopilados deben ser públicos y no se los puede ocultar;
P/S significa que los datos recopilados son públicos por defecto, pero el registratario los puede ocultar;
R/S significa que los datos recopilados son restrictos por defecto, pero el registratario los puede publicar, sin consentimiento informado.

[5] Para los datos suministrados por registros y registradores al RDS,
P/N significa que los datos suministrados deben ser públicos y no se los puede ocultar, mientras que
R/N significa que todos los datos suministrados deben ser restrictos; ningún elemento de datos se clasifica en esta categoría.

[6] Para los datos recopilados de titulares de contactos con un propósito,
P/N significa que todos los datos suministrados deben ser públicos y no se los puede ocultar,
P/S significa que todos los datos recopilados son públicos por defecto, pero el titular de contacto los puede ocultar.

[12] Las mejores prácticas recomendadas para publicar varios elementos de datos de PBC están basadas en la experiencia operativa de los miembros del EWG. Los elementos obligatorios representan un requisito operativo mínimo para llevar a cabo esos propósitos. Sin embargo, en la práctica, si existe un método de comunicación para un propósito determinado (por ejemplo, un formulario web para informar problemas, un correo electrónico alternativo para comunicarse con el personal técnico), este método alternativo es de gran utilidad y a menudo preferido para el manejo de problemas. Esto varía de PBC en PBC, por ejemplo, una dirección postal es más útil para propósitos de contacto legal o comercial y, en gran medida, inútil para resolver rápidamente propósitos de contacto técnico o para informar abusos. Por lo tanto, el EWG elaboró recomendaciones específicas para los elementos de datos de cada tipo de PBC.

Tenga en cuenta que el hecho de que los elementos de datos restrictos estén disponibles para un usuario determinado depende de los fines permisibles. Cuando un registratario opta por hacer público un elemento restricto por defecto, se vuelve accesible para todos. Cuando un registratario opta por restringir un elemento público por defecto, el acceso se limita a fines permisibles.

DATOS SUMINISTRADOS POR REGISTRO/REGISTRADOR	Recopilación (Oblig u Op)	Divulgación por defecto (P o R)	¿Se puede cambiar la divulgación?	Notas Consulte [3] Definición de recopilación y [5] Definición de divulgación
Estado de registración	**Oblig**	**P**	**N**	
Delegación de DNSSEC	Op	**P**	**N**	
Estado de cliente (registrador)	**Oblig**	**P**	**N**	Contiene todos los valores aplicables al nombre de dominio en el nivel de registrador: eliminación prohibida (DeleteProhibited), renovación prohibida (RenewProhibited), transferencia prohibida (TransferProhibited)
Estado del servidor (registro)	**Oblig**	**P**	**N**	No está en RAA; similar a lo anterior, pero en el nivel de registro
Registrador	**Oblig**	**P**	**N**	
Revendedor	Op	**P**	**N**	
Jurisdicción del registrador	**Oblig**	**P**	**N**	No está en RAA
Jurisdicción del registro	**Oblig**	**P**	**N**	No está en RAA
Idioma del acuerdo de registro	**Oblig**	**P**	**N**	No está en RAA
Fecha de creación	**Oblig**	**P**	**N**	
Fecha de registración original	Op	**P**	**N**	No está en RAA
Fecha de vencimiento del registrador	**Oblig**	**P**	**N**	
Fecha de actualización	**Oblig**	**P**	**N**	
URL del registrador	**Oblig**	**P**	**N**	
Número de IANA del registrador	**Oblig**	**P**	**N**	
Dirección de correo electrónico para informe de abusos del registrador	**Oblig**	**P**	**N**	
Número de teléfono de contacto para informe de abusos del registrador	**Oblig**	**P**	**N**	
URL de sitio de reclamos de InterNIC	**Oblig**	**P**	**N**	

DATOS DEL REGISTRATARIO recopilados del registratario	Recopilación (Oblig u Op)	Divulgación por defecto (P o R)	¿Se puede cambiar la divulgación?	Notas Consulte [1] Definición de recopilación y [4] Definición de divulgación
Nombre de dominio	**Oblig**	**P**	**N**	
Servidores de DNS	**Oblig**	**P**	**N**	
Nombre del registratario	**Oblig**	R	S	
Tipo de registratario	**Oblig**	**P**	**N**	
ID de contacto del registratario	**Oblig**	**P**	**N**	Reemplaza el ID de registratario/registro emitido por el validador en RDS
Estado de validación de contacto de registratario	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Última marca de tiempo validada de contacto del registratario	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Organización del registratario	Op	**P**	S	Recopilados cuando tipo de registratario = persona jurídica o proveedor de servicios de representación
Identificador de empresa de registratario (p. ej., nombre comercial, DUNS)	Op	**P**	S	Identificadores reales emitidos para negocios por fuentes, como Dunn y Bradstreet Recopilados cuando tipo = persona jurídica No está en RAA
Calle del registratario	**Oblig**	R	S	
Ciudad del registratario	**Oblig**	R	S	
Estado/provincia del registratario	Op	R	S	Según el RAA 2013, todos los elementos de "Estado/provincia" recopilados cuando corresponde
Código postal del registratario	Op	R	S	Según el RAA 2013, todos los elementos de "Código postal" recopilados cuando corresponde
País del registratario	**Oblig**	R	S	
Número de teléfono y extensión del registratario	**Oblig**	R	S	Extensión recopilada, si corresponde
Número de teléfono alternativo y extensión del registratario	Op	R	S	Nueva opción, no está en RAA
Dirección de correo	**Oblig**	**P**	**N**	

electrónico del registratario				
Correo electrónico alternativo del registratario	Op	**P**	S	Nueva opción, no está en RAA
Fax y extensión del registratario	Op	R	S	Según el RAA 2013, todos los elementos de "Fax" y "Fax y extensión" recopilados cuando corresponde
SMS del registratario	Op	R	S	Nueva opción, no está en RAA
Mensajería instantánea del registratario	Op	R	S	Nueva opción, no está en RAA
Redes sociales del registratario	Op	R	S	Nueva opción, no está en RAA
Redes sociales alternativas del registratario	Op	R	S	Nueva opción, no está en RAA
URL de contacto del registratario	Op	R	S	Nueva opción, no está en RAA
URL para informe de abusos del registratario	Op	R	S	Nueva opción, no está en RAA

CONTACTOS CON UN PROPÓSITO Contacto administrativo	Recopilación (Oblig, R u Op)	Divulgación por defecto (P o R)	¿Se puede cambiar la divulgación?	Notas Consulte [2] Definición de recopilación y [6] Definición de divulgación
Propósitos: Compra/venta y control de nombre de dominio, investigación de DNS				
ID de contacto administrativo	**Oblig**	**P**	**N**	
ID de PBC	**Oblig**	**P**	**N**	No está en RAA
Estado de validación de PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Última marca de tiempo validada del PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Nombre del PBC	**Oblig**	**P**	**N**	
Organización del PBC	**Oblig**	**P**	**N**	
Calle del PBC	R	**P**	S	
Ciudad del PBC	R	**P**	S	
Estado/provincia del PBC	Op	**P**	S	
Código postal del PBC	Op	**P**	S	
País del PBC	**Oblig**	**P**	**N**	
Número de teléfono y extensión del PBC	Op	**P**	S	
Número de teléfono alternativo y extensión del PBC	Op	**P**	S	No está en RAA
Correo electrónico del PBC	**Oblig**	**P**	**N**	
Correo electrónico alternativo del PBC	Op	**P**	S	No está en RAA
Fax y extensión del PBC	Op	**P**	S	
SMS del PBC	Op	**P**	S	No está en RAA
Mensajería instantánea del PBC	Op	**P**	S	No está en RAA
Redes sociales del PBC	Op	**P**	S	No está en RAA
Redes sociales alternativas del PBC	Op	**P**	S	No está en RAA
URL de contacto del PBC	Op	**P**	S	No está en RAA
URL para informe de abusos del PBC	Op	**P**	S	No está en RAA

CONTACTOS CON UN PROPÓSITO Contacto legal	Recopilación (Oblig, R u Op)	Divulgación por defecto (P o R)	¿Se puede cambiar la divulgación? 	Notas Consulte [2] Definición de recopilación y [6] Definición de divulgación
Propósitos: acciones legales, cumplimiento de normas regulatorias/contratos, investigación de DNS, control de nombres de dominio				
ID de contacto legal	**Oblig**	**P**	**N**	No está en RAA
ID de PBC	**Oblig**	**P**	**N**	No está en RAA
Estado de validación de PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Última marca de tiempo validada del PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Nombre del PBC	**Oblig**	**P**	**N**	
Organización del PBC	**Oblig**	**P**	**N**	
Calle del PBC	**Oblig**	**P**	**N**	
Ciudad del PBC	**Oblig**	**P**	**N**	
Estado/provincia del PBC	Op	**P**	S	
Código postal del PBC	Op	**P**	S	
País del PBC	**Oblig**	**P**	**N**	
Número de teléfono y extensión del PBC	**Oblig**	**P**	**N**	
Número de teléfono alternativo y extensión del PBC	Op	**P**	S	No está en RAA
Correo electrónico del PBC	**Oblig**	**P**	**N**	
Correo electrónico alternativo del PBC	Op	**P**	S	No está en RAA
Fax y extensión del PBC	**R**	**P**	**S**	
SMS del PBC	Op	**P**	S	No está en RAA
Mensajería instantánea del PBC	Op	**P**	S	No está en RAA
Redes sociales del PBC	Op	**P**	S	No está en RAA
Redes sociales alternativas del PBC	Op	**P**	S	No está en RAA
URL de contacto del PBC	Op	**P**	S	No está en RAA
URL para informe de abusos del PBC	Op	**P**	S	No está en RAA

CONTACTOS CON UN PROPÓSITO Contacto técnico	Recopilación (Oblig, R u Op)	Divulgación por defecto (P o R)	¿Se puede cambiar la divulgación?	Notas Consulte [2] Definición de recopilación y [6] Definición de divulgación
Propósitos: Resolución de cuestiones técnicas, control de nombre de dominio, investigación de DNS				
ID del contacto técnico	**Oblig**	**P**	**N**	
ID de PBC	**Oblig**	**P**	**N**	No está en RAA
Estado de validación de PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Última marca de tiempo validada del PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Nombre del PBC	R	**P**	S	
Organización del PBC	R	**P**	S	
Calle del PBC	R	**P**	S	
Ciudad del PBC	R	**P**	S	
Estado/provincia del PBC	Op	**P**	S	
Código postal del PBC	Op	**P**	S	
País del PBC	**Oblig**	**P**	**N**	
Número de teléfono y extensión del PBC	**R**	**P**	S	
Número de teléfono alternativo y extensión del PBC	**R**	**P**	S	No está en RAA
Correo electrónico del PBC	**Oblig**	**P**	**N**	
Correo electrónico alternativo del PBC	**R**	**P**	S	No está en RAA
Fax y extensión del PBC	Op	**P**	S	
SMS del PBC	**R**	**P**	S	No está en RAA
Mensajería instantánea del PBC	**R**	**P**	S	No está en RAA
Redes sociales del PBC	Op	**P**	S	No está en RAA
Redes sociales alternativas del PBC	Op	**P**	S	No está en RAA
URL de contacto del PBC	**R**	**P**	S	No está en RAA
URL para informe de abusos del PBC	Op	**P**	S	No está en RAA

CONTACTOS CON UN PROPÓSITO Contacto para informe de abusos	Recopilación (Oblig, R u Op)	Divulgación por defecto (P o R)	¿Se puede cambiar la divulgación?	Notas Consulte [2] Definición de recopilación y [6] Definición de divulgación
Propósito: Mitigación de abusos, control de nombre de dominio, investigación de DNS				
ID de contacto para informe de abusos	**Oblig**	**P**	**N**	No está en RAA
ID de PBC	**Oblig**	**P**	**N**	No está en RAA
Estado de validación de PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Última marca de tiempo validada del PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Nombre del PBC	R	**P**	S	
Organización del PBC	R	**P**	S	
Calle del PBC	R	**P**	S	
Ciudad del PBC	R	**P**	S	
Estado/provincia del PBC	Op	**P**	S	
Código postal del PBC	Op	**P**	S	
País del PBC	**Oblig**	**P**	**N**	
Número de teléfono y extensión del PBC	**Oblig**	**P**	**N**	
Número de teléfono alternativo y extensión del PBC	Op	**P**	S	No está en RAA
Correo electrónico del PBC	**Oblig**	**P**	**N**	
Correo electrónico alternativo del PBC	Op	**P**	S	No está en RAA
Fax y extensión del PBC	Op	**P**	S	
SMS del PBC	Op	**P**	S	No está en RAA
Mensajería instantánea del PBC	**R**	**P**	S	No está en RAA
Redes sociales del PBC	**R**	**P**	S	No está en RAA
Redes sociales alternativas del PBC	Op	**P**	S	No está en RAA
URL de contacto del PBC	**R**	**P**	S	No está en RAA
URL para informe de abusos del PBC	**R**	**P**	**S**	No está en RAA

CONTACTOS CON UN PROPÓSITO Contacto de proveedor de servicios de privacidad/representación (PP)	Recopilación (Oblig, R u Op)	Divulgación por defecto (P o R)	¿Se puede cambiar la divulgación?	Notas Consulte [2] Definición de recopilación y [6] Definición de divulgación
Propósitos: Protección de datos personales, control de nombres de dominio, investigación de DNS				
ID de contacto de PP	**Oblig**	**P**	**N**	No está en RAA
ID de PBC	**Oblig**	**P**	**N**	No está en RAA
Estado de validación de PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Última marca de tiempo validada del PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Nombre del PBC	**Oblig**	**P**	**N**	
Organización del PBC	**Oblig**	**P**	**N**	
Calle del PBC	**Oblig**	**P**	**N**	
Ciudad del PBC	**Oblig**	**P**	**N**	
Estado/provincia del PBC	Op	**P**	S	
Código postal del PBC	Op	**P**	S	
País del PBC	**Oblig**	**P**	**N**	
Número de teléfono y extensión del PBC	**Oblig**	**P**	**N**	
Número de teléfono alternativo y extensión del PBC	Op	**P**	S	No está en RAA
Correo electrónico del PBC	**Oblig**	**P**	**N**	
Correo electrónico alternativo del PBC	Op	**P**	S	No está en RAA
Fax y extensión del PBC	Op	**P**	S	
SMS del PBC	Op	**P**	S	No está en RAA
Mensajería instantánea del PBC	Op	**P**	S	No está en RAA
Redes sociales del PBC	Op	**P**	S	No está en RAA
Redes sociales alternativas del PBC	Op	**P**	S	No está en RAA
URL de contacto del PBC	**Oblig**	**P**	**N**	No está en RAA
URL para informe de abusos del PBC	**Oblig**	**P**	**N**	No está en RAA

CONTACTOS CON UN PROPÓSITO Contacto comercial	Recopilación (Oblig, R u Op)	Divulgación por defecto (P o R)	¿Se puede cambiar la divulgación?	Notas Consulte [2] Definición de recopilación y [6] Definición de divulgación
Propósitos: Uso individual de Internet, control de nombre de dominio, investigación de DNS				
ID de contacto comercial	**Oblig**	**P**	**N**	No está en RAA
ID de PBC	**Oblig**	**P**	**N**	No está en RAA
Estado de validación de PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Última marca de tiempo validada del PBC	**Oblig**	**P**	**N**	Nuevos, suministrados por el validador
Nombre del PBC	**Oblig**	**P**	**N**	
Organización del PBC	**Oblig**	**P**	**N**	
Calle del PBC	**Oblig**	**P**	**N**	
Ciudad del PBC	**Oblig**	**P**	**N**	
Estado/provincia del PBC	Op	**P**	S	
Código postal del PBC	Op	**P**	S	
País del PBC	**Oblig**	**P**	**N**	
Número de teléfono y extensión del PBC	R	**P**	S	
Número de teléfono alternativo y extensión del PBC	Op	**P**	S	No está en RAA
Correo electrónico del PBC	R	**P**	S	
Correo electrónico alternativo del PBC	Op	**P**	S	No está en RAA
Fax y extensión del PBC	Op	**P**	S	
SMS del PBC	Op	**P**	S	No está en RAA
Mensajería instantánea del PBC	Op	**P**	S	No está en RAA
Redes sociales del PBC	Op	**P**	S	No está en RAA
Redes sociales alternativas del PBC	Op	**P**	S	No está en RAA
URL de contacto del PBC	**R**	**P**	**S**	No está en RAA
URL para informe de abusos del PBC	Op	**P**	S	No está en RAA

El EWG también reitera su recomendación de llevar a cabo un análisis de riesgo/impacto de amplio alcance para confirmar que estas clasificaciones basadas en principios, de

hecho, dan como resultado la recopilación y la divulgación de datos adecuados para los propósitos definidos.

Consonancia con RAA 2013 y nuevos elementos de datos

Para facilitar la transición y la comprensión, los nombres de elementos de datos recomendados por el EWG se han alineado con los identificados en el RAA 2013 cuando fuere posible (por ejemplo, delegación de DNSSEC, fecha de vencimiento de RDS). Sin embargo, los nombres de los elementos de datos utilizados en el RAA 2013 para los elementos de datos de contacto no son suficientes para reflejar la propuesta del EWG para contactos con un propósito (consulte la Sección III). Para ocuparse de esto, el EWG aplicó las asignaciones siguientes:

> Cuando el ID de contacto administrativo de RDS hace referencia a un PBC,
> Nombre de PBC de RDS = Nombre de contacto administrativo de RAA
> Organización de PBC de RDS = Organización de contacto administrativo de RAA
> y así sucesivamente para otros elementos de datos de contacto administrativo de RAA
>
> Cuando el ID de contacto técnico de RDS hace referencia a un PBC,
> Nombre de PBC de RDS = Nombre de contacto técnico de RAA
> Organización de PBC de RDS = Organización de contacto técnico de RAA
> y así sucesivamente para otros elementos de datos de contacto técnico de RAA

Nota: El EWG recomienda que el portal de RDS cree definiciones para cada tipo de PBC fácilmente accesible para los usuarios de RDS (por ejemplo, definiciones de ventana emergente, movimientos del mouse) para indicar claramente que los PBC se publiquen para atender consultas relacionadas con fines permisibles y que se debe designar un punto de contacto para cubrir esos propósitos. Los registratarios pueden optar por recibir consultas ellos mismos (designar el ID de registratario como PBC), contratar a un proveedor acreditado de servicios de privacidad/representación (contratar a un PP para suministrar esos elementos de datos, por lo general, direcciones de reenvío o direcciones del proveedor) o designar una entidad específica para recibir esas consultas (por ejemplo, un proveedor de servicios, proveedor de hosting, representante legal, departamento de servicio al cliente).

Los elementos de datos se componen de lo definido en el RAA 2013, con los agregados siguientes:

Jurisdicción del registrador y registro: la jurisdicción legal en la cual opera el registrador o registro, según lo indicado en el acuerdo firmado con la ICANN.

Idioma del acuerdo de registro: el idioma en el cual se redactó el contrato del registrador con el registratario.

Fecha de registración original: la fecha en la cual el dominio se registró por primera vez.[13]

Estado del cliente, estado del servidor: estos elementos de datos, que se amplían desde los valores de estado del cliente de RAA 2013, incluyen los valores de estado del registrador (cliente) y del registro (servidor) aplicados al nombre de dominio: eliminación prohibida (DeleteProhibited), renovación prohibida (RenewProhibited), transferencia prohibida (TransferProhibited).

Identificador de empresa de registratario: el número comercial del Reino Unido, el número de DUNS u otro identificador de empresa único y real asignado al registratario por un directorio de negocios público. Esto permite buscar una empresa por fuera del RDS.

ID de contacto del registratario: un identificador único asignado a un bloque prevalidado de datos de contacto identificados como el registratario de este nombre de dominio. Consulte la Sección V para obtener una definición más detallada del ID de contacto y de cómo se lo crea y se lo utiliza. Este ID permite la reutilización y el mantenimiento de los datos de contacto en RDS. Tenga en cuenta que cuando el tipo de registratario es el proveedor de servicios de privacidad/representación, el ID de contacto del registratario refleja el identificador único asignado a ese proveedor acreditado de servicios de privacidad/representación.

Estado de validación del contacto de PBC/registratario, última marca de tiempo validada del contacto de PBC/registratario: el nivel más alto de validación alcanzado y la fecha en la cual se validó por última vez, como se define en la Sección V.

Redes sociales, mensajería instantánea, SMS del PBC/registratario: nuevos medios de contacto que se pueden utilizar opcionalmente para comunicarse con el registratario o el PBC mediante SMS, mensajería instantánea u otro medio de comunicación alternativo de redes sociales.

---

[13] Es diferente de la fecha de creación, ya que la fecha de creación toma la última fecha en que se registró el nombre de dominio y es posible que el nombre de dominio haya sido registrado previamente y luego eliminado varias veces. La fecha de registración original establece la fecha en la cual el nombre de dominio se registró por primera vez.

Correo electrónico, teléfono y redes sociales alternativos del PBC/registratario: nuevas direcciones alternativas que se pueden utilizar opcionalmente para comunicarse con el registratario o el PBC cuando falla la dirección principal. Estos nuevos elementos de datos están diseñados para abordar necesidades comunes, como la resolución de problemas técnicos cuando el nombre de dominio deja de funcionar, y para permitir el contacto más rápido a través del teléfono móvil o las redes sociales.

URL de contacto o para informe de abusos del PBC/registratario: nuevos elementos de datos que pueden dirigir a páginas web en las cuales se pueden colocar medios de contacto o formularios, políticas o instrucciones para informar abusos a fin de facilitar una comunicación más productiva.

ID de contacto de PBC: un identificador único asignado a un bloque prevalidado de datos de contacto identificados como el PBC de este nombre de dominio, con el rol indicado por el rol de contacto. El ID de contacto de registratario o de PBC pueden referirse a contactos diferentes.

Nota: Se deben considerar los desafíos de transición y cumplimiento asociados con estos nuevos elementos de datos antes de implementar RDS.

b. Principios para acceso a datos restrictos y no autenticados

El EWG recomienda que se adopte un nuevo enfoque para el acceso a los datos de registración y se abandone el acceso totalmente anónimo por todos a todo en favor de un nuevo paradigma que combine el acceso público a algunos datos con el acceso restricto a otros datos. A continuación, se presentan los principios que reflejan esta recomendación.

N.º	Principios de acceso a datos
41.	Los usuarios de RDS no autenticados deben poder acceder a un conjunto mínimo de datos, al menos en consonancia con el régimen de privacidad más estricto.
42.	Se deben apoyar varios niveles de acceso autenticado a datos, de manera coherente con los fines permisibles.
43.	Las credenciales de acceso de usuarios de RDS deben vincularse con un proceso de acreditación auditable, como se define en la Sección IV (c), Acreditación de usuarios de RDS.
44.	El acceso no debe ser discriminatorio (es decir, el proceso debe crear reglas de participación parejas para todos los solicitantes, dentro del mismo

N.º	Principios de acceso a datos
	propósito).
45.	Con el fin de disuadir el uso indebido y promover la responsabilidad: • Todo acceso a elementos de datos se debe basar en un propósito establecido; • El acceso a los elementos de datos restrictos debe limitarse a los solicitantes autenticados que demuestren un fin permisible; y • Los solicitantes deben poder solicitar y recibir credenciales de uso para utilizar en futuras solicitudes autenticadas de acceso a datos.
46.	Se debe solicitar algún tipo de acreditación a los solicitantes de acceso restricto: • Cada vez que los solicitantes acreditados consulten datos, deben aclarar su propósito. • Podrán aplicarse distintos términos y condiciones a las distintas finalidades. • Se deben aplicar penalidades ante un incumplimiento de los términos y las condiciones por parte de los solicitantes acreditados.
47.	Para elevar el nivel de protección de los datos de registración de gTLD, para todas las consultas y respuestas de RDS, se deben utilizar medidas de autenticación y cifrado de mensajes comúnmente disponibles a fin de proteger la confidencialidad y la integridad de los datos en tránsito.
48.	Para satisfacer las necesidades de los usuarios autenticados de RDS con fines permisibles, el RDS debe proporcionar un servicio de consulta inversa que busque un valor especificado en elementos de datos públicos y restrictos, y devuelva una lista de nombres de dominio que hagan referencia a ese valor.
49.	Para satisfacer las necesidades de los usuarios autenticados de RDS con fines permisibles, el RDS debe proporcionar un servicio WhoWas que devuelva instantáneas del historial de elementos de datos públicos y restrictos para nombres de dominio especificados, limitadas a los datos de historial disponibles de RDS.
50.	El RDS debe admitir servicios innovadores que utilicen elementos de datos de RDS, de la siguiente manera.

N.º	Principios de acceso a datos
	• Debe ser posible que terceros presten servicios innovadores existentes y futuros, incluso consultas inversas y WhoWas, usando elementos de datos públicos y en virtud de los términos y condiciones de uso de datos de RDS. • En el caso de que terceros ofrezcan servicios innovadores que involucren elementos de datos restrictos, los terceros deben estar acreditados y respetar los términos y condiciones de uso de datos de RDS.
51.	Toda divulgación de elementos de datos restrictos se debe realizar usando métodos de acceso de RDS definidos (incluso los descritos anteriormente). Todo el conjunto de datos de RDS para gTLD (o todo el conjunto de datos del registro de un solo gTLD) se debe exportar de forma masiva en caso de acceso no controlado.
52.	La divulgación se puede dar mediante la muestra interactiva y otros métodos de acceso de RDS. • Con el fin de que los datos se encuentren más fácilmente y de manera uniforme, se debe ofrecer un punto de acceso centralizado (por ejemplo, un portal web). • Debe haber acceso a datos públicos para todos los solicitantes a través de un método de consulta sin autenticar (como mínimo, mediante un sitio web). • El acceso seguro a datos restrictos debe contar con soporte en la Web y en otros métodos y formatos de acceso (por ejemplo, respuestas XML de RDAP, SMS, correo electrónico), según la finalidad y el propósito del solicitante. • Los solicitantes deben poder obtener datos autoritativos en tiempo real de RDS cuando lo necesiten. • El RDS debe incorporar la automatización para búsquedas a gran escala para varios casos de uso y fines permisibles.
53.	Para ser verdaderamente global, el RDS debe mostrar los datos de registración en múltiples idiomas, códigos de escritura y conjuntos de caracteres, incluso nombres de dominio internacionalizados (IDN).

N.º	Principios de acceso a datos
54.	El RDS debe admitir todas las políticas futuras de transliteración definidas por GNSO para gTLD.
55.	El RDS debe permitir la recopilación y la visualización de los elementos de datos de registración en idiomas locales.

Ilustración de acceso a datos públicos

Como se describe en la ilustración siguiente, todavía cualquiera puede solicitar elementos de datos públicos desde el RDS, con autenticación o sin ella. Consulte el Anexo E para observar una ilustración más detallada de los elementos de datos devueltos de una consulta de datos públicos sin autenticar.

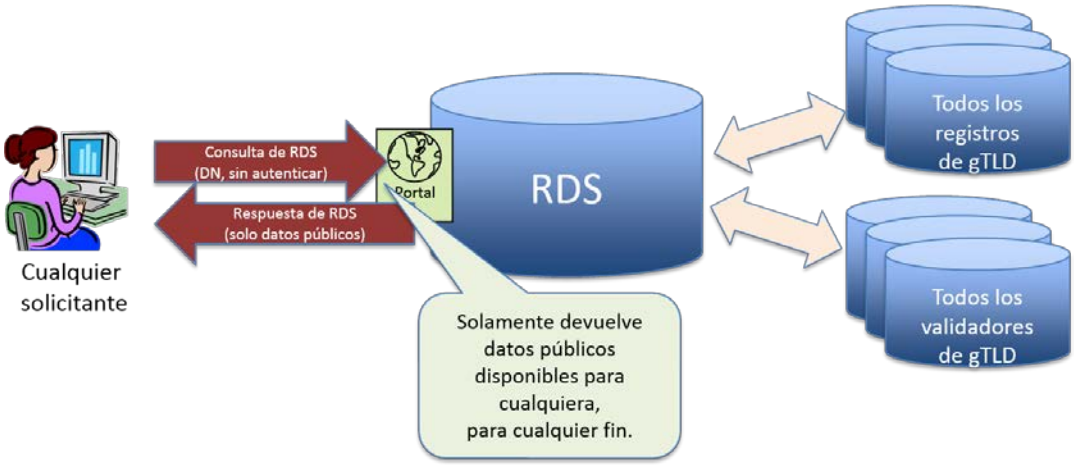


Figura 6: Acceso a los datos públicos de registración sin autenticar mediante RDS

El Anexo I también contiene diagramas de flujo y un caso de uso de ejemplo para ilustrar los pasos necesarios para acceder a los elementos de datos pertinentes.

Ilustración de acceso a datos restrictos

Como se muestra en la ilustración siguiente, los elementos de datos restrictos también se pueden solicitar por medio del RDS. Para hacerlo, los solicitantes primero deben estar acreditados. Posteriormente, los solicitantes pueden enviar consultas autenticadas para solicitar elementos de datos para un propósito establecido. Consulte el Anexo E para observar una ilustración más detallada de los elementos de datos devueltos de una consulta de datos restrictos con autenticación.

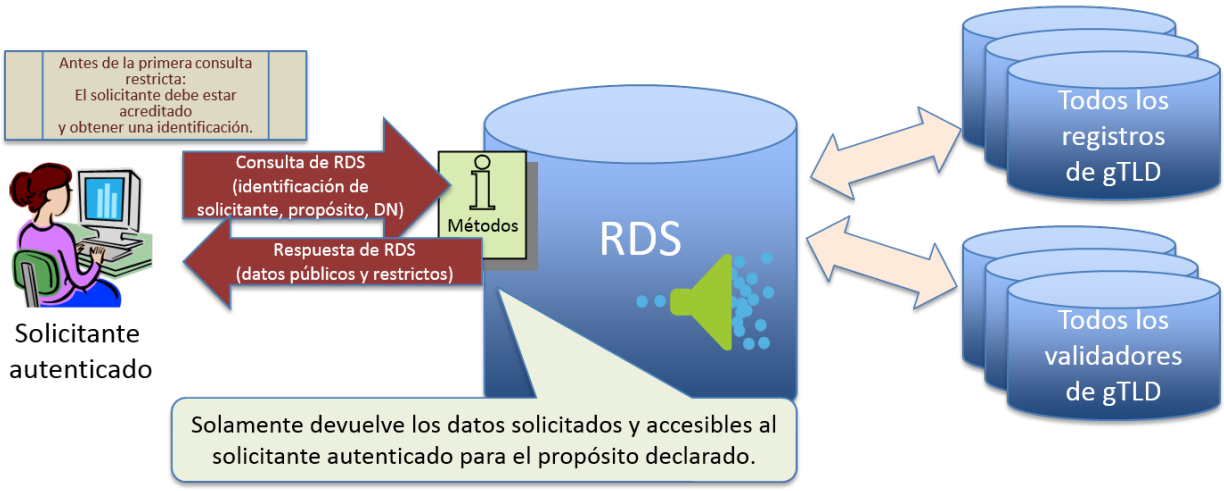


Figura 7: Acceso a los datos de registración restrictos mediante RDS

Protocolos técnicos y métodos de acceso

El EWG examinó si los protocolos técnicos implementados en el sistema de registración de dominios actual (por ejemplo, EPP[14]), y en fase de desarrollo en IETF (como el grupo de trabajo WEIRDS), podrían admitir las características de diseño recomendadas por el EWG. El grupo WEIRDS está cerca de finalizar un nuevo estándar denominado Protocolo de acceso a datos de registración (RDAP). La adopción de estos protocolos en el modelo recomendado por el EWG puede generar menores costos de transición para cada una de las partes afectadas.

El EWG analizó si EPP podría admitir todos los elementos de datos incluidos en su RDS recomendado y si RDAP podría admitir los principios de credenciales de acceso recomendados por el EWG. El análisis del EWG sugiere que tanto el PPE y como el RDAP pueden ser utilizados por el RDS, sin importar cuál de los modelos alternativos se elija. Sin embargo, esto puede requerir un par de extensiones, agregados o la utilización de "observaciones" a RDAP. En el Anexo G, se incluye una evaluación detallada de estos protocolos.

c. Principios de acreditación de usuarios de RDS

Como se señaló en la Sección III, Propósitos, algunos propósitos requieren acceso a todos los elementos restrictos o un subconjunto aprobado de elementos de datos restrictos. Como se señaló en la Sección IV (b), Principio n.º 46, todo propósito que solicite acceso a datos restrictos requiere la acreditación del usuario. No obstante, la

[14] Consulte EPP: estándar 69, RFC 5730 a 5734.

acreditación del usuario no implica acceso ilimitado a los datos restrictos. Todo acceso debe ser con un propósito y debe devolver solamente elementos de datos para el propósito indicado.

El EWG recomienda que, para cada comunidad de usuarios de RDS identificada en la Sección III que desee acceder a los datos restrictos para fines permisibles, los expertos de la comunidad deben ser consultados a fin de confirmar el propósito de los datos de registración identificados por el EWG, los elementos de datos que deben ser accesibles para ese propósito y los posibles acreditadores de usuarios del RDS.

Muchas organizaciones pueden celebrar contratos con la ICANN para servir como acreditadores de usuarios de RDS. A pesar de que todos los acreditadores de usuarios del RDS deben guiarse por un conjunto común de principios, es posible que haya diferencias de implementación en cada comunidad de usuarios del RDS. Por ejemplo:

Escenario n.º 1: Organismo de acreditación independiente del operador de acreditación, en el cual el organismo aprueba usuarios, pero un tercero administra el acceso de los usuarios acreditados al RDS

Para una comunidad de usuarios de RDS, como titulares de marcas, una organización del sector podría asumir la responsabilidad de acreditar a sus propios miembros que deseen acceder a los datos restrictos para fines permisibles. Este organismo de acreditación puede administrar cuentas de usuarios o autenticar solicitudes de acceso enviadas al RDS. En su lugar, el organismo de acreditación establece reglas de membresía, términos de servicio y procesos de solicitud y aplicación, etc., para una comunidad de usuarios de RDS dada. El organismo de acreditación puede entonces contratar un tercero que trabaje como operador de acreditación para crear y administrar las cuentas de usuarios de RDS, emitir credenciales de acceso a RDS, autenticar las solicitudes de acceso a RDS y manejar los informes de abuso de primer nivel, incluso la suspensión temporal de cuentas. El operador de acreditación simplemente implementa y hace cumplir las reglas de acceso al RDS establecidas por el organismo de acreditación para una comunidad determinada. Toda apelación a la suspensión de una cuenta u otras disputas se deberían escalar al organismo de acreditación.

Escenario n.º 2: Organismo de acreditación combinado con operador de acreditación, que aprueba solicitudes autenticadas de acceso al RDS

Para una comunidad de usuarios de RDS como OpSec, una organización del sector podría asumir la responsabilidad de acreditar a sus propios miembros a través de un proceso de acreditación (aprobado) que ya utiliza para conceder a los usuarios el acceso a otros sistemas. En este ejemplo, la organización sirve como organismo de acreditación

y como operador de acreditación. Así aprovecha un sistema existente en uso por sus propios miembros para autenticar y luego aprobar las solicitudes de acceso restricto para fines permisibles al RDS. Aquí el usuario de RDS es responsable de cumplir con los términos y condiciones, y la organización del sector debe establecer un proceso para hacer frente a los abusos de acceso, las suspensiones, etc., aplicados a accesos del RDS de un usuario específico.

Escenario n.º 3: Organismo de acreditación combinado con operador de acreditación, que actúa como representante de las solicitudes de acceso al RDS de parte de sus miembros (es decir, el modelo de la Interpol)

Para una comunidad de usuarios de RDS, como los organismos encargados del cumplimiento de la ley, una organización reconocida y de confianza podría asumir la responsabilidad de acreditar a sus propios miembros a través de un proceso de acreditación (aprobado) que ya utiliza para conceder a los usuarios el acceso a otros sistemas. En este ejemplo, la organización sirve como organismo de acreditación y como operador de acreditación. Así aprovecha un sistema existente en uso por sus propios miembros para autenticar y luego representar las solicitudes de acceso restricto para fines permisibles al RDS. Aquí la organización se considera el usuario del RDS y acepta la responsabilidad por las acciones de sus miembros respecto de las solicitudes de representación y el cumplimiento de los términos y condiciones. A pesar de que el RDS no esté al tanto de las actividades específicas de los usuarios, la organización debe establecer un proceso para tratar con abusos de acceso, suspensiones, etc., de una manera que permita que la organización audite los accesos de usuarios específicos y detecte los abusos.

Para permitir el acceso de usuarios acreditados del RDS a elementos de datos restrictos para fines permisibles, el EWG recomienda los siguientes principios de acreditación de usuario del RDS.

N.º	Principios de acreditación de usuarios de RDS
56.	El acceso no acreditado ni autenticado a datos no restrictos (es decir, públicos) debe ser posible en tiempo real.
57.	La acreditación de los usuarios del RDS para acceder a datos de RDS no tiene que ocurrir en tiempo real para todos los casos de uso o solicitantes.

N.º	Principios de acreditación de usuarios de RDS
58.	El RDS solamente debe aplicar el mínimo "programa de acreditación" necesario para proporcionar acceso a usuarios del RDS a elementos de datos restrictos para el propósito indicado.[15]
59.	No debe haber ningún requisito de "preaprobación" ni proporcionar credenciales a cada usuario potencial del RDS. Se puede crear un proceso de solicitud y cumplimiento para cada "tipo" de usuario acreditado de RDS (es decir, la comunidad de usuarios de RDS).
60.	La acreditación de usuarios de RDS que buscan acceso a datos para fines permisibles se debe poder otorgar de tres maneras: • Ninguna (es decir, acceso no autenticado solamente a datos públicos, como se describió antes). • Autoacreditación por parte de la persona o la entidad que solicita los datos, como un sistema en el que el usuario simplemente establece su identidad, los datos que solicita y el motivo, y luego se le otorga acceso a ese nivel de datos. Por ejemplo, esto podría aplicarse a los registratarios que necesitan acceso a los datos de su propio nombre de dominio con propósitos de control de nombre de dominio, en los cuales su autotestimonio está ligado a la registración real de un nombre de dominio, lo que los califica para obtener credenciales para acceder a esa información en el RDS. • Acreditación por parte de un tercero de confianza (es decir, un acreditador de usuarios del RDS; consulte el principio n.º 64 a continuación).
61.	En los casos posibles, un proceso de acreditación del RDS por un tercero debe aprovechar los procesos de acreditación existentes de cada comunidad de usuarios de RDS identificada en la Sección III como una comunidad que requiere credenciales.
62.	Estos procesos de acreditación de terceros deben ser investigados por una autoridad responsable de aplicar y hacer cumplir la política de acreditación de usuarios del RDS (por ejemplo, la ICANN, un panel de múltiples partes interesadas) y revisados de forma periódica.
63.	Cualquier organización que actúe como acreditador de usuarios del RDS debe tener un acuerdo firmado con la ICANN o con el proveedor del RDS para ofrecer este tipo de proceso de acreditación en virtud de las directrices

[15] Por ejemplo, esta acreditación no tiene por qué requerir declaraciones juradas de factores múltiples ni debe servir de sistema esencial para obtener la mayoría de los tipos de datos.

N.º	Principios de acreditación de usuarios de RDS
	acordadas y establecer un marco para garantizar el debido proceso, la responsabilidad, la seguridad, el acceso equitativo y el cumplimiento de la ley aplicable.
64.	Los acreditadores pueden tomar una de las siguientes responsabilidades o ambas. • Un acreditador de usuarios del RDS puede definir y administrar una comunidad de usuarios, incluso establecer un criterio de membresía, fijar requisitos de acreditación y definir y determinar sus propios términos y condiciones de afiliación. • Un operador de acreditación de usuarios del RDS puede ofrecer una plataforma utilizada por organismos de acreditación para cumplir funciones, como la creación de cuentas de usuario, la emisión, la suspensión y la revocación de credenciales, la gestión de cuentas de usuario, y los procesos asociados, como el manejo de disputas y la aplicación de ToC. Un acreditador puede aceptar ambas responsabilidades, pero no está obligado a hacerlo.
65.	Los acreditadores que deseen participar en el manejo de solicitudes de datos de RDS de parte de sus miembros pueden hacerlo de dos maneras: • Un acreditador puede proporcionar acceso mediante representación al RDS mediante su propio sistema de autenticación y aceptar toda la responsabilidad por uso según las normas. Aunque el acreditador tendrá que rendir cuentas en caso de abuso, las solicitudes de representación a través de acreditadores deben ser autenticadas de forma que permitan realizar auditorías y solucionar quejas de abuso relativas al acceso de un usuario individual. • Un acreditador puede proporcionar acceso al RDS mediante su propio sistema de autenticación y enviar las solicitudes autenticadas al RDS. Las solicitudes enviadas a través del acreditador deben identificar unívocamente al usuario del RDS, que es responsable del uso según las normas y deberá responder en caso de abuso.
66.	Como se define en la Sección IV (b), Principio n.º 50, el RDS debe proporcionar acceso en tiempo real a los solicitantes acreditados mediante diferentes métodos. Los solicitantes pueden recibir autenticación de un operador de acreditación adecuado y las credenciales de acceso al RDS emitidas durante la

N.º	Principios de acreditación de usuarios de RDS
	acreditación deben ser adecuadas para usarlas con todos los métodos de acceso definidos.[16]
67.	Se pueden definir mejores prácticas para la administración de credenciales. Se espera que los acreditadores adhieran a dichas prácticas.
68.	El RDS debe solicitar credenciales individuales para el acceso autenticado.
69.	El acceso autenticado a RDS no debe ser transitivo (es decir, ningún usuario autenticado de RDS debe compartir datos restrictos con otros que no tengan su acreditación).
70.	Se debe crear y aplicar un proceso para la revelación responsable de datos restrictos a fin de ampliar el propósito original por el cual se los solicitó. (Por ejemplo, permitir que el propietario de IP que investiga una infracción de marca presente un reclamo de UDRP; permitir que un usuario de OpSec que investiga posible actividad criminal notifique a las autoridades).
71.	Una organización que busca el acceso a datos del RDS podría solicitar la acreditación de usuarios del RDS y hacer que todas las personas utilicen el RDS en su organización en virtud de esa acreditación.[17] Cada organización es responsable de la gestión del acceso acreditado dentro de su propia organización. El uso indebido del sistema por los miembros de una organización de usuarios del RDS puede generar sanciones para toda la organización.
72.	Un usuario del RDS con diferentes roles puede tener varias credenciales para acceder a diferentes tipos de datos para diversos propósitos. Sin embargo, se aconseja desde la perspectiva de la facilidad de uso, que se proporcione una sola credencial por usuario del RDS, que puede ser utilizada para múltiples propósitos, siempre y cuando se establezca cada propósito por acceso como se define en la Sección IV (b).
73.	Se deben utilizar auditorías y análisis de datos para identificar abusos del sistema y credenciales de acceso.
74.	Se debe definir un proceso de apelación para que los usuarios del RDS refuten las acusaciones de abuso cuando intenten reactivar o restituir las credenciales

[16] Las interfaces de autenticación se deben definir durante la implementación. Por ejemplo, para algunos métodos de credenciales, el RDS puede usar un marco estándar, como el lenguaje de marcado para confirmaciones de seguridad (SAML), para permitir la autenticación por parte del operador de acreditación que emitió esa credencial.

[17] Depende de la organización asegurar la integridad de las credenciales expedidas para acceder al RDS.

N.º	Principios de acreditación de usuarios de RDS
	de acceso de RDS.
75.	Todos los registratarios deben recibir una credencial para examinar sus propios datos de contacto según los almacenó el RDS en relación con los nombres de dominio registrados a su nombre. (Consulte la Sección III, Propósito de control de nombre de dominio).
76.	Se debe establecer un proceso para añadir acreditadores de usuarios del RDS que complemente el proceso actual o que ofrezca maneras nuevas e innovadoras de acreditar usuarios para propósitos aprobados del RDS. Estos acreditadores de usuarios del RDS deben cumplir con los requisitos mínimos según se describen en los principios enumerados en el presente.

d. Resumen de beneficios clave de responsabilidad

La incorporación de acceso acreditado a elementos de datos restrictos es una parte integral del RDS para la próxima generación; mejorará la responsabilidad, ya que exigirá que se identifiquen quienes deseen acceder a datos confidenciales y declaren el propósito por el cual necesitan los datos. En concreto, los beneficios que derivarán de la adopción de los principios de elementos de datos y de acceso recomendados por el EWG incluyen los siguientes:

- Establecer un paradigma de divulgación y recopilación de datos con un propósito a fin de promover la responsabilidad de las entidades que usan datos de registración para fines permisibles.
- Ofrecer un marco de apoyo para cumplir con las leyes de protección de datos en varias jurisdicciones.
- Establecer un método para proporcionar responsabilidad para quienes accedan a datos por diversos propósitos. Esto respalda aún más los requisitos de protección de datos y de privacidad en varias jurisdicciones y garantiza un equilibrio de responsabilidad entre quienes son obligados a proporcionar datos precisos y quienes los usan para propósitos aprobados. Afronta la iniquidad fundamental del sistema actual de WHOIS, en el cual los solicitantes de datos no tienen responsabilidad por el acceso y el uso de datos de contacto.
- Explicarles claramente a los registratarios y los contactos los propósitos por los cuales se recopilan datos de registración y se aplica mayor control discrecional sobre qué información personal es pública o restricta.

- Cumplir con necesidades universales de datos de registración con un conjunto básico de datos públicos y reducir los datos públicos por defecto, además de autenticar a quienes acceden a datos restrictos.
- Aumentar la precisión de los datos, gracias a la protección de elementos de datos confidenciales de divulgación pública, lo que probablemente mejore el uso compartido de datos más precisos por parte de registratarios y PBC. A excepción del uso por delincuentes, cuando se protegen los datos de la publicación general, los asuntos de los datos a menudo brindan información más precisa a fin de recibir los beneficios de proporcionarla, ya que se mitiga el riesgo fundamental percibido.
- Mejorar la eficiencia y la flexibilidad de la comunicación en general para los registratarios y los usuarios del RDS mediante la incorporación de nuevos elementos de datos opcionales para facilitar el contacto a través de métodos de comunicación nuevos o alternativos.
- Admitir consultas inversas y WhoWas mediante un portal central para permitir búsquedas en todas las registraciones de gTLD por parte de usuarios del RDS para fines permisibles solamente.
- Permitir capacidades mejoradas de acceso para mejorar la eficiencia general del "sistema".
- Brindar acceso, sin autenticar a datos públicos y mediante credenciales a datos restrictos, para eliminar la mezcla de capacidades de acceso, niveles de servicio y formatos de las respuestas de WHOIS de gTLD actual, y permitir la implementación sencilla de consultas automatizadas de RDS mediante un solo estándar.
- Proporcionar un servicio de calidad y acceso responsable, lo que permite quitar varias medidas antiabuso distribuidas en el ecosistema.

Para lograr estos beneficios, es fundamental educar a los usuarios del RDS acerca de los fines permisibles y los usos adecuados de los datos recuperados del RDS. Encontrar acreditadores que deseen aceptar la responsabilidad de aprobar el acceso a RDS por parte de los miembros de su comunidad puede ser un reto. En un principio, puede haber cierta confusión del usuario respecto de cómo identificar al acreditador adecuado, en especial, para usuarios que interactúan con RDS para varios propósitos. Las consultas automatizadas de RDS también requerirán la actualización de las herramientas. Sin embargo, estas inversiones iniciales necesarias para establecer el acceso con un propósito establecerán una base sólida para que los usuarios del RDS usen los datos de registración de manera responsable.

V. Mejora de la calidad de los datos

El EWG recomienda fijar una validación más sólida de los datos de los registratarios que la del sistema de WHOIS actual o aplicar mejoras que se pueden obtener por medio de una implementación integral del RAA 2013. En primer lugar, el suministro de PBC de los registratarios debería generar mejoras significativas a la accesibilidad de los contactos adecuados para varios propósitos y crear un incentivo para que los registratarios brinden información apropiada para esos roles. En segundo lugar, el acceso restricto a elementos de datos confidenciales debería reducir la intención de los registratarios de proporcionar datos inexactos, además de más responsabilidad para garantizar la precisión de los datos.

Para lograr estos objetivos, el EWG recomienda dos mejoras relacionadas aunque independientes:

- El RDS debe aplicar la validación estándar a todos los datos de registración de gTLD. Además de las revisiones periódicas, la validación debe realizarse en el momento de la recopilación, con la opción de prevalidar bloques de datos de contacto para su reutilización en varias registraciones de nombres de dominio.
- El ecosistema de RDS debe incluir un directorio de contacto prevalidado, conceptualmente independiente del directorio de nombres de dominio, para promover la calidad y la reutilización de los elementos de datos usados para contactar a los registratarios de nombres de dominio y a individuos u organizaciones que puedan designar los registratarios como PBC para diversos propósitos asociados con una registración de nombres de dominio y para disuadir el uso fraudulento de datos personales.

Los principios y los procesos que detallan estas recomendaciones se explican a continuación. Para obtener el máximo beneficio, el EWG recomienda ambas mejoras, pero advierte que la creación de un directorio de contactos es posible sin la validación mejorada y viceversa.

a. Principios de validación y precisión de datos

La prevalidación de la información de contacto del registratario u otro contacto se necesita para:

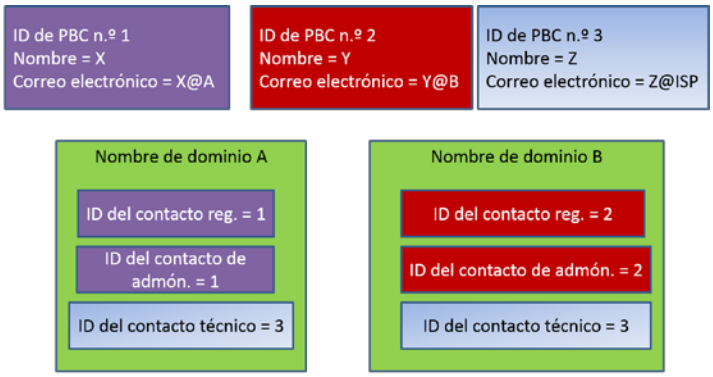
- Incrementar la precisión de la información de contacto mediante la utilización de prevalidación para comprobar los datos antes de su uso para un nuevo nombre de dominio y para promover los datos coherentes en todas las registraciones (reduce los errores y el fraude);

- Evitar la necesidad de validar los datos del registratario u otros datos de contacto de PBC cada vez que un registrador registra un nuevo nombre de dominio realizando la validación una vez y luego reutilizando el bloque de datos de contacto para varias registraciones de dominios (simplifica el proceso y reduce los requisitos de trabajo); y
- Evitar el retraso del procesamiento de la registración de un dominio, ya que la validación debe tener lugar en el momento de la registración.

Muchos proveedores de servicios, representantes legales y otros terceros a menudo son los puntos de contacto principales para varias funciones (por ejemplo, roles técnicos, de facturación, informes de abuso, procesos legales) en los dominios registrados por una amplia variedad de registratarios (a menudo de cientos a cientos de miles de dominios).

Para lograr una precisión mucho mayor en un espacio tan diverso y facilidad de uso para este tipo de contactos, se aconseja proporcionar mecanismos para permitir el uso fácil de este tipo de contactos por varios registratarios; por ejemplo, una empresa de hosting que ofrece su ID único de NOC para contactos técnicos y de informe de abusos para dominios controlados por sus clientes. Además, cuando tal entidad necesita actualizar su información de contacto para reflejar una nueva dirección/número de teléfono o una fusión/adquisición, esa información debe ser fácil de actualizar en un solo lugar y tiene que reflejar todos los dominios asociados con ese conjunto de datos de contactos (como se designa con un solo identificador).

La siguiente figura ilustra un paradigma en el que se deberían crear contactos con un propósito (PBC), asociados con identificadores únicos (ID de PBC), y luego se los reutiliza en múltiples registraciones de nombres de dominio. Como se detalla en la Sección III, los PBC no representan necesariamente a personas individuales, sino que son puntos de contacto publicados, expresamente creados por titulares de contacto y destinados a hacer posible la comunicación con propósitos relacionados con DNS.



Las actualizaciones realizadas a ID de PBC n.º 3 se reflejan automáticamente en los datos de registración de los nombres de dominio A y B.

N.º	Principios de ID de contacto y datos asociados
77.	La administración de contactos debe ser factible independientemente de la administración de dominios, lo que permite la portabilidad de los contactos y la responsabilidad independiente de los nombres de dominio y controlada por individuos o entidades reales incluidos en esos contactos.
78.	Los contactos se deben administrar con validadores que administren bases de datos de contactos, implementen regímenes de validación y mantengan la información sobre el nivel de validez del contacto y sus elementos de datos (accesibles a través del RDS).[18]
79.	Las registraciones de dominios pueden estar asociados con ID de contacto designados por sus registratarios y aprobados por los contactos designados para varios propósitos asociados con el nombre de dominio.
80.	Tales contactos deben contener elementos de datos obligatorios y válidos. Se requieren políticas y supervisión para administrar estos procesos con el objetivo de garantizar que los ID de contacto no se utilicen sin la autorización del contacto y que cumplan los estándares mínimos.
81.	El titular de contacto controla la administración de cambios y la autorización de uso de información de contacto y afecta a todos los dominios asociados con un contacto. Se deben desarrollar procesos y políticas para garantizar la aplicación precisa, auténtica y oportuna de los cambios deseados sin cargar los PBC o los registratarios a fin de apoyar este nuevo paradigma.

[18] NOTA: Los registradores pueden convertirse en validadores acreditados, y es probable que así sea, con el fin de proporcionar servicios de validación para los contactos asociados con los nombres de dominio que registran.

N.º	Principios de ID de contacto y datos asociados
82.	Cada bloque individual de datos de contacto debe tener un ID de contacto que identifique tanto al validador como al titular de contacto de manera única para permitir la recuperación y la actualización de los datos de contacto asociados. Este ID de contacto debe ser publicado en cualquier visualización pública de datos de RDS.

b. Proceso de prevalidación

Para hacer frente a estas necesidades, se recomienda el siguiente proceso de prevalidación:

a) Cada solicitante envía los datos de contacto a través de un validador de su elección (por ejemplo, registrador, registro, proveedor acreditado de servicios de administración de contactos).

b) El validador lleva a cabo la validación sintáctica y operativa (según SAC-058).

c) **OPCIONAL**: Los validadores pueden efectuar la validación de la identidad por medio de entidades, como oficinas postales, administradores de ccTLD, empresas telefónicas, oficinas de impuestos, etc.*Tenga en cuenta que los contactos que cumplieron con estándares de validación de identidad opcionales se pueden designar como tales en sus estados a fin de mejorar la confianza del usuario, lo que facilita el comercio en línea. También observe que este tipo de servicios de valor agregado probablemente tengan un costo asociado que debería asumir la entidad que solicita este nivel adicional de validación.*

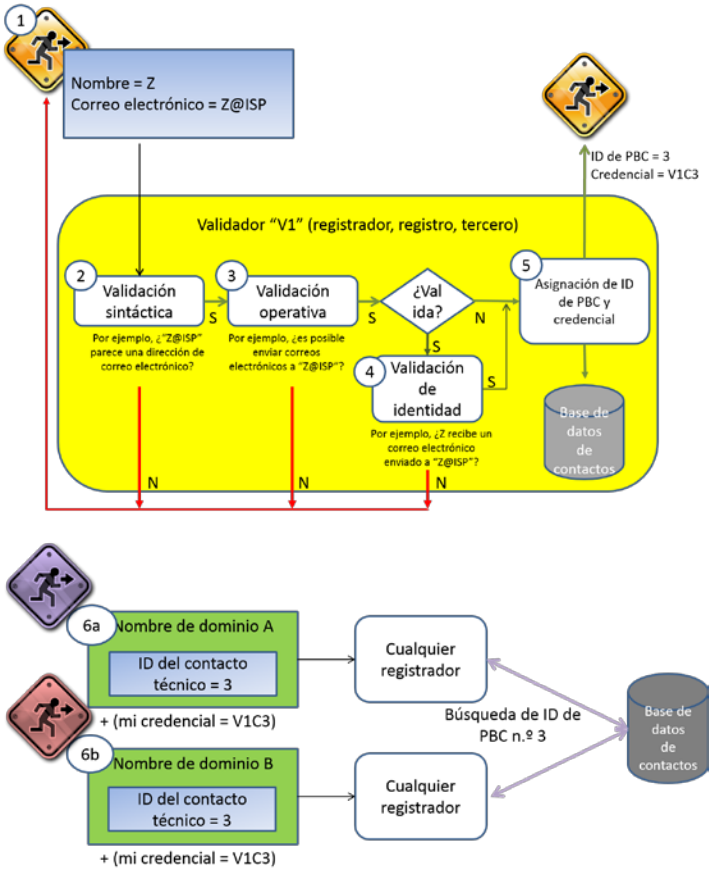
d) Después de efectuar una validación sintáctica satisfactoria y cualquier validación operativa requerida, el validador emite un identificador para el bloque de datos de contacto (contacto), que identifica de manera única tanto al validador como al contacto para permitir la posterior recuperación y actualización.

e) El validador almacena los datos de contacto en su propia base de datos, emite credenciales (según corresponda, que permitan actualización futura del contacto) y reenvía el identificador único al solicitante (de aquí en adelante, denominado "titular de contacto").

f) El titular de contacto ofrece este ID de contacto a los registratarios, que podrán proceder con cualquier registrador, utilizando este identificador único, para registrar los nombres de dominio usando los ID de contacto como contactos con un propósito designado (es decir, PBC). *Como se define en la Sección III, se debe implementar un proceso de autorización para garantizar que el registratario y el contacto designado*

están de acuerdo en los propósitos que aceptará el PBC para cada nombre de dominio.

g) Los ID de contacto validados se pueden designar como PBC para un nombre de dominio (por ejemplo, registratario, contacto técnico, administrativo, comercial, legal, para informe de abusos, proveedor de servicios de privacidad/representación) según los principios de contactos con un propósito, como se define en la Sección III (e).



Observe que cada validador mantiene su propia base de datos. También se deben proporcionar estos datos al RDS, pero ese mecanismo depende del modelo del RDS, según se describe en la Sección VII. Por ejemplo, en el modelo sincronizado, las incorporaciones y actualizaciones de los datos de contacto se pueden transferir al RDS mediante EPP. En el modelo federado, los datos de contacto se pueden transferir al RDS en tiempo real mediante RDAP.

c. Proceso de remediación, auditoría y precisión

Los siguientes procesos se recomiendan para asegurar la continua precisión de los datos de registración y la remediación de los datos de registración inexactos:

a) **Autocorrección**: el titular de contacto utiliza al validador para corregir o actualizar los datos usando las credenciales emitidas anteriormente. La información fluye de forma automática a través de los dominios que utilizan ese contacto en particular (según lo designado por el ID de contacto único).

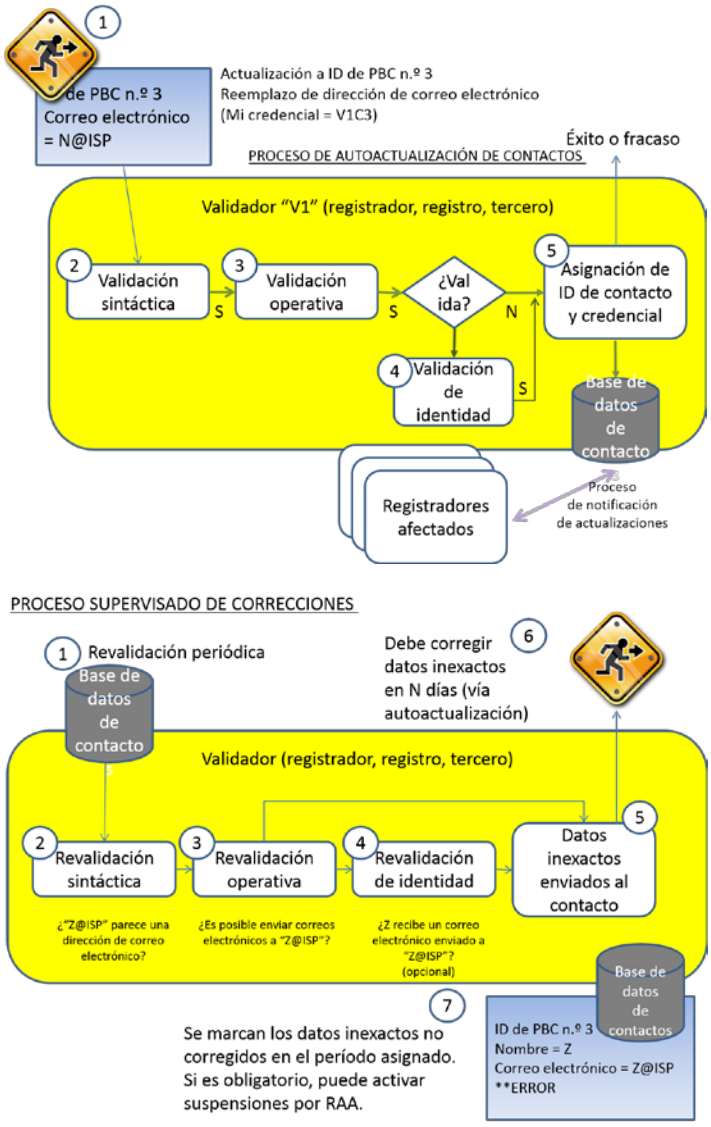
b) **Proceso supervisado**: los validadores realizan validaciones de identidad operativas periódicas y de identidad opcionales en los conjuntos de datos administrados mediante su servicio. *Nota: Esos procedimientos de validación no deben ser demasiado engorrosos, pero se pueden ver reflejados en los estados publicados de los contactos (por ejemplo, el contacto es operativamente válido hasta el 1.º de enero de 2016).*

c) Los validadores informan las inexactitudes detectadas en los datos al titular de contacto, lo que le da un período específico (por ejemplo, 14 días) al titular de contacto para corregir la inexactitud. Se puede notificar a los registratarios, los registros y los registradores de los dominios afectados. El titular de contacto utiliza al validador antes seleccionado para corregir la inexactitud usando las credenciales emitidas previamente.

d) Si los datos de registración siguen siendo inexactos pasada la fecha límite, se los marca como incorrectos. Si los datos marcados son obligatorios para cualquier PBC que hace referencia a este ID de contacto, los dominios asociados se colocan en un proceso de remediación que notifica al registratario la inexactitud y le permite rectificarla en el período especificado por el RAA. Si no se la corrige, se puede incurrir en sanciones para el nombre de dominio, que pueden incluir la suspensión o la eliminación en virtud del RAA aplicable.

e) Una vez que los datos marcados se reemplazan por datos válidos, se quitan las sanciones de los dominios afectados.

f) En el caso de los informes de precisión presentados para cumplimiento ante la ICANN, el validador será notificado para repetir la validación sintáctica y operativa. Si la revalidación es satisfactoria, la parte que presenta el informe de precisión puede realizar otras acciones según corresponda a su situación (por ejemplo, presentar un reclamo de UDRP o enviar una solicitud de revelación). Si la revalidación no es satisfactoria, los registratarios de los nombres de dominio que utilizan ese ID de contacto inexacto deben ser notificados y deben seguir el proceso de remediación normal que se describió anteriormente.



d. Marco operativo para ID de contacto

El marco siguiente se recomienda para administrar ID de contacto y asociarlos con la información de registración:

a) Los ID de contacto deben ser únicos en todos los validadores a fin de garantizar la portabilidad de ID de contacto y proporcionar asignaciones definitivas entre nombres de dominio y la información del directorio necesaria.

b) Los ID de contacto que identifican al contacto y al validador se deben asociar con bloques discretos de información de contacto para permitir la recuperación y la actualización. Explicación: un ID de contacto asigna un conjunto de datos de

contacto útil para la comunicación con contactos de nombres de dominio designados. La información que no cumple con este requisito es inútil.

c) Los ID de contacto deben ser emitidos por validadores acreditados. Una entidad puede postularse para ser validador, según un criterio análogo con el utilizado para acreditar registradores. Los validadores acreditados pueden incluir registradores, registros y terceros proveedores de validación. Fundamentos: los validadores son necesarios para crear bases de contactos. El nivel de validación puede variar por contacto, pero el proceso debe ser armonizado entre los validadores para garantizar la precisión y la responsabilidad de los registratarios de dominios y sus contactos designados.

d) Para asociarse con un nombre de dominio, el registratario o PBC designado debe obtener un ID de contacto.

e) Los ID de contacto se pueden asignar a varios roles de uno o varios dominios. Por ejemplo, un ID de PBC se puede utilizar como identificador de registratario de un dominio y un contacto técnico y contacto para informe de abusos, para otros dominios.

f) Los contactos se pueden crear y modificar en cualquier momento, incluso como parte del proceso de registración de dominios.

e. Interacción con validadores

El EWG recomienda los siguientes principios para la interacción del validador con titulares de contacto (es decir, las partes que crean bloques de datos de contacto satisfactoriamente validados y reutilizables).

N.º	Principios de interacción entre titulares de contacto y validadores
83.	Para cualquier ID de contacto, el titular de contacto puede elegir cualquier validador.[19]
84.	Se deben elaborar políticas de supervisión y responsabilidad relacionadas con la administración de ID de contacto.
85.	Los titulares de contacto deben poder modificar la información de contacto asociada con un ID de contacto por medio del validador emisor.

[19] Según el Principio n.º 88, los ID de contacto identifican al validador y al titular de contacto. Se debe implementar de manera tal que permita la portabilidad de ID de contacto entre validadores.

N.º	Principios de interacción entre titulares de contacto y validadores
86.	Los validadores deben usar la autenticación de titular de contacto para disuadir la modificación no autorizada de información de contacto asociada con un ID de contacto.
87.	Los validadores pueden ofrecer múltiples niveles de autenticación de titular de contacto, que van desde la autenticación básica de PIN hasta la autenticación de dos factores. Los titulares de contacto deben ser capaces de elegir a los proveedores sobre la base de propuestas de costo/beneficio vinculadas con la facilidad de uso, la seguridad, los costos y otros factores comerciales lógicos.
88.	Los validadores deben publicar sus políticas de autenticación de manera que se las pueda utilizar en todo el mundo para la gestión de la reputación. Esto fomenta la mejor precisión y la responsabilidad de la información de contacto que se muestra.
89.	Los validadores deben poder validar información de contacto enviada en la lengua materna del titular de contacto. Esto debería mejorar la precisión de los datos en lengua materna y apoyar la escalabilidad del sistema de registración de nombres de dominio en un entorno plurilingüe. Por ejemplo, los registradores podrían trabajar con los validadores en varias localidades para proporcionar servicios de validación ampliados a un gran número de registratarios y contactos designados sin tener que invertir en costosas herramientas para validar datos en idiomas desconocidos para su propio personal.

f. Principios para la validación de contactos

Los datos de contacto se pueden validar en tres niveles diferentes: sintáctico, operativo y de identidad, según SAC 058. El EWG recomienda los siguientes principios de nivel de validación.

N.º	Principios para la validación de contactos
90.	Los elementos de datos de contacto asociados a un ID de contacto se deben validar a nivel sintáctico. Esto representa un nivel básico de validación que debe alcanzar cualquier entidad del sector.

N.º	Principios para la validación de contactos
91.	Todos los elementos de datos de contacto obligatorios vinculados con un ID de contacto de un propósito particular se deben validar de manera operativa[20] para que se pueda incluir al ID de contacto en los datos de registración del nombre de dominio para ese propósito.
92.	Un titular de contacto puede, de manera voluntaria, buscar niveles más altos de validación opcional (por ejemplo, validación opcional de identidad), haciéndose cargo de los costos generados por los beneficios percibidos (por ejemplo, mayor confianza de los consumidores en los nombres de dominio registrados para entidades con identidad validada).[21]
93.	Debido a los costos relacionados con la validación opcional de la identidad, se aconseja implementar un mecanismo de bajo costo para que los titulares de contacto económicamente desfavorecidos reciban validación opcional de identidad.
94.	Para conservar las asociaciones que facilitan un proceso de corrección, el ID de contacto puede tener el estado "inexacto" y permanecer en el sistema.
95.	El estado de validación del ID de contacto se debe rastrear y publicar según corresponda cuando se acceda a información del RDS, junto con la hora más reciente en que se determinó el estado de validación.
96.	Terceros pueden presentar informes de inexactitud para desafiar el estado de validación de un ID de contacto, como se describe en la Sección V (c), lo que puede desencadenar un proceso de remediación estándar que puede generar que se marque el ID de contacto como "inexacto" y otras consecuencias para los nombres de dominio que utilicen ese ID de contacto como PBC.
97.	Los dominios activos no pueden tener un contacto obligatorio con el estado "inexacto" sin algún tipo de remediación. No obstante, el programa se puede

[20] Consulte SAC 058 y el *Resumen de resultados de la encuesta de validación y verificación de datos de WHOIS para ccTLD* (ccTLD WHOIS Data Verification/Validation Survey Results Summary) para conocer las maneras posibles de implementar prácticas de ccTLD existentes y de validación operativa.

[21] Por ejemplo, la validación opcional de la identidad puede ser un complemento con precio por separado o se puede incluir en un paquete con la registración del nombre de dominio o se puede ofrecer como incentivo a clientes de grandes volúmenes. Consulte la *RFI sobre validación de datos de contacto y sistemas de verificación* (RFI on Contact Data Validation and Verification Systems) para conocer ejemplos de los servicios comerciales que brinda esa validación.

N.º	Principios para la validación de contactos
	determinar en otro lugar.
98.	Se debe comprobar un nivel mínimo de validación entre campos de todos los elementos de datos de contacto asociados con un ID de contacto donde se aplica la validación entre campos (por ejemplo, una dirección física).
99.	Es necesario llevar a cabo la revalidación de los datos de contacto de forma regular por medio de un validador para garantizar que los datos sean precisos en el nivel declarado.
100.	Si un titular de contacto proporciona elementos de datos opcionales, dichos elementos al menos deben estar sintácticamente validados. Los elementos de datos opcionales no deben validarse más allá del nivel sintáctico a menos que el contacto solicite y pague los costos asociados con esa validación.
101.	El nivel de validación alcanzado más allá de la validación sintáctica de los elementos de datos que se puede validar a nivel operativo u opcionalmente de identidad lo debe registrar y mantener el validador. Por ejemplo, elementos como el correo electrónico, el teléfono y la dirección podrían ser validados a nivel operativo, mientras que el nombre o el nombre de la organización no se pueden validar a nivel operativo, pero opcionalmente se puede validar su identidad.
102.	Además, el validador debe determinar y publicar como elemento de datos del RDS el estado general de validación alcanzado por cada ID de contacto. Por ejemplo, si TODOS los elementos de datos obligatorios que se pueden validar a nivel operativo aprueban los controles, el estado de validación general del contacto sería "validado operativamente". Si ALGÚN elemento de datos obligatorio que se puede validar a nivel operativo desaprueba los controles, el estado de validación general del contacto sería "validado sintácticamente". Si TODOS los elementos de datos obligatorios cuya identidad se puede validar aprueban el control opcional, el estado de validación general del contacto se actualizaría a "identidad validada". Para promover la precisión y la comunicación eficiente, este estado de validación general debe ponerse a disposición de los usuarios de RDS como un nuevo elemento de datos consolidado por contacto.[22]

[22] El EWG también consideró publicar los elementos de datos de publicación de RDS para transmitir el estado de validación individual de cada elemento de datos de contacto individual (por ejemplo, estado de dirección de correo electrónico de PBC = validado operativamente; estado del nombre de PBC = identidad validada). Publicar el estado de validación con este nivel de granularidad requeriría un protocolo significativo, elemento

N.º	Principios para la validación de contactos
103.	Para cualquier elemento de datos que ha sido objeto de validación, la marca de tiempo de la validación debe ser registrada y mantenida por el validador.
104.	La marca de tiempo del último cambio del estado general de validación de todo un ID de contacto también debe ser determinado por el validador y publicado como un nuevo elemento de datos del RDS por contacto.

g. Capacidad de datos de contacto únicos

Para combatir la suplantación de identidad, la difamación y el abuso, el titular de contacto puede afirmar que sus datos de contacto son únicos y que no los puede usar ningún otro reclamante de titular de contacto.

a) Los datos únicos pueden incluir muchos elementos del conjunto de contactos, en particular, la dirección de correo electrónico y el número de teléfono. Puede ser de difícil a imposible garantizar la calidad de único de un nombre o una dirección.

b) Si un titular de contacto solicita que se lo trate como único, tiene que haber un mecanismo previsto para que otros validadores comparen un conjunto de datos solicitado con el titular de contacto para garantizar que los nuevos solicitantes de ID de contacto (o los titulares de contacto existentes que modifiquen su información) no interfieran con datos únicos protegidos.[23]

c) Se debe validar la identidad de cualquier dato designado como único para evitar la suplantación de identidad y los ataques de "denegación de servicio" (un contacto legítimo que no puede usar sus datos verdaderos).

h. Resumen de beneficios clave de calidad de datos

Adoptar sistemas de validación y administración de ID de contacto como parte integral del RDS para la próxima generación mejorará la calidad de los datos, ya que hará que sea más difícil que los registratarios inserten datos falsos en el RDS y reducirá la incidencia de fraudes y robo de identidad. En concreto, los beneficios de adoptar los

---

de datos y cambios en la interfaz gráfica de usuario o la aplicación de cliente, por lo tanto, no se recomienda en este momento, pero se debe estudiar.

[23] Este control de calidad de único se puede realizar de manera relativamente sencilla en el modelo de RDS sincronizado, pero puede ser más difícil de efectuar en el modelo de RDS federado.

principios de validación y precisión de datos recomendados por el EWG incluyen los siguientes:

- Mejor capacidad para que los individuos y las organizaciones controlen y mantengan sus propios datos de contacto sin importar dónde se los use en el ecosistema de nombres de dominio.
- Mayor dificultad para que los criminales obtengan nombres de dominio, ya que todos los contactos se deben validar a un nivel mínimo cuando se los crea o se los actualiza. Los requisitos de acreditación del validador deben permitir la identificación y la sanción de validadores pícaros o negligentes que no cumplen con las normas operativas. Si se identifican criminales mediante la registración de un solo dominio, se pueden identificar otros dominios del mismo criminal y mitigarlos mediante los PBC en común.
- La creación de datos más consistentes entre varios nombres de dominio registrados por un registratario. A pesar de que puede haber costos por adelantado en la validación de un contacto, proporcionar un ID de contacto único y portátil permite que las registraciones adicionales no presenten problemas y debería reducir significativamente los costos de mantenimiento de varios registratarios.
- Mejor capacidad para detectar información de contacto no válida con el paso del tiempo y aplicar correcciones a todo el conjunto de dominios usando la información de contacto. Los requisitos de controles de validación periódica realizados por validadores, o cuando se realicen las actualizaciones, deberían resaltar problemas de información de contacto desactualizada y aplicar todas las actualizaciones a las registraciones de nombres de dominio afectados con un solo cambio.
- Mejoras de costos y eficiencia para todo el ecosistema. A pesar de que se introducen nuevas complejidades al sistema de registración, la administración de contactos se puede separar de la administración de registración de dominios, lo que permite aplicar actualizaciones a gran escala en dominios y la localización de la administración de los datos de contacto.
- Capacidad de que los proveedores de servicios actualicen detalles de contacto sin problemas y sin tener que actualizar registraciones individuales de dominios para aquellos que aparecen como contactos con un propósito. En situaciones de muchos proveedores, esto podría permitir una fácil actualización a miles o incluso millones de nombres de dominio.

- Reducir el abuso mediante suplantación de identidad en datos de registración proporcionando validación de identidad opcional. A pesar de que la validación opcional de identidad posiblemente genere costos para el titular de contacto que la obtiene, la capacidad de reducir los abusos por suplantación (robo) de identidad que sufren a menudo entidades de alto nivel, grandes proveedores de servicios o individuos objetivo de ataques maliciosos, seguramente vale la pena.
- La separación de la administración de datos de contacto y la validación de registración/administración de nombres de dominio alinea los asuntos de los datos de manera más cercana con los datos, lo que facilita la aplicación de la ley de protección de datos pertinente, ya que los validadores se pueden encontrar en jurisdicciones locales respecto del titular de contacto, sin importar la ubicación del registratario o del registro.
- Los validadores pueden prestar servicios en la lengua materna de los registratarios y los titulares de contacto, lo que mejora la calidad y la precisión de los datos, y reduce los costos por validación. Esto podría permitir que los registradores presten servicios en idiomas que no podían ofrecer con facilidad ni validar por sí mismos, a través de un conjunto distribuido de validadores.

VI. Consideraciones legales y contractuales

En su labor, el EWG se ha guiado por principios jurídicos generales:

Los datos personales deberán ser: • procesados legalmente, de manera justa y transparente en relación con el asunto de los datos; • recopilados para propósitos específicos, explícitos y legítimos, y no se los debe procesar de manera incompatible con dichos propósitos; • adecuados, pertinentes y limitados al mínimo necesario en relación con los propósitos para los cuales se procesan; y • precisos y actualizados según sea necesario para los propósitos especificados.
El procesamiento legal, incluso la transferencia y la divulgación (en función de la jurisdicción pertinente), se puede basar en: • el consentimiento del asunto de los datos; • la necesidad de desempeño de un contrato del cual forma parte el asunto de los datos; y • la necesidad de cumplimiento de una obligación legal de la cual es sujeto el controlador.
Se debe garantizar el derecho de acceso a la información y de corregir la inexactitud del asunto de los datos.

El EWG recomienda que estos y otros principios relacionados que normalmente se encuentran en la ley de protección de datos sean considerados en la elaboración de políticas finales y de procesos de implementación del RDS. Además, es bien sabido que, en algunas jurisdicciones, los derechos de privacidad se extienden a las personas jurídicas y a las entidades con respecto a la libertad de expresión y la libertad de asociación. El EWG reconoce estos dos conjuntos separados de derechos, que están protegidos por separado y de manera diferente en todo el mundo.

Sobre esta base, el EWG evaluó opciones y luego formuló principios de RDS para la protección de los datos y de la privacidad, y para el acceso de organismos de aplicación de la ley. Esos principios de EWG se presentan en esta sección, con el apoyo de los principios de cumplimiento contractual, responsabilidad y auditoría.

a. Principios de protección de datos

Hoy en día, las prácticas que pretenden hacer frente a la legislación nacional aplicable sobre privacidad y protección de los consumidores son desiguales. Algunas leyes exigen que cuando los datos se exportan fuera de la jurisdicción de la persona o del procesador de datos regido por esa ley, se apliquen protecciones de datos similares o equivalentes. La directiva europea de 1995 sobre protección de datos no permite la transferencia de datos fuera de esa jurisdicción a menos que la legislación local se haya evaluado como "adecuada". Muchas otras jurisdicciones fuera de la Unión Europea han buscado disposiciones contractuales sólidas, pero en cualquier caso, la mayoría de las leyes exigen que los que tienen los datos personales no los transfieran ni revelen a otros sin su consentimiento a menos que se garantice la protección. La limitación de responsabilidad se puede acumular en este punto de transferencia. Por el momento, la ICANN ha abordado este tema permitiendo una exención en el contrato de RAA para los registradores que demuestren que están sujetos a la ley de protección de datos que prohíbe la custodia de datos. Esta no es la única disposición del ecosistema de la ICANN que representa un riesgo para aquellos que buscan cumplir con la ley de protección de datos, por lo que se ha sugerido que el statu quo debe ser examinado cuidadosamente. Dado el enfoque que asumió el EWG al asumir la responsabilidad de este trabajo, se analizó el requisito de ser responsable por la protección de datos.

Por el momento, los requisitos de que la entidad que recibe los datos personales debe garantizar la protección adecuada y consistente con la protección provista para el asunto de los datos "en casa " tendría que cumplirse **caso por caso**, dependiendo de si la entidad que recibe datos brinda protección de datos legislados o una protección adecuada similar. Esto significa que, o bien la adecuación está garantizada por la ley aplicable a la entidad que recibe los datos u otras garantías están puestas en marcha para permitir que la transferencia de datos sea legal en virtud de la legislación aplicable al asunto de los datos.

Mecanismos de protección de datos

Dada la situación actual, se examinaron cuatro opciones progresivas para la protección de datos personales a través del ecosistema de RDS:

(0) no hacer nada;

(1) presentar mecanismos para facilitar la recopilación y transferencia de datos legales;

(2) introducir mecanismos que tratan de armonizar la privacidad y la protección de datos en todo el ecosistema de la ICANN, para proporcionar un "piso" básico de

protección de datos que establece las mejores prácticas aceptadas de política de privacidad; y

(3) presentar la política como un conjunto de "normas corporativas vinculantes".

Nota: En esta sección, con "ecosistema de RDS" se hace referencia a todos los actores enumerados en la Sección VIII (c), Relaciones contractuales y cumplimiento, y la Sección VIII (d), Responsabilidad y auditoría. Esto incluye a la ICANN (una corporación sin fines de lucro de los Estados Unidos), todos los registradores y registros de gTLD (cada uno de los cuales opera como empresa independiente con base en diferentes países) y todas las nuevas entidades acreditadas propuestas por el EWG en este documento: el proveedor de RDS, los validadores, los aprobadores de credenciales con protección de seguridad, los acreditadores de usuarios del RDS, el cumplimiento de la ICANN y otras entidades encargadas de manejar datos personales.

Opción (0): "No hacer nada"

No hacer nada podría resultar en una complejidad muy alta debido a la persistencia del riesgo de incumplimiento de la ley de protección de datos y la necesidad de examinar cada registración para determinar la ley aplicable. Probablemente genere costos extra para algunos operadores, en particular, registros. Para los registradores, podría imponer el alto costo de supervisar la adecuación de la protección requerida por los registradores y registros. Tal vez agregue la posibilidad de inseguridad jurídica para todas las partes, incluso la ICANN y otras partes interesadas del sistema de nombres de dominio. El aumento en el número de gTLD y la variedad de lugares de registro crea nuevos desafíos en materia de la ley aplicable y la jurisdicción de los regímenes contractuales de la ICANN, ya que corresponden a la protección de consumidores y privacidad del registratario. El desorden, la incertidumbre y las prácticas irregulares pueden requerir más esfuerzo por parte de la ICANN para garantizar el cumplimiento contractual y reducir el riesgo potencial. Estos desafíos existen independientemente de la cuestión del RDS. Con la introducción de 1000 gTLD, la cuestión se vuelve más complicada. Lo más importante es que la protección del asunto de los datos no se puede garantizar de forma coherente. Un marco para la armonización, que reduzca el riesgo, minimice la carga y disminuya la complejidad resultaría beneficioso para todas las partes interesadas.

Opción (1): Presentar mecanismos para facilitar la recopilación y transferencia de datos legales

La segunda opción considerada es la introducción de un sistema que evalúe la ley de protección de datos y privacidad pertinente, y presente la legislación en una lista para que las partes interesadas puedan aplicarla. Así los individuos podrían ser conscientes de dónde estaban sus datos y qué ley se correspondía. El RDS podría aplicar esta lista automáticamente a través de un "motor de reglas" como se define en la siguiente sección. Si una persona vive en un país que tiene ley de protección de datos y esa ley se aplica fuera del país a los datos personales transferidos del individuo a un tercero (en este caso, el registrador) podría aplicar esa ley. Si el registrador se encuentra en un país cuyas leyes de protección de datos se aplican a todas las personas (es decir, no solamente a sus propios ciudadanos), definitivamente se aplicaría esa ley. Los datos en cuestión o en el alcance de nuestros propósitos son solamente los que se recopilan en el RDS[24]. Codificar los datos respecto de las jurisdicciones que corresponden en el ecosistema podría simplificar la vida de los actores involucrados, garantizaría los derechos de protección de datos (si hubiera) del registratario y reduciría el riesgo de incumplimiento. Sin embargo, en las jurisdicciones sin una ley de protección de datos que se aplique al negocio de registración de nombres de dominio, registros o la ICANN y sus mecanismos de cumplimiento, este escenario ofrece poca protección al registratario individual. Esto podría resultar en un sistema de varios niveles de derechos de privacidad, algunos registratarios no tendrían ningún derecho humano y otros los tendrían todos, y una causa de acción con supervisión judicial.

Opción (2): Introducir mecanismos que tratan de armonizar la protección de datos en todo el ecosistema del RDS para proporcionar un "piso" básico de protección de datos que establezca las mejores prácticas aceptadas de política de privacidad.

Se podrían redactar cláusulas contractuales para rectificar las deficiencias de protección de la privacidad (se analiza en más detalle en la etapa de implementación) y podrían basarse en una serie comúnmente aceptada de protección de la privacidad, que sería la base de una política de privacidad de la ICANN. Esta política podría ser concisa y enumerar las cláusulas pertinentes en un apéndice. Esto podría permitir la transferencia sin restricciones de datos entre los actores del ecosistema de RDS, proporcionando un nivel de protección de datos lo suficientemente alto para evitar objeciones por razones de privacidad personal, protección de datos y derechos de los consumidores.

[24] Esto no necesariamente simplificaría la vida del registrador, que controla información mucho más confidencial, como datos bancarios, información de tarjetas de crédito, registros de atención al cliente, etc., que no son transferidos al RDS, aunque un "motor de reglas" sería realmente útil en algunas situaciones, dada la complejidad del sistema de gTLD futuro.

Los mecanismos para facilitar la recopilación legal de datos y su transferencia por el ecosistema de RDS pueden tener diferentes formas, pero todos deberían basarse en una política de protección de datos coherente y que pueda aplicar el RDS. La ICANN podría aplicar esta política con todas las partes interesadas por medio de disposiciones contractuales, como se hace con la mayoría de las otras políticas.

Opción (3): Sobre la base de la opción (2) anterior, la política desarrollada podría presentarse como un conjunto de "normas corporativas vinculantes", como la reconocen la APEC y la UE en la ley de protección de datos y de privacidad.

Esta opción permitiría simplificar las transferencias de datos entre los 28 países miembros de la Unión Europea, ya que proporciona una determinación de la protección de datos adecuada para los propósitos de los estados de la organización, lo que elimina el carácter ad hoc de las decisiones de protección de datos dictadas por flujos de datos de todo el ecosistema de RDS. A pesar de que esta opción puede requerir más tiempo, puede reducir el riesgo de incumplimiento y garantizar una mejor protección. También puede proporcionar una supervisión independiente de la política de privacidad.

N.º	Resumen de los mecanismos de protección de datos considerados
(0)	No hacer nada.
(1)	Una solución mínima debería: a) identificar las transferencias para las que la protección adecuada de la privacidad está garantizada por la ley y publicar la lista respectiva; e b) introducir reglas comunes en el contrato para aquellos actores del ecosistema de RDS cuyas transferencias no estarían protegidas por una adecuación legal suficiente, lo que brinda a la función de cumplimiento una plataforma única y simple para el mantenimiento.
(2)	Se podría redactar una política básica de privacidad de la ICANN para el RDS, basada en las mejores prácticas estándar para protección de la privacidad, y podrían elaborarse cláusulas contractuales tipo para dar efecto a esta política en todo el ecosistema del RDS. Se pueden incluir cláusulas tipo en todos los contratos entre la ICANN y los actores del ecosistema del RDS que participan en transferencias de datos, lo que garantizaría un nivel de protección de datos lo suficientemente alto para facilitar la transferencia sin restricciones dentro del ecosistema.
(3)	Tomando a la ICANN como una corporación multinacional sin fines de lucro, todo

	el ecosistema de RDS bajo su control podría estar sujeto al instrumento de normas corporativas vinculantes (BCR), que han demostrado ser efectivas para permitir las transferencias internacionales de datos dentro de una organización. En este caso, el ecosistema se convierte en el asunto de cumplimiento. La ICANN podría verse como un "controlador de datos", para usar terminología de APEC y UE, ya que establece requerimientos contractuales y de políticas.

Evaluación:

Opción (0): No hacer nada. Dada la creciente complejidad global del sistema, y el foco en el aumento de la precisión y la responsabilidad, esta opción fue considerada inaceptable.

Opción (1): Mecanismos para facilitar la recopilación y transferencia de datos legales. Esta opción es más compleja y dinámica, ya que leyes cambian en las distintas jurisdicciones y se tendría que considerar un flujo de datos complejo dentro del ecosistema. Como se analizó anteriormente, un registratario puede tener un registrador en una jurisdicción diferente, utilizar un validador en una tercera jurisdicción, mantener datos en un registro en una cuarta jurisdicción y confiar en un proveedor de RDS en una quinta jurisdicción.

Opción (2): Cláusulas contractuales tipo que tratan de armonizar la protección de datos en todo el ecosistema del RDS. Esta opción puede exigir el cumplimiento de la legislación aplicable a las partes interesadas establecidas, en particular, a registratarios, registradores, Registros y la ICANN. También puede incluir a los nuevos actores del ecosistema del RDS recomendados en este informe: validadores, proveedores del RDS, acreditadores de usuarios del RDS, etc.

Además de obligar a cumplir con las leyes locales de protección de datos, esta opción, que incluye elementos comunes provenientes de la ley de protección de datos de la APEC y la UE, podría hacer mucho para garantizar el cumplimiento. Las cláusulas podrían especificar las condiciones de consentimiento, los derechos de acceso, las políticas de retención y otros elementos mediante, por ejemplo, la incorporación de requerimientos de la Unión Europea en materia de procesamiento de datos y elementos apropiados abordados por normas corporativas vinculantes. Estas cláusulas contractuales tipo no necesariamente requerirían la autorización o la supervisión de autoridades de protección de datos, excepto en jurisdicciones donde dichas autorizaciones son obligatorias.

Opción (3): BCR para el ecosistema del RDS. Además de obligar a cumplir con las leyes locales de protección de datos, esta opción podría incluir elementos comunes provenientes de la ley de protección de datos de la APEC y la UE. Como sucede con la opción (2), las cláusulas podrían especificar las condiciones de consentimiento, los derechos de acceso, las políticas de retención y otros elementos mediante, por ejemplo, la incorporación de requerimientos de la Unión Europea en materia de procesamiento de datos y elementos apropiados abordados por normas corporativas vinculantes. Estas cláusulas contractuales tipo no necesariamente requerirían la autorización o la supervisión de autoridades de protección de datos, excepto en jurisdicciones donde dichas autorizaciones son obligatorias. Sin embargo, las BCR tendrían que ser adaptadas a las especificaciones del ecosistema del RDS. Las BCR son, posiblemente, más aplicables a entidades corporativas con una estructura de control tradicional que a un ecosistema conectado vagamente como el operado por la ICANN, pero es sin duda el caso de que las empresas multinacionales imponen sus normas de privacidad vinculantes por medio de exactamente los mismos tipos de contratos que utiliza la ICANN para acreditar y controlar a las partes interesadas.

En conclusión, "no hacer nada" no es una opción real, sobre todo, si se aceptan las recomendaciones del EWG para mejorar la precisión y la responsabilidad. La opción (1) puede tornarse legalmente muy compleja y no proporciona derechos equitativos para todos los registratarios, mientras que la opción (3) genera preocupaciones respecto de la aplicabilidad en el ecosistema del RDS (es decir, ¿son factibles las normas corporativas vinculantes? ¿Serán aceptadas? ¿Cuáles serían las implicaciones para la ICANN en términos de responsabilidad?).

Por lo tanto, el EWG recomienda la opción (2): elaborar una política usando las cláusulas contractuales tipo armonizadas con las leyes de protección de datos para implementar los requerimientos de la política y garantizar, por medio de diversos mecanismos de auditoría, que estas protecciones de la privacidad se apliquen mediante contratos entre todos los actores del ecosistema del RDS involucrados en el manejo de información personal.

Implementación de mecanismos de protección de datos

Para todos los escenarios mencionados anteriormente, la cuestión de la implementación del RDS es relevante, específicamente con respecto a la localización del proveedor de RDS.

Si el RDS va a contener datos personales, sería conveniente que esos datos se encontraran en una jurisdicción que proporcione los derechos de protección de datos

aplicables, para evitar preguntas relacionadas con la legalidad de las transferencias de datos y la responsabilidad por la violación de datos. Este problema está claro si el RDS contiene datos residentes y ubicados junto con el procesador de datos. Se debería aplicar un marco similar para su consideración, incluso si los datos no residen sino que se los transfiere para su procesamiento (por ejemplo, su validación) y luego se los envía a otra ubicación. El EWG consideró tres opciones de implementación de protección de datos.

N.º	Resumen de las opciones de implementación de protección de datos consideradas
(0)	La opción "No hacer nada" corresponde si no se tiene en cuenta el nivel legal de protección de datos aplicable a la localización del RDS cuando se realiza la elección geográfica. Esto podría hacer que el RDS se localice en una jurisdicción con un bajo nivel de protección de datos.
(1)	El RDS podría prever una compartimentación legal. Específicamente, los elementos de datos se podrían etiquetar según la ley aplicable del asunto de los datos (por ejemplo, el registratario) y se los podría tratar de manera acorde. Para lograr esta compartimentación legal, el RDS podría implementar un "motor de reglas" que aplicaría las leyes de protección de datos correspondientes a cada transferencia específica. Más específicamente, el "motor de reglas" se refiere a una característica que podría implementarse en el RDS para administrar (a) el almacenamiento, la recopilación y el procesamiento de información de nombres de dominio sobre la base de registratarios, contactos, registradores, registros y jurisdicciones de RDS (representados por los siguientes elementos de datos: registratario y código de país de contacto, registrador y jurisdicciones de registro) y (b) leyes de protección de datos de las jurisdicciones aplicables, de acuerdo con la política por definirse de la ICANN para el RDS. Esto es de por sí complejo, como se describe más arriba, y difícil de aplicar si el RDS se encuentra en una jurisdicción sin ley de protección de datos que proporcione acceso a un tribunal.

N.º	Resumen de las opciones de implementación de protección de datos consideradas
(2)	La localización del RDS se selecciona de acuerdo con el criterio de la transferencia de datos más fácil y menos complicada. Hacer esto puede implicar seleccionar ubicaciones para el almacenamiento de datos del RDS donde la ley de protección de datos nacional aplicable ofrezca un nivel más alto de protección.

Evaluación:

La **opción (0) "No hacer nada"** mantiene el statu quo y aumenta la complejidad de muchas transferencias de datos porque:

- Restablece un proceso que dificulta, y en la práctica imposibilita, respetar los marcos jurídicos;
- Impone cargas administrativas y legales a los registradores, y a otros actores del ecosistema, incluso al cumplimiento de la ICANN; y
- Dista de ser transparente respecto del cumplimiento de la privacidad y la ley de protección de datos local, y no es escalable.

La **opción (1) de compartimentación legal mediante un "motor de reglas"** es innovadora, pero se deberá probar técnicamente su viabilidad. En términos legales, hay una serie de preguntas abiertas, en especial, relacionadas con la definición, la aceptación legal y la implementación de un sistema de este tipo.

La **opción (2) de localización de datos en jurisdicciones seleccionadas** puede ser una solución elegante y simple para lograr un alto nivel de protección para todas las transferencias de datos. Sin embargo, esta opción no permite por sí misma la aplicación de todas las leyes de protección de datos locales de cada asunto.

Debido a que la opción (0) no es viable, y las opciones (1) y (2) no se excluyen entre sí, *el EWG recomienda que se consideren las opciones (1) y (2) por el momento, como medio de implementación de una protección de datos de alto nivel que se garantizará por medio de cláusulas contractuales tipo y políticas.*

Después de considerar todas estas opciones relacionadas con las políticas de protección de datos, los mecanismos y la implementación, el EWG acordó los siguientes principios:

N.º	Principios de protección de datos

N.º	Principios de protección de datos
105.	Se deben adoptar mecanismos para facilitar la rutina de recopilación de datos que cumpla con la ley y la transferencia entre actores del ecosistema de RDS.
106.	Las cláusulas contractuales tipo armonizadas con las leyes de privacidad y protección de datos se codifican en una política y se aplican mediante contratos entre todos los actores del ecosistema del RDS involucrados en el manejo de información personal.
107.	Se debe considerar un sistema de información para aplicar leyes de protección de datos (es decir, un "motor de reglas") y la localización del almacenamiento de datos del RDS como dos medios para implementar la protección de datos de alto nivel requerida. Esto se debe garantizar a través de cláusulas contractuales tipo, que se derivan de una política de privacidad lógica para el ecosistema del RDS.

b. Principios para el acceso a datos mediante la aplicación de la ley

A diferencia del caso de protección de datos, la protección jurídica del asunto de los datos en los casos de acceso mediante la aplicación de la ley no se puede "exportar". Para acceder mediante la aplicación de la ley, se consideran tres opciones.

N.º	Resumen de opciones consideradas de acceso mediante aplicación de la ley
(0)	"No hacer nada". El acceso mediante aplicación de la ley debería seguir las reglas existentes en la medida en que la legislación nacional tenga acceso a los datos de RDS almacenados en cada repositorio de datos en el nivel nacional respectivo. En el portal centralizado del RDS, se brindará acceso según la legislación nacional del país huésped del portal del RDS.
(1)	En el nivel del portal de RDS central, donde los datos no están disponibles públicamente y donde no se requieren procedimientos legales específicos por parte de la aplicación de la ley según la legislación nacional aplicable, se pueden especificar las condiciones de acceso para el sistema del RDS y se pueden implementar de dos maneras: a) Europol e Interpol podrían celebrar un acuerdo contractual con el RDS para implementar y ejecutar el sistema, que actúa como intermediario activo en tiempo real para todos los accesos de aplicación de la ley y es responsable de la protección de los datos y el uso adecuados. b) Europol e Interpol podrían celebrar un acuerdo contractual con el RDS para servir como acreditadores de usuarios para la comunidad de

N.º	Resumen de opciones consideradas de acceso mediante aplicación de la ley
	aplicación de la ley, para evaluar solicitantes de emisión de credenciales de RDS que luego utilizan organismos para acceder a datos de RDS restrictos y ser responsable de la protección de los datos y el uso adecuados.
(2)	Además, a nivel central, se podrían establecer mecanismos que permitan el acceso al portal central de RDS mediante el cumplimiento de la ley, incluso cuando existan requerimientos específicos en las relaciones bilaterales tradicionales que serían manejadas en virtud de los tratados de asistencia legal mutua (MLAT). Una compartimentación de los datos con respecto a la legislación aplicable podría apoyar el establecimiento de un mecanismo de ese tipo.

Evaluación:

La **opción (0) "No hacer nada"** claramente no proporciona el valor agregado de acceso para la aplicación de la ley.

En la **opción (2) de MLAT en el nivel de portal de acceso de usuarios del RDS**, no se espera que ninguno de los elementos de datos restrictos recomendados disponibles mediante RDS requiera una autorización judicial adicional para el acceso mediante aplicación de la ley. Por lo tanto, la opción (2) no se debe considerar más.

La **opción (1) de enfoque de portal de acceso de usuario acreditado del RDS** facilita el acceso mediante aplicación de la ley. Aunque ambas variantes (1a) y (1b) pueden servir de base para estructuras existentes, la variante (1a) (acceso acreditado con la compartimentación a través de un intermediario en tiempo real) también se basaría en los mecanismos existentes de aplicación de la ley y evita la creación de una capa adicional de complejidad. Sin embargo, la capacidad de detectar y remediar potenciales abusos individuales todavía tendría que garantizarse.

La variante (1a) se analiza con más detalle en la Sección IV (c), Acreditación de usuarios de RDS, escenario n.º 3, que detalla cómo los posibles acreditadores, como la Interpol, pueden representar solicitudes de acceso autorizado mediante aplicación de la ley a RDS mientras evitan posibles abusos. Consulte los principios de acreditación de usuarios del RDS para conocer las recomendaciones relacionadas.

Además, para la opción (1), se debe garantizar que el marco jurídico para la aplicación de la ley nacional en jurisdicciones donde se almacenan datos del RDS no anula el marco

establecido por el RDS. La geografía de localización del RDS, por lo tanto, es de importancia crítica.

N.º	Principios de acceso mediante aplicación de la ley
108.	El RDS debe almacenar los datos en las jurisdicciones donde la aplicación de la ley sea de confianza para todo el mundo, independientemente del modelo de implementación.

c. Principios de relación contractual y cumplimiento

El EWG recomienda el siguiente conjunto de principios respecto de las relaciones contractuales entre las partes dentro del ecosistema del RDS:

N.º	Principios de relación contractual
109.	El RDS debe ser operado por un proveedor externo que sea una organización no gubernamental internacional.
110.	La ICANN debe celebrar contratos apropiados con un proveedor externo de RDS para permitir el cumplimiento, la auditoría y la disponibilidad.
111.	La ICANN debe celebrar contratos apropiados con validadores, proveedores de servicios de privacidad/representación, aprobadores de credenciales con protección de seguridad y demás proveedores que puedan interactuar con el RDS (consulte la Sección III (c), Principio n.º 1).
112.	La ICANN debe modificar los acuerdos existentes (RAA, acuerdos de registro) para incorporar el RDS y eliminar los requerimientos legados.
113.	El RDS se debe aplicar a todos los registros de gTLD, tanto existentes como nuevos. No debería permitirse ninguna cláusula de derechos adquiridos ni excepciones especiales.

d. Responsabilidad y principios de auditoría

El EWG recomienda que los actores del ecosistema del RDS sean responsables por las acciones realizadas con la información de registración, de la siguiente manera:

N.º	Responsabilidad y principios de auditoría
114.	Todas las entidades que forman el ecosistema del RDS deben ser responsables de uno o más de los requisitos indicados en la Tabla 6: a) proporcionar información de registración precisa y confiable; b) usar la información solamente para el propósito designado;

N.º	Responsabilidad y principios de auditoría
	c) proteger la información recopilada, almacenada y reenviada; d) validar o autenticar la información recopilada; e) actualizar la información previamente proporcionada de manera oportuna; f) aplicar las políticas de privacidad del RDS y los términos de uso (ToU); g) detectar abusos relacionados con información de registración; h) responder y hacer un seguimiento de los reclamos; i) cumplir con las políticas establecidas de términos de uso y de servicio; j) establecer mecanismos para impedir la recolección de datos por terceros y la creación masiva de cuentas fraudulentas; k) fijar un proceso continuo de auditoría y remediación. Las siguientes partes interesadas[25] tienen roles de responsabilidad en el ecosistema del RDS: a) Usuarios del RDS que buscan datos (USD), enumerados en la Sección III b) Registratarios c) Registradores[26] d) Registros[27] e) Proveedor de servicios de directorio de registración f) ICANN g) Proveedores de servicios de privacidad/representación h) Aprobador de credenciales con protección de seguridad i) Validadores j) Acreditadores de usuarios del RDS k) Contactos con un propósito l) Proveedores de servicios de custodia
115.	El RDS debe establecer procedimientos para manejar los reclamos sobre la falta de disponibilidad de datos, el uso indebido de los datos, el acceso no autorizado a los datos, las violaciones de políticas de privacidad y la entrada de datos inexactos; por ejemplo: elementos de datos de contacto para informes de abusos y un portal para recibir reclamos de USD y registratarios.
116.	El RDS debe establecer remediaciones escaladas de datos inexactos; por

[25] Estos roles y responsabilidades se extienden a agentes de partes interesadas y los asigna (por ejemplo, revendedores).

[26] Según se define en http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm

[27] Según se define en http://newgtlds.icann.org/en/applicants/agb/agreement-approved-09jan14-en.pdf

N.º	Responsabilidad y principios de auditoría
	ejemplo: advertencia de correo electrónico, marca de usuario/navegador visible en los registros, acción de cumplimiento de la ICANN y otros nuevos incentivos para fomentar la precisión. (Consulte la Sección V, Mejora de la calidad de los datos, para conocer los requisitos de precisión).
117.	El RDS debe establecer remediaciones escaladas por acceso no autorizado a los datos; por ejemplo: advertencia de correo electrónico, límites de frecuencia, bloqueo temporal, suspensión de la acreditación, finalización y otras medidas disuasorias. (Consulte la Sección IV, Mejora de la responsabilidad, para conocer los requisitos de acceso restricto).
118.	El RDS debe establecer remediaciones escaladas por uso inadecuado de los datos; por ejemplo: advertencia de correo electrónico, límites de frecuencia, bloqueo temporal, suspensión de la acreditación, finalización y otras medidas disuasivas. (Consulte la Sección III, Usuarios y propósitos, para conocer los fines permisibles).
119.	El RDS debe establecer mecanismos de auditoría con el fin de detectar el abuso de credenciales de acceso de RDS y violaciones de términos de uso; por ejemplo: mecanismos para detectar patrones de comportamiento inusuales. (Consulte la Sección IV, Mejora de la responsabilidad, para conocer los requisitos de acreditación de usuarios del RDS).
120.	El RDS debe establecer mecanismos de auditoría con el fin de detectar el abuso de datos de registración para propósitos que no son los establecidos; por ejemplo: mecanismos para detectar patrones de comportamiento inusuales. (Consulte la Sección III, Usuarios y propósitos).
121.	El RDS debe establecer mecanismos de auditoría con el fin de detectar el abuso por parte de validadores; por ejemplo, capacitación de validadores, muestreo aleatorio periódico de datos para controlar la validación adecuada. (Consulte la Sección V, Mejora de la calidad de los datos).
122.	El RDS debe establecer mecanismos de auditoría con el fin de detectar el abuso por parte de acreditadores de usuarios de RDS; por ejemplo: mecanismos para detectar patrones de comportamiento inusuales. (Consulte la Sección IV, Mejora de la responsabilidad, para conocer las definiciones de abusos).
123.	El RDS debe establecer mecanismos de auditoría con el fin de detectar el

N.º	Responsabilidad y principios de auditoría
	abuso por parte de proveedores de servicios de privacidad/representación y aprobadores de credenciales con protección de seguridad; por ejemplo: mecanismos para detectar patrones de comportamiento inusuales. (Consulte la Sección IV, Mejora de la privacidad del registratario, para conocer las definiciones de abusos).
124.	Los USD del RDS deben estar de acuerdo con la auditoría de acceso a datos, uso y suministro de información precisa de identidad y propósito respecto de los términos de uso.
125.	El RDS debe establecer un proceso de remediación, suspensión o terminación de validadores si los datos no se validan, almacenan y protegen debidamente. (Consulte la Sección V, Mejora de la calidad de los datos, para conocer los requisitos de VR).
126.	El RDS debe establecer un proceso de remediación, suspensión o terminación de aprobadores de credenciales con protección de seguridad si la evaluación no es correcta ni adecuada. (Consulte la Sección VII, Mejora de la privacidad del registratario, para conocer los requerimientos).
127.	El RDS debe establecer un proceso de remediación, suspensión o terminación de acreditadores de usuarios del RDS si los datos no se acreditan, almacenan y protegen debidamente. (Consulte la Sección IV, Mejora de la responsabilidad, para conocer los requisitos de acreditador de usuarios del RDS).
128.	La ICANN debe establecer políticas de términos de servicio para garantizar que los registros, los registradores y los validadores proporcionan datos actualizados, precisos y oportunos al RDS. (Consulte la Sección VI, Consideraciones legales y contractuales, para conocer los requisitos de registro y RDS, que se reflejarán en el RAA y RIA).
129.	El RDS debe establecer un proceso de auditoría de registros, registradores y validadores, y un proceso para la presentación de informes a la ICANN si el registro, el registrador o el validador no proporciona datos actualizados, precisos y oportunos. (Consulte la Sección VI, Consideraciones legales y contractuales, para conocer los requisitos de registro y RDS, que se reflejarán en el RAA y RIA).
130.	El RDS debe establecer mecanismos de auditoría para asegurar la calidad continua y la integridad de los datos recopilados por el RDS y almacenados en

N.º	Responsabilidad y principios de auditoría
	custodia. (Consulte la Sección VIII, Almacenamiento de datos, custodia y registro).
131.	La ICANN debe establecer mecanismos de auditoría con el fin de detectar las infracciones de cualquier término de uso por parte del proveedor de RDS. Por ejemplo: permite el uso no autorizado de los datos, no responde a las quejas sobre abuso de datos, abuso de credenciales o abuso de validación. (Consulte la Sección VI, Consideraciones legales y contractuales).
132.	La ICANN debe establecer un proceso de remediación, suspensión o terminación del proveedor de RDS si no cumple con las responsabilidades contractuales. Por ejemplo: la disponibilidad, la confiabilidad, la privacidad, los derechos de acceso y los requisitos de rendimiento. (Consulte la Sección VI, Consideraciones legales y contractuales).
133.	La ICANN debe definir y establecer mejoras anuales hacia el logro de los principales objetivos del RDS: (I) mejor calidad de datos, (ii) mejor responsabilidad, (iii) mejor privacidad. El RDS debe demostrar un progreso sostenido en las tres áreas en tasas similares, con un proceso para identificar y solucionar problemas imprevistos que ralenticen la mejora de cualquier área.

En la tabla siguiente, se resumen las entidades del ecosistema del RDS y los tipos de requisitos de auditoría y responsabilidad que se les deben aplicar; esto amplía el Principio n.º 114.

Requisitos aplicables	Usuario de RDS que	Registratario	Registrador	Registro	Proveedor de RDS	ICANN	Proveedor de servicios	Aprobador de credencial	Validador	Acreditador de usuarios	Contacto con un	Proveedores de servicios
Suministro de datos precisos y confiables		✔	✔	✔	✔		✔	✔	✔		✔	✔
Uso para propósito designado	✔		✔	✔	✔	✔	✔	✔	✔			✔
Información segura			✔	✔	✔	✔	✔	✔	✔			✔
Validación/autenticación					✔				✔	✔		
Actualizaciones oportunas		✔	✔	✔			✔	✔	✔		✔	
Ejecución de políticas de privacidad			✔	✔	✔	✔	✔	✔	✔			✔
Detección de abusos					✔	✔				✔		
Proceso de reclamos			✔	✔	✔	✔	✔	✔	✔	✔		
Impedimento de que un tercero efectúe recolección masiva de datos				✔	✔				✔			
Auditoría y remediación					✔	✔				✔		

Tabla 6: Requisitos de cumplimiento en entidades del ecosistema del RDS

VII. Mejora de la privacidad del registratario

Es central para el mandato del EWG cómo diseñar un sistema que mejore la precisión de los datos recabados y ofrecer protección para los registratarios que busquen cuidar y mantener la privacidad. El EWG reconoce que la información personal está resguardada por leyes de protección de datos y que, incluso cuando no rige ninguna ley, existen razones legítimas para que los individuos busquen la mejor protección para su información personal. Asimismo, algunos negocios y organizaciones pueden buscar protección para su información con propósitos legítimos, por ejemplo, cuando van a lanzar una nueva línea de productos o, en el caso de las pequeñas empresas, cuando la información de contacto incluye datos personales.

En consecuencia, el EWG recomienda los siguientes principios básicos:

N.º	Principios de privacidad
134.	Además de la privacidad lograda gracias al cumplimiento de las leyes de protección de datos, el ecosistema del RDS debe afrontar necesidades de privacidad mediante la inclusión de lo siguiente: • Un servicio acreditado de privacidad/representación para la protección de datos personales y generales, y el cumplimiento de la ley de privacidad local; y • Un servicio acreditado de credenciales con protección de seguridad para personas en riesgo y en lugares en los cuales no se respete el derecho de libertad de expresión o se persiga a quienes deseen expresarse.
135.	Debe haber una acreditación para los proveedores de servicios de privacidad/representación y reglas para el suministro y uso de servicios de privacidad/representación acreditados.
136.	Fuera de los nombres de dominio registrados mediante servicios de privacidad/representación acreditados, todos los registratarios deberían asumir la responsabilidad por los nombres de dominio que registren.
137.	La ICANN debe investigar el desarrollo de una política de privacidad única y armonizada que rija las actividades del RDS de manera integral, como veremos a continuación.

Además de las leyes de protección de datos, otras leyes y constituciones nacionales de privacidad protegen los derechos de los cientos de millones de usuarios de Internet para

hablar en línea y expresar sus puntos de vista sin que se haga un seguimiento fácil e inmediatamente de sus nombres y direcciones. Estas leyes de privacidad son la Declaración de los Derechos Humanos de las Naciones Unidas (artículo 19),[28] que protegen los derechos de libertad de expresión y la libertad de expresión, y preservan la capacidad e incluso la obligación de los grupos, organizaciones, individuos y empresas (como los medios de comunicación y las empresas de periodismo) de analizar y criticar las prácticas de liderazgo, ejercicio del liderazgo y la administración de un país, cultura o sociedad.

Las leyes de privacidad que protegen la libertad de expresión a menudo reconocen la necesidad de ejercer estos derechos conforme a las reglas que disocian los nombres y las direcciones de las organizaciones y los grupos del discurso que están emitiendo y que pueden ser críticos de un gobierno, la sociedad, la comunidad o el barrio. Pueden fomentar el mercado de las ideas y la necesidad de las sociedades abiertas de comunicarse por encima de la autoridad que persigue a los oradores o la posibilidad de prejuzgar un mensaje, simplemente porque a alguien no le gusta su proponente.

Las leyes de privacidad y derechos constitucionales también pueden proteger la libertad de asociación, religión, etnia, moral y comunidad. Colectivamente, pueden impedir la necesidad de las personas o las organizaciones de declarar sus nombre e incluso sus direcciones en el ejercicio de puntos de vista minoritarios o poco populares, para que no se los persiga de inmediato y se los menosprecie o peor. En esta década de disturbios políticos de raíz y antagonismo a cualquier punto de vista opuesto, las leyes de privacidad protegen voces minoritarias y preservan la capacidad de los oradores en línea de instar poderosamente el cambio y la reforma.

A lo largo de este informe, se reconoce que cuando se habla de la privacidad y protección de datos personales, nos referimos a reconocer estos dos conjuntos separados de derechos, que a menudo están protegidos mediante una legislación diferente, algo que se hace de manera diferente en todo el mundo.

a. Principios de servicios acreditados de privacidad y representación

Actualmente, hay servicios que se ofrecen para ocultar la identidad o la dirección de las entidades que utilizan los nombres de dominio. Esto apareció debido a la naturaleza

abierta de WHOIS. Aunque haya muchas variantes, el acuerdo de acreditación de registradores de 2013 define dos servicios:

- Un "servicio de privacidad" es un servicio mediante el cual el nombre registrado se registra para el usuario beneficiario como titular de nombre de contacto, pero para el cual el proveedor de PP proporciona información de contacto alternativa y confiable para la visualización de información de contacto del titular de nombre registrado en el servicio de datos de registración (WHOIS) o un servicio equivalente.
- Un "servicio de representación" es un servicio mediante el cual el titular de nombre registrado licencia el uso de un nombre registrado al cliente de PP para proporcionarle el uso del nombre de dominio y se muestra la información de contacto del titular de nombre registrado en el servicio de datos de registración (WHOIS) o un servicio equivalente, en lugar de la información de contacto del cliente de PP.

En estas definiciones, "proveedor de PP" o "proveedor de servicios" es el proveedor de servicios de privacidad/representación, incluso un registrador y sus afiliados, según corresponda. "Cliente de PP" significa (independientemente de la terminología que utilice el proveedor de PP) el licenciatario, cliente, usuario beneficiario u otro destinatario de los servicios de privacidad o representación.

Los servicios de privacidad y representación actuales no están estandarizados. Los proveedores no tienen relación contractual con la ICANN, aunque el RAA 2013 introduce el concepto de acreditación por la ICANN y una base de obligaciones, como se detalla en una especificación provisional. No obstante, algunos proveedores también son registradores. Los registradores están sujetos al RAA, que establece lo siguiente acerca de los nombres de dominio registrados mediante representación:[29]

> 3.7.7.3 Todo Titular de Nombre registrado que tenga la intención de otorgar la licencia de uso de un nombre de dominio a un tercero será, no obstante, el Titular del Nombre registrado del registro y será responsable de facilitar su propia información de contacto completa y proporcionar y actualizar la información de contacto técnica y administrativa adecuada para permitir la resolución oportuna de *todos los problemas que surjan*[30] en relación con el Nombre registrado. Todo Titular de nombre registrado que otorgue una licencia

[29] El nuevo RAA 2013 fue aprobado por la Junta Directiva de la ICANN el 27 de junio de 2013; la sección 3.7.7.3 (citada en el presente) mantiene casi todo el texto del RAA de 2009, excepto por la adición de un período de 7 días.

[30] Nota: El EWG sugiere que la ICANN considere si "todos los problemas" podría ser demasiado amplio.

de uso de un Nombre registrado en virtud de esta disposición aceptará la responsabilidad por los daños causados por el uso indebido del Nombre registrado, a menos que revele la información de contacto actualizada suministrada por el licenciatario y la identidad del licenciatario en un plazo de siete (7) días a la parte que esté suministrando la evidencia razonable de daño procesable por parte del Titular del nombre registrado.

WHOIS para un dominio registrado hoy mediante un servicio de representación se ve de la siguiente manera:

```
  Nombre de dominio: EJEMPLO-DOMINIO.COM
      Fecha de creación: 31/10/2011
      Fecha de vencimiento: 31/10/2013
      Fecha de última actualización: 19/09/2012

   Registratario:
   Domains By Proxy, LLC                        ← Nombre del registratario =
representación
   DomainsByProxy.com                           ← Organización registrataria =
representación
   14747 N Northsight Blvd Suite 111, PMB 309   ← Dirección del registratario =
representación
   Scottsdale, Arizona 85260
   Estados Unidos

   Contacto administrativo: [lo mismo para el contacto técnico]
      Privado. Registración
      ejemplo-dominio.com @dominioporrepresentación.com     ← Correo
                                                            electrónico =
                                                            dominio@representación
      Domains By Proxy, LLC                                 ← Nombre = representación
      DomainsByProxy.com                                    ← Organización =
representación
      14747 N Northsight Blvd Suite 111, PMB 309            ← Dirección =
representación
      Scottsdale, Arizona 85260
      Estados Unidos
      (480) 624-2599      Fax -- (480) 624-2598             ← Teléfono/fax =
representación
```

WHOIS de un dominio registrado hoy con lo que actualmente se conoce como servicio de privacidad es similar, excepto que el nombre del registratario (y a menudo los nombres de contacto técnico/administrativo) identifican directamente al cliente de servicio de privacidad, no al proveedor de servicios de representación.

No hay procesos estándares que empleen todos los proveedores de servicios de privacidad/representación en la actualidad. Sin embargo, hay varias necesidades comunes, a menudo admitidas en cierto grado:

- Enviar comunicaciones a clientes de servicio de privacidad/representación, a menudo se realiza un reenvío automático de correos electrónicos a la

dirección de correo electrónico del contacto administrativo o técnico. Muchos proporcionan retransmisión, pero no todos los proveedores.

- Revelar la identidad del licenciatario y los detalles de contacto directo de un cliente de representación en respuesta a una queja sobre el nombre de dominio. Los procesos, la documentación, la capacidad de respuesta y las acciones realizadas varían y dependen con frecuencia de relaciones que se establecen entre los solicitantes y los proveedores.
- Desenmascarar la identidad del licenciatario mediante la publicación de su nombre y detalles de contacto del cliente de servicios de representación en el WHOIS.
- Cuando los solicitantes no pueden ponerse en contacto con un cliente de servicios de representación ni conseguir una resolución del proveedor de servicios de representación, a menudo recurren al registrador (que puede o no estar afiliado con el proveedor de servicios de representación).

Las deficiencias de los servicios de privacidad/representación están bien documentadas.[31] Para afrontar las necesidades de los registratarios de nombres de dominio y de las partes interesadas de servicios de privacidad/representación uniformes y confiables que permitan generar mayor responsabilidad, el EWG recomienda los principios siguientes:

N.º	Principios de servicios acreditados de privacidad/representación
	General
138.	La ICANN debe acreditar a los proveedores de servicios de privacidad/representación.[32]
139.	Como mínimo, el programa de acreditación debe seguir los compromisos de privacidad/representación en el marco de la especificación del RAA 2013.
	Principios de servicios acreditados de privacidad
140.	Las entidades y las personas físicas podrán registrar nombres de dominio

[31] Consulte el **Anexo B** para conocer los estudios e informes que documentan las deficiencias de WHOIS además de los servicios de privacidad/representación.

[32] El GNSO conformó un grupo de trabajo para elaborar políticas de acreditación de servicios de privacidad/representación. El EWG recomienda que el RDS reutilice las bases establecidas por el grupo de trabajo PPSAI, las modifique según sea necesario para reflejar los métodos de acceso de RDS y elementos de datos; más notablemente, P/P publicó contactos con un propósito.

N.º	Principios de servicios acreditados de privacidad/representación
	usando servicios de privacidad que no revelan los datos de contacto del registratario, a excepción de circunstancias definidas (por ejemplo, la violación de términos de servicio, citación judicial).
141.	La ICANN debe exigir que se incluyan términos específicos en los términos del servicio. Los términos de servicio deben incluir la obligación del proveedor de servicios de esforzarse por dar aviso en caso de suspensiones rápidas.
142.	Los servicios acreditados de privacidad deben proporcionarle al registrador (usando un PBC creado por medio de un validador) detalles de contacto precisos y confiables para todos los contactos con un propósito a fin de comunicarse con el proveedor de servicios de privacidad y las entidades autorizadas a resolver problemas técnicos, administrativos y otras cuestiones de parte del registratario.
143.	Los servicios acreditados de privacidad están obligados a reenviar al registratario los correos electrónicos recibidos en la dirección de correo electrónico de reenvío del registratario.
	Principios de servicios acreditados de representación
144.	Las entidades y las personas físicas podrán registrar nombres de dominio usando servicios de representación que registren nombres de dominio de parte del cliente de servicios de representación.
145.	Los proveedores acreditados de servicios de representación deben proporcionarle al registrador (usando un PBC creado por medio de un validador) sus propios detalles de contacto y nombre de registratario, incluso una dirección única de correo electrónico para contactar a la entidad autorizada para registrar el nombre de dominio de parte del cliente de servicio de representación.
146.	Como titular del nombre registrado, los proveedores acreditados de servicios de representación deben asumir las responsabilidades usuales de registratario por ese nombre de dominio, incluso el suministro de contactos con un propósito obligatorios precisos y confiables y otros datos de registración.
147.	Los servicios acreditados de representación deben proporcionarle al registrador (usando un PBC creado por medio de un validador) detalles de contacto precisos y confiables para todos los contactos con un propósito a fin de comunicarse con el proveedor de servicios de representación y las entidades autorizadas a resolver problemas técnicos, administrativos y otras cuestiones de parte del cliente del servicio de representación.

N.º	Principios de servicios acreditados de privacidad/representación
148.	Los servicios acreditados de representación están obligados a reenviar al registratario los correos electrónicos recibidos en la dirección de correo electrónico de reenvío del registratario, como se describe en el Anexo H.
149.	Los servicios acreditados de representación están obligados a responder a las solicitudes de revelación de manera oportuna, como se describe en los procedimientos de escalamiento del Anexo H.

b. Principios de credenciales con protección de seguridad

Se ha reconocido que algunas personas y grupos que desean mantener su anonimato en Internet, o al menos evitar la publicación de su dirección e información personal para aquellos que podrían ser una amenaza, tienen una necesidad legítima de proteger más la privacidad. Estas partes pueden ejercer sus derechos bajo la ley de privacidad si corresponde o utilizar los servicios de registro de representación. Pero por desgracia estos mecanismos pueden no ser lo suficientemente seguros para aquellos que están realmente en peligro. Si los detalles de la persona registrada no están disponibles en Internet, los perseguidores de estos individuos o grupos se comunican con los validadores, los registradores o los registros con sus solicitudes de información, a menudo utilizando técnicas de ingeniería social que estas partes no están bien preparadas para detectar.

El objetivo de ofrecer credenciales con protección de seguridad es proporcionar un registro anónimo y seguro para individuos o grupos amenazados. Esto puede incluir a aquellos que deseen ejercer la libertad de expresión (que está ampliamente considerada como protegida) o los oradores cuya identificación podría causar una amenaza para sus vidas o la de sus familias.

Aquí se presentan cinco ejemplos diferentes:

1. Minorías religiosas

En muchas jurisdicciones, existen minorías religiosas que se encuentran bajo amenaza de grupos más grandes de la población o de personas de la misma fe. Desean contar con un sitio web para compartir información con sus miembros, pero deben mantener el secreto de dónde y cómo operan. Por ejemplo, una sinagoga en Roma no da a conocer su dirección a causa de amenazas de bomba frecuentes; sin embargo, publica las horas de servicio para los miembros que conocen su ubicación.

2. Abuso doméstico

Muchas jurisdicciones ofrecen algún tipo de cambio de identidad para las personas que han sufrido violencia doméstica o que huyen de sus agresores. Esto también se aplica a aquellos que huyen de determinadas comunidades religiosas y cultos, y para quienes están bajo programas de protección de testigos. Los refugios para mujeres que sufren violencia doméstica pueden necesitar publicar sus servicios en Internet y asegurar los puntos de contacto y direcciones para las víctimas genuinas a fin de que lleguen a las instalaciones, etc. Los individuos y las familias que han cambiado su identidad pueden tener deseos legítimos de crear sitios web sin tener que revelar su verdadera dirección y la identidad. Se debe destacar que hay muchas personas que trabajan para gobiernos que operan bajo identidades cambiadas por diversas razones, en general, relacionadas con la aplicación de la ley y la seguridad nacional, y estas personas también necesitan mejor protección tanto en el campo como en la vida privada.

3. Discurso político

En varios países del mundo, un partido de oposición o los candidatos no victoriosos suelen irse después de una elección. También pueden querer administrar un sitio web desde donde proporcionar detalles sobre los acontecimientos en su país de origen o la persecución a la que son sometidos. El gobierno en el poder puede perseguir la página web, alegando traición u otros delitos, después de que aparezca documentación de sus abusos en el sitio web. Son situaciones delicadas, ya que el derecho a la libertad de expresión varía de estado en estado y rara vez se supera la acusación de traición. El derecho a registrar un dominio es por lo único que la ICANN y sus registradores acreditados se tienen que preocupar.

4. Grupos sociales, étnicos u otros

Los grupos étnicos a menudo sufren acoso y discriminación, y pueden querer administrar sitios web para compartir información vital para sus miembros. Por ejemplo, es posible que desee tener un sitio web donde los usuarios puedan publicar los incidentes de acoso sin temor a la identificación y represalias. Otros grupos, como los homosexuales, las lesbianas o los transexuales, pueden querer contar con un sitio web informativo muy normal para su comunidad; sin embargo, pueden tener miedo a la identificación de los miembros debido a las leyes restrictivas de su país o represalias por parte de vigilantes o grupos de

odio. Hay casos incluso de represalias contra los operadores de sitios que ofrecen información sobre la salud y la nutrición de las mujeres, información sobre derechos de reproducción, etc.

5. Periodistas que trabajan en territorio hostil

Los periodistas que publican historias desde territorios hostiles pueden tener la necesidad o deseen manejar un sitio web conservando la seguridad y la privacidad respecto de su identidad y su paradero, incluso la de sus colaboradores, traductores, etc.

Análisis de tecnologías de credenciales con protección de seguridad

Existen varias credenciales seguras en el mercado, como U-Prove de Microsoft (http://research.microsoft.com/en-us/projects/u-prove/) e Identity Mixer de IBM (http://researcher.watson.ibm.com/researcher/view_project.php?id=664). Estos enfoques permiten al destinatario probar distintos atributos, por ejemplo, que ha sido reconocido y autenticado por una autoridad de confianza, que han pagado por un determinado bien o servicio, sin revelar ninguna información personal sobre ellos mismos ni proporcionar ningún dato que permita rastrearlos con los atributos activados. Los usuarios de confianza tienen pruebas criptográficas seguras de que la entidad que emite las credenciales seguras cuenta con la aprobación de una autoridad de confianza y no necesitan saber quiénes son ni cómo consiguieron la aprobación.

Esa tecnología se puede utilizar para establecer un proceso mediante el cual las entidades en situación de riesgo descritas anteriormente pueden obtener un nombre de dominio registrado con una credencial protegida y segura. Ni el registrador ni el validador tendrían información sobre quién es la entidad en situación de riesgo más allá de los contactos necesarios responsables de atender problemas de DNS. Por lo tanto, legítimamente no pueden responder a solicitudes de información personal ni de dirección. Obviamente, existen dudas acerca de la conformidad técnica, el abuso y las medidas de mitigación de estos riesgos (véase más adelante). El punto clave es que los nombres de dominio registrados utilizando credenciales seguras, registradores y registros ya no cargarán con la responsabilidad ni el riesgo de identificación de las personas vulnerables por parte de sus agresores.

Cuestiones operativas

Para descomprimir los problemas y riesgos asociados con este tipo de servicio, el EWG analizó las siguientes situaciones posibles:

1. Un solicitante de información desea conocer el nombre o la dirección verdaderos de una persona, como se describió en 2, 3 y 4, para propósitos legítimos según esta persona (alegación de abuso de marca, deseo de comprar o vender un nombre de dominio, intento de investigación de la seguridad de un producto, etc.). Tenga en cuenta que en una situación de vida o muerte, un registrador está en una posición difícil cuando se trata de determinar si el solicitante está actuando de manera fraudulenta, y no se puede esperar que el personal entienda qué tipo de amenazas desconocidas pueden enfrentar las personas, sobre todo, en los casos de cambio de identidad.

2. Un solicitante se contacta con el registrador de un nombre de dominio (o un validador de PBC designado), alegando algún tipo de actividad delictiva o calumniosa y exige que se suspenda un sitio web utilizando ese nombre de dominio. En estas situaciones, se deben respetar los términos de servicio del proveedor de servicio de representación y del registrador, lo que puede dar lugar a una petición de revelar la identidad y la dirección del licenciatario del nombre de dominio. Sin embargo, para los nombres de dominio registrados utilizando credenciales seguras, en una revelación satisfactoria solamente se muestra información de la autoridad de confianza que aprobó la credencial segura. En este punto, la autoridad de confianza sería la responsable de investigar el potencial de abuso de DNS. En algunos casos, como la actividad criminal, se pueden suspender sitios web de manera expedita.

3. En los casos en que las agencias gubernamentales denuncian una intervención política en ascenso hasta el nivel de traición o de otros asuntos penales, los registradores pueden verse obligados a utilizar la suspensión expedita de sitios web utilizando nombres de dominio registrados con credenciales seguras, en función de la legislación pertinente en la jurisdicción.

Debido a estas limitaciones, las credenciales seguras pueden proporcionar mucha más seguridad a las entidades en situación de riesgo de la que tienen actualmente y si el nuevo RDS requiere mejor precisión de datos y responsabilidad, se requiere un servicio como este. Para lograr esto, sería necesario desarrollar las siguientes funciones clave:

1. Un proceso para establecer criterios de elegibilidad de credenciales seguras para personas en riesgo, comenzando por los ejemplos de usuarios mencionados y cualquier otro que la comunidad de la ICANN considere oportuno por medio del desarrollo de políticas.

2. Formularios de solicitud, certificaciones solicitadas y sistemas financieros, todo centrado en garantizar que las entidades en riesgo (y, en algunos casos, los responsables de emitir la certificación) estén seguras. En cualquier sistema anónimo, este es uno de los principales puntos débiles.
3. Una junta de revisión independiente para evaluar y aprobar las solicitudes de credenciales seguras y las certificaciones de entidades de confianza, como gobiernos que han autorizado cambios de nombre, organizaciones de las Naciones Unidas que participan en la protección de refugiados, asociaciones internacionales de periodistas, etc.
4. Las entidades de confianza (como las enumeradas en el punto n.º 3) que desean reenviar solicitudes de credenciales seguras y los nombres de dominio resultantes a la junta de revisión independiente o desde ella. Estas entidades de confianza, a las que se hace referencia en lo sucesivo como "destinatarios de credenciales seguras", deben dar fe de la necesidad de anonimato que tiene la entidad en situación de riesgo y aceptar la responsabilidad por cualquier posible abuso de DNS por los nombres de dominio registrados con credenciales seguras.
5. Proveedores acreditados de servicios de representación que deseen aceptar las credenciales seguras al registrar nombres de dominio con licencia de un aprobador de credenciales seguras, junto con los sistemas financieros para realizar los pagos.
6. Políticas relacionadas con procedimientos de suspensión expedita y otras mitigaciones de abuso de DNS. Esto podría incluir supervisión de seguridad mejorada de nombres de dominio registrados con credenciales seguras, para mitigar el posible uso indebido de DNS y el abuso, y para ayudar a proteger los nombres de dominio contra los ataques. Las entidades que declaran abusos de DNS podrían llevar su caso a la junta que aprobó la solicitud de la entidad en situación de riesgo; ese aprobador de credenciales seguras tendría que evaluar el abuso denunciado.

En la figura siguiente, se ilustran las posibles relaciones entre estas entidades, sus responsabilidades y el flujo de comunicación entre ellas.

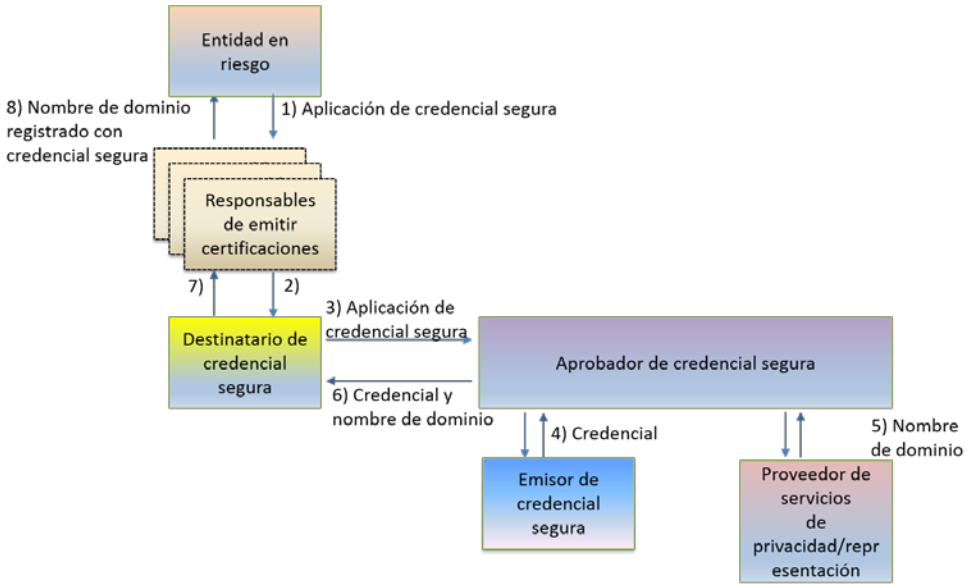


Figura 8: Modelo de credenciales con protección de seguridad

Riesgos residuales

Las credenciales seguras no se utilizan ampliamente porque, entre otras razones, su implementación es compleja, en particular, en relación con la registración y la revocación. Se ha afirmado que todas las partes deberían tener derecho a dicha registración, pero teniendo en cuenta el umbral de trabajo necesario para establecer este servicio y garantizar que no se utilice con propósitos fraudulentos o criminales, el EWG considera que este enfoque es inviable. El EWG recomienda que las credenciales con protección de seguridad se desarrollen con uso limitado y después de asegurarse de que las entidades que utilizan el servicio efectivamente tienen necesidad legítima de mantener el anonimato.

También se reconoce que una vez que un nombre de dominio está registrado y la página web está en funcionamiento, diversos tipos de metadatos de tráfico de Internet y el contenido pueden conducir a la identificación del usuario del nombre de dominio. Esto está más allá del alcance de la preocupación de la ICANN, que se centra exclusivamente en las cuestiones de registración de dominios y los datos extra que se recopilan, se usan y se divulgan para cumplir con los propósitos definidos en el mandato de la ICANN. La información generada a partir de la utilización real de un nombre de dominio debe ser responsabilidad de las entidades que solicitan y utilizan los nombres de dominio registrados con credenciales seguras, y puede ser importante para proporcionar información que subraya este riesgo. La responsabilidad de la ICANN termina con el sistema de nombres de dominio.

N.º	Principios para credenciales con protección de seguridad
150.	Los individuos y los grupos que pueden demostrar que estarían en riesgo si se los identificara deben solicitar de manera anónima y recibir nombres de dominios registrados usando credenciales seguras, con la ayuda de los responsables de emitir certificaciones y de terceros confiables para ofrecer una protección entre las entidades en riesgo y los registratarios/validadores.
151.	La ICANN debe facilitar el establecimiento de una junta de revisión independiente y confiable que valide los reclamos de individuos u organizaciones en riesgo para aprobar (y rechazar, cuando sea necesario) las credenciales. Dicha organización —de ahora en adelante, denominada "aprobador de credenciales seguras" (SCA)— debe desarrollar otros servicios, como educar a los usuarios acerca de los riesgos y las prácticas de seguridad en Internet.
152.	La ICANN debe facilitar el desarrollo o la concesión de licencias de un emisor de credenciales seguras que reconozca aprobaciones de SCA y genere las credenciales seguras correspondientes.
153.	Este aprobador de credenciales seguras debe utilizar credenciales seguras emitidas para dar licencia a nombres de dominio por medio de proveedores de servicios de representación de la manera habitual. La información del proveedor de servicio de representación aparecerá en el RDS. El RDS no debe conocer los datos acerca de la entidad en situación de riesgo que utiliza el nombre de dominio registrado con credenciales seguras y se debería utilizar algún sistema de pago anónimo o mediante representación.
154.	Los nombres de dominio registrados utilizando credenciales con protección de seguridad deben seguir ciertos procedimientos normales de suspensión y revelación de proveedores acreditados de servicios de privacidad/representación. Si el cliente del proveedor de servicios de privacidad/representación (es decir, el aprobador de credenciales seguras) no responde de manera oportuna, o muestra evidencia de abuso de DNS, puede generar la suspensión expedita de los nombres de dominio registrados con credenciales seguras.
155.	Para mitigar el riesgo, se puede considerar la mejora de la seguridad de la

N.º	Principios para credenciales con protección de seguridad
	supervisión de estos nombres de dominio, al reconocer que los nombres de dominio registrados utilizando credenciales con protección de seguridad podrían estar en riesgo de ataque cibernético o que la investigación de delitos sería difícil.
156.	Se deben establecer políticas y procesos para la aprobación y la revocación de solicitudes de credenciales con protección de seguridad. • El proceso de aprobación debe permitir cero o más emisores de credenciales para proteger suficientemente la identidad y la ubicación de la entidad en situación de riesgo del destinatario de credenciales seguras de confianza que presente la solicitud ante el SCA. El número y la identidad de los emisores de credenciales es transparente para el RDS; la única parte que se conecta directamente con el SCA en el destinatario de credenciales seguras. • El proceso de revocación debe permitir una protección similar de identidad y la ubicación del individuo en situación de riesgo, mientras se aplican términos de servicio de credenciales seguras. El SCA debe ser responsable de investigar los abusos de DNS declarados que impliquen credenciales seguras y de hacer cumplir los términos del servicio. En el caso de abuso de DNS lo suficientemente grave como para justificar la revocación de credenciales, el SCA deberá responsabilizar al destinatario de credenciales seguras.

c. Resumen de beneficios clave de privacidad

Con las mejoras en la precisión y la responsabilidad, será aún más importante proteger a los ciudadanos, especialmente a los más vulnerables. La incorporación de mecanismos y procesos de protección de datos, de servicios acreditados de privacidad/representación y de credenciales con protección de seguridad como parte integral del RDS para la próxima generación mejorará la privacidad de los registratarios y los contactos.

Los principios de protección de datos recomendados por el EWG deberían:

- Proteger de manera más uniforme los datos personales mediante la aplicación de una política armonizada de RDS, implementada de manera coherente en todo el ecosistema del RDS, y el uso de un "motor de reglas" para aplicar la ley local.
- Requerir que menos datos de contacto y de registración estén disponibles de manera pública y anónima.

- Proteger mejor los datos de contacto y del registratario contra el uso indebido.

Los principios para proveedores acreditados de servicios de privacidad/representación recomendados por el EWG deberían:

- Proporcionar una mayor claridad para los registratarios que busquen servicios de privacidad/representación mediante el establecimiento de un marco de acreditación para los proveedores que ofrecen estos servicios.
- Solicitar identificación del nombre de dominio como si hubiese sido registrado usando servicios ofrecidos por un proveedor acreditado de servicios de privacidad/representación.
- Indicar claramente en los datos de registración cómo ponerse en contacto con ese proveedor de servicios de privacidad/representación.
- Evitar que terceros utilicen los datos de contacto del proveedor de servicios de privacidad/representación sin autorización.
- Solicitar que el proveedor acreditado de servicios de privacidad/representación reenvíe el correo electrónico al registratario subyacente y responda consultas.
- Ofrecer expectativas más consistentes y previsibles de aplicación de la ley y otros informes de abuso de terceros y revelar los solicitantes.

Los principios de credenciales con protección de seguridad recomendados por el EWG deberían:

- Por primera vez, establecer procedimientos para permitir que los grupos vulnerables y desfavorecidos beneficiarse de las muchas ventajas de tener sus propios dominios en Internet.
- Proteger a aquellos que más necesitan utilizar Internet para propósitos de libertad de expresión y comunicación en grupos, mientras proporcionan soluciones para el abuso potencial.
- Eliminar la responsabilidad potencial de los validadores y los registradores, que hoy llevan la carga de responsabilidad de revelar información personal altamente confidencial mediante intentos de ingeniería social.
- Proporcionar seguridad adicional a los nombres de dominio registrados utilizando credenciales con protección de seguridad.
- Solicitar la suspensión expedita de sitios web registrados con credenciales con protección de seguridad con uso indebido de DNS.

VIII. Posibles modelos de RDS

a. Principios de diseño de modelo

Este informe proporciona detalles acerca de varios modelos alternativos explorados por el EWG, junto con el análisis de cómo estos modelos pueden satisfacer los principios recomendados por el EWG. Todos los modelos se evaluaron por medio de un conjunto de criterios multifacéticos, como se muestra en el Anexo F.

Al llevar a cabo su análisis, el EWG aplica los siguientes principios de diseño:

N.º	Principios de diseño de modelo
157.	**Recopilación:** En la actualidad, los registradores o los afiliados de registradores recopilan y almacenan información de registración de sus propios clientes (registratarios). Este proceso es inherentemente distribuido. Además de que los registradores o los afiliados de registradores continúen recopilando los datos de los registratarios, el EWG propone que validadores recopilen los datos de contacto.
158.	**Almacenamiento:** Existen diversos modelos posibles para el almacenamiento de información de registración en todos los gTLD. El EWG identificó una variedad de modelos posibles y destacó los dos que aparecen como los más prometedores. Recomienda que se seleccione uno por medio del criterio de evaluación, que se describe en el Anexo F**.**
159.	**Acceso:** Para proteger la privacidad del asunto de los datos, mediante una interfaz centralizada se debe permitir a los solicitantes acceder a información de registración en todos los gTLD, incluso el acceso a datos públicos no autenticados para cualquiera y a datos restrictos autenticados para usuarios acreditados.
160.	**Protocolo:** El RDS debe usar RDAP[33] o EPP (según corresponda para cada interfaz) como protocolo subyacente de acceso a directorios a fin de obtener información de registración de las ubicaciones de almacenamiento, donde sea que se encuentren.

[33] http://tools.ietf.org/html/draft-ietf-weirds-rdap-query-02

b. Modelos considerados

Para probar los modelos de sistema alternativos considerados por el EWG en su informe inicial y los modelos adicionales sugeridos por la comunidad de la ICANN, el EWG primero determinó qué modelos deberían ser analizados en profundidad. Cada modelo difiere en varios aspectos, incluso en la manera en que se copia la información de registración o se la consulta por medio del RDS. Estas diferencias se resumen en la siguiente tabla[34] y se explican con más detalle en el Anexo F.

MODELOS POSIBLES	Recopilación	Almacenamiento	Copia	Acceso
WHOIS actual	RR	RR/Ry	n/a	RR/Ry
Federado	RR y V	RR/Ry y V	n/a	RDS
Sincronizado*	RR y V	RR/Ry y V	RDS	RDS
Regional	RR y V	RR/Ry y V	Regional	RDS
Exclusión	RR y V	RR/Ry y V	Opcional	RDS
Evasión	RR y V	RR y V	RDS	RDS

* **Nota**: El modelo antes denominado **"RDS agregado (SDRA)"** ahora se llama **"RDS sincronizado (SRDS)"** para reflejar mejor la propiedad del modelo de utilización de los datos que residen en múltiples lugares de forma coherente y coordinada. TODOS los modelos que aquí se consideran se implementarían utilizando las mejores prácticas de ingeniería para lograr la tolerancia a fallos, alta disponibilidad y balanceo de carga, incluso centros de datos geográficamente dispersos, conectividad sólida e infraestructura redundante en cada centro de datos.

c. Modelo recomendado

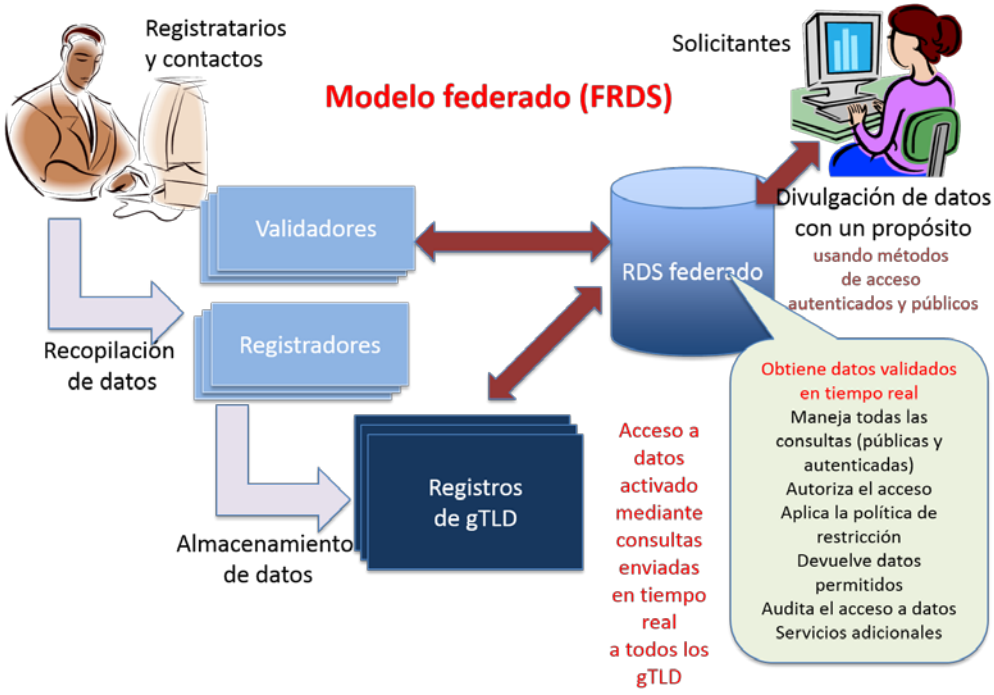
De los modelos de sistemas posibles identificados anteriormente, cada uno difiere en la manera en que se copia la información de registración o se la consulta por medio del RDS. El EWG analizó todos los modelos con detenimiento a fin de determinar el impacto de estas diferencias en varios atributos. Después de comparar estos modelos posibles, el EWG concluyó que, a excepción del WHOIS actual, todos son capaces de satisfacer en cierta medida los principios de RDS recomendados por el EWG. De estos, el EWG se

[34] Clave para la tabla de descripción de modelos: RR significa registradores; Ry significa registros; V significa validadores.

centró en los dos modelos más prometedores para examinarlos con mayor detenimiento: el modelo federado y el modelo sincronizado (antes denominado "modelo agregado"), **y recomendó el modelo sincronizado (SRDS).**

Modelo federado (segunda posición)

Este modelo describe un RDS que extrae información de registración a partir de áreas de almacenamiento distribuido operadas por los registros y validadores amplios, que utilizan un esquema de datos federado común. No hay agregación de datos en una sola ubicación de almacenamiento, sino acceso unificado público/restricto por medio del RDS a la información de registración obtenida en tiempo real de todos los registros de gTLD (datos de nombres de dominio) y validadores (información de contacto).



En este modelo, los datos son tomados por los FRDS de validadores y registradores/registros a través de RDAP. El flujo de contacto y los datos de registración asociados a este modelo se detallan en el Anexo I, Diagramas de flujo de procesos de RDS, y se ilustran en el Anexo E utilizando consultas de ejemplo.

Modelo sincronizado (SRDS) (recomendado)

Este modelo describe un RDS que copia, casi en tiempo real, datos recibidos de áreas de almacenamiento distribuido operadas por registros y validadores amplios en un sistema sincronizado que agrega y almacena datos en una arquitectura distribuida operada por el RDS.

En este modelo, el RDS es la fuente de datos autorizada y proporciona acceso autorizado, como se explicó. Como resultado, el RDS está más allá del requisito actual de RAA (y la necesidad actual) para tiempos de registro y registradores de actualizaciones. Los registradores, los registros y los validadores puede brindarles a los clientes acceso a sus propios datos, pero las solicitudes de datos restrictos debe ser respondidas mediante consultas al RDS. Este modelo responde a las recomendaciones de WHOIS anteriores y las solicitudes para reducir la confusión del consumidor en cuanto a dónde y cómo acceder a los datos de registración, y también minimiza los costos y los requisitos de responsabilidad para los registradores y los registros.

Aunque el RDS proporciona acceso a los datos, los datos no se almacenan en un solo lugar, sino en varias ubicaciones, diversificadas y redundantes según las mejores prácticas de ingeniería para sistemas que requieren tolerancia a fallos, alta disponibilidad y balanceo de carga. Los registros y los validadores continúan almacenando sus propios datos, pero el RDS puede usar copias sincronizadas de esos datos para procesar solicitudes de acceso con mayor efectividad.

En este modelo, los datos son enviados al SRDS por validadores y registradores/registros a través de EPP. El flujo de contacto y los datos de registración asociados a este modelo se detallan en el Anexo I, Diagramas de flujo de procesos de RDS, y se ilustran en el Anexo E utilizando consultas de ejemplo. A continuación se describe una comparación

relativa de estos dos modelos preferidos del EWG, después de aplicar la metodología indicada en el Anexo F.

- **Implicancias de seguridad**: ambos modelos generan resultados similares cuando se los evalúa en comparación con su impacto en la seguridad. Aunque hubo comentarios públicos de que un modelo agregado (posteriormente llamado sincronizado) como se sugiere en el informe inicial planteaba un riesgo debido al "punto único de falla" desde una interfaz centralizada, el EWG encontró que no era muy diferente de los riesgos planteados hoy por los grandes registros de gTLD y los sitios web de escala global de Internet. Las mejores prácticas actuales establecen que los grandes sistemas basados en la información utilizan varios centros de datos, sistemas de recuperación de desastres y almacenamiento de respaldo, además de una infraestructura totalmente redundante y geográficamente dispersa para mitigar estos riesgos.

  Los modelos sincronizados tienen la ventaja añadida de ser más capaces de garantizar la implementación consistente de seguridad y el cumplimiento de las políticas. Al utilizar estrechamente los componentes del sistema, un modelo sincronizado con arquitectura distribuida y administrado por un solo operador probablemente dé como resultado un enfoque más uniforme hacia los objetivos de seguridad establecidos en comparación con el modelo federado. En parte, esto se debe a que en un modelo federado, potencialmente miles de registros, registradores y validadores gestionarían sus respectivas bases de datos, con diferentes niveles de experiencia de registrador/registro/validador e inversión en prácticas de seguridad.

- **Preocupaciones de privacidad y jurisdicción**: ambos modelos generan resultados similares al evaluar los impactos de privacidad y jurisdicción. En el modelo federado, los datos se almacenan y se controlan en el nivel del registro, y las copias adicionales se conservan en otros lugares (en el centro de datos del registrador, del validador y de copias de seguridad ubicados en todo el mundo).El modelo sincronizado almacena y controla los datos en diferentes ubicaciones separadas del registro, y las copias adicionales se conservan en otros lugares (en el centro de datos del registrador, del registro, del validador y de copias de seguridad ubicados en todo el mundo). Al mirar todos los modelos evaluados, la mayoría no eliminó la transferencia de datos en múltiples ubicaciones, excepto por el "modelo de evasión", que elimina la necesidad de registros para almacenar los datos de contacto.

Además, el modelo sincronizado permite una aplicación más consistente de reglas para ajustarlas a los requisitos de privacidad locales, ya que es más fácil manejar reglas administradas por una entidad (el operador del RDS sincronizado) en lugar de por los posiblemente más de mil participantes en un modelo federado.

- **Acreditación**: la solicitud de requisitos de acreditación es posible en el modelo federado y el modelo sincronizado. Ambos modelos ofrecen características para realizar un seguimiento y hacer cumplir a los abusadores del sistema de acreditación, aunque puede ser más fácil hacer esto cuando la base de datos es administrada por una entidad en un modelo sincronizado, en comparación con los potencialmente más de mil participantes del modelo federado. Además, la implementación de un modelo federado requeriría gastos adicionales, así como las obligaciones contractuales detalladas, acuerdos de nivel de servicio y la supervisión de cumplimiento de la ICANN para apoyar la capacidad de ejecución y auditoría consistentes.

- **Funcionamiento**: el modelo sincronizado ofrece niveles de eficiencia en algunas áreas operativas que son más difíciles de lograr en el modelo federado. Por ejemplo, la implementación de un portal fácil de usar que muestra los datos en múltiples idiomas/códigos puede ser más fácil en el modelo sincronizado, donde los datos de contacto se podrían traducir o transliterar en un formato más compatible. Para lograr consistencia similar en un modelo federado, los acuerdos tendrían que tener especificaciones de los estándares de traducción/transliteración claramente articulados. Ambos modelos pueden ser diseñados para permitir auditorías aleatorias de calidad de los datos, aunque esto es probablemente más fácil de lograr en un modelo sincronizado.

  Las preocupaciones de latencia de datos y sincronización se reducen en un modelo federado, ya que los datos para mostrar provienen directamente del registro. Sin embargo, la extracción de datos a partir de un modelo sincronizado presenta problemas de latencia que pueden superarse haciendo que los validadores y los registradores (mediante registros) apliquen actualizaciones de EPP oportunas al SRDS (consulte el principio de cumplimiento n.º 108).

- **Implementación**: el modelo federado está más estrechamente alineado con el modelo distribuido del WHOIS actual que el modelo sincronizado. Sin embargo, los requisitos de rendimiento y las capacidades de búsqueda necesarios para proporcionar las características sólidas recomendados por el EWG requerirían

especificaciones detalladas y métricas de rendimiento que superan con creces lo ofrecido por el WHOIS actual. Se necesitaría una mayor supervisión y más recursos de cumplimiento de la ICANN para asegurar que todas las partes del sistema federado se desempeñen en el nivel esperado. Bajo cualquiera de los modelos, los participantes afectados tendrían que actualizar su plataforma de software para interactuar con la interfaz de RDS a fin de entregar los resultados de la búsqueda y los datos de contacto necesarios.

- **Costos**: los registradores y los registros (también los validadores) pueden obtener ahorros en costos con el modelo sincronizado, ya que se liberarán de la carga operativa de responder constantemente a consultas complejas desde la interfaz del RDS (como consultas inversas) como se requeriría en el sistema federado. En particular, la comparación de costos de los modelos (más detallada en el Anexo F) generó las siguientes conclusiones:

  (1) Con los supuestos utilizados, el sistema del RDS principal es un poco más económico en el modelo de RDS federado (FRDS) que el modelo de RDS sincronizado (SRDS). Sin embargo, el modelo federado es muy sensible al número de consultas inversas. **Con una mayor cantidad de consultas inversas, el modelo de FRDS se vuelve sustancialmente más costoso que el SRDS.** Por ejemplo, con una carga de consultas inversas del 3% en lugar del 1%, el costo del modelo de FRDS pasa a ser un 35% más costoso que el modelo de SRDS. Con un 5% de consultas inversas, se espera que el costo global de FRDS aumente alrededor del 85%. Este es un factor importante de incertidumbre y riesgo asociado con el modelo de FRDS. El modelo de SRDS se cree que es menos sensible a la cantidad de consultas inversas.

  (2) Además, **el modelo de FRDS tiene un costo más alto en todo el ecosistema debido a que [por su mayor costo] impacta en los operadores de registro**. En el modelo de FRDS, cada operador de registro tendría que implementar y admitir —en virtud del SLA— las respuestas a las consultas del RDAP de RDS, en tiempo real, incluso consultas inversas y consultas históricas de WhoWas. En el último caso, los datos históricos también tendrían que ser mantenidos por los operadores de registro, lo que aumenta aún más el costo a los registros. Tenga en cuenta que este costo adicional por registro estaría por encima del impacto en el sistema de RDS principal estimado anteriormente.

(3) Además, **el modelo de FDRS requeriría más operaciones de aplicaciones, soporte, mantenimiento y esfuerzos de prueba** en comparación con el modelo de SRD, ya que se espera una mayor interacción con los operadores de registro.

Se pueden encontrar más detalles acerca de este modelo de análisis de costos, su alcance y metodología, y los supuestos subyacentes y medición volumétrica en el Anexo F y en "*Análisis de costos del modelo de implementación del servicio de directorio de registración (RDS)*[35]" (Registration Directory Service [RDS] Implementation Model Cost Analysis), elaborado por IBM para la ICANN en marzo de 2014.

d. Principios de almacenamiento de datos, custodia y registro

N.º	Requerimientos comunes para almacenamiento, custodia y registro
161.	Se deben elaborar políticas de acceso, privacidad, retención y ubicación.
162.	Las políticas de almacenamiento, custodia y registro y las implementaciones deben cumplir con las leyes locales e internacionales.
	Principios de almacenamiento
163.	Para mantener sistemas redundantes y eliminar el único punto de falla, los datos deben estar alojados en múltiples ubicaciones (por ejemplo, validador, registrador, registro, custodia de datos y proveedor de RDS).
164.	Cuando hay datos en varios lugares, se debe mantener la consistencia.
165.	El RDS debe mantener los elementos de datos de forma segura, protegiendo la confidencialidad y la integridad de los elementos de datos en riesgo, y preservándolos del uso y la divulgación no autorizados.
166.	Los datos de transacciones deben almacenarse indefinidamente para mantener un registro exacto de los cambios de los datos en el tiempo y admitir la funcionalidad WhoWas, pero no más de los límites (si los hay) necesarios para el cumplimiento de las leyes de protección de datos aplicables. La información de contacto "huérfana" también se debe purgar periódicamente, en virtud de la legislación (por ejemplo, un año después de la baja).
	Principios [36]de custodia de datos

[35] https://community.icann.org/display/WG/EWG+Public+Research+Page

[36] La custodia hace referencia a la copia de seguridad del sistema cifrado en el sistema de un tercero de confianza (proveedor de servicios de custodia) para propósitos de recuperación en caso de desastre, fallo del sistema, etc. Consulte el RAA para obtener más detalles.

167.	Se deben efectuar auditorias de datos en custodia para evaluar su formato e integridad, y que los depósitos sean completos.
168.	La custodia y la auditoría de la custodia pueden ser más fáciles de coordinar con el modelo de RDS sincronizado.
169.	Los datos en custodia deben estar cifrados y ser opacos para los auditores.
170.	Los datos en custodia se deben conservar durante un período en virtud de los requisitos del acuerdo de acreditación del registrador, los acuerdos individuales de registración de gTLD y las leyes de protección de datos aplicables. En la actualidad, sería por la duración del patrocinio de la entidad que publica los datos y durante un período de dos años más a partir de esa fecha o más si así lo establece el acuerdo de registración de gTLD, pero no más de lo máximo permitido por la ley.
	Principios de registro
171.	Las consultas de RDS se deben registrar para proporcionar registros de cómo se utiliza el sistema.
172.	La agregación de registros puede ser necesaria para detectar abusos dirigidos a sistemas distribuidos.
173.	Los cambios se deben registrar para proporcionar un historial de elementos de datos en el tiempo.
174.	El acceso a los registros operativos de RDS debe limitarse a aquellos individuos y entidades autenticados, autorizados y de confianza con un propósito específico y "necesidad de saber". Debe incluir a los operadores autorizados del RDS (para confirmar y solucionar la operación de RDS) y a las entidades autorizadas de protección de datos (para supervisar el cumplimiento de RDS con la legislación de protección de datos). (Consulte también la Sección VIII (b), Acceso mediante aplicación de la ley).

IX. Costos e impactos

a. Principios de costos

Como se señala en el Anexo F, Metodología para la comparación de modelos, el EWG también consideró los costos y los impactos de RDS. El EWG reconoce que algunos aspectos del modelo recomendado incurrirán en nuevos costos, pero cree que muchos otros costos ocultos ocasionados por la ineficiencia y frecuente inexactitud del sistema

de WHOIS se reducirán. Como el RDS recomendado presta nuevos y mejores servicios, tanto los beneficios como los costos deben evaluarse. El enfoque recomendado les proporcionará a los responsables de elaboración de políticas la opción, por primera vez, de crear maneras para aquellos que soliciten datos de registración del sistema para contribuir con eficiencia a la operación de ese sistema.

Los costos de funcionamiento de WHOIS son desconocidos hoy, pero incluyen los costos de todo el ecosistema, no solamente de los registros y registradores que ofrecen los servicios de WHOIS. Los registradores no están obligados a desglosar los costos de WHOIS y pueden tener dificultades para distinguir entre los costos de prestación de esos servicios para gTLD en comparación con ccTLD. Otros actores del ecosistema incurren en costos como resultado de las ineficiencias y las deficiencias del WHOIS actual, como los titulares de marcas que pagan por los servicios de empresas de protección de marca y servicios de WHOIS comerciales para identificar a los cibercriminales.

El EWG recomienda los siguientes principios relacionados con los costos:

N.º	Principios de costos
175.	El acceso no autenticado (no restricto) a elementos de datos públicos debe ser libre.
176.	El acceso autenticado (restricto) mediante la aplicación de la ley a elementos de datos autorizados (según un proceso) puede estar sujeto a una consideración especial de costos.
177.	El diseño del RDS debe abogar por la minimización y la eficiencia de costos, sin comprometer otros objetivos.
178.	El RDS debería funcionar en un modelo de recuperación de costos.
179.	Para facilitar la migración de WHOIS, se debería crear una plataforma de desarrollo de software de RDS, financiada por la ICANN, para minimizar los costos de implementación de RDS en registradores/registros, validadores y acreditadores de usuarios de RDS.
180.	El suministro de esta plataforma de desarrollo de software no debería ser una carga excesiva para los demás usuarios de RDS.

Sin entrar en detalles específicos de implementación, los costos se podrían compartir en todo el ecosistema. Ejemplos en los que los costos podrían ser recuperados incluyen la imposición de diversas tarifas por licencia, dependiendo del usuario, los elementos de datos a los que se accede o el propósito (por ejemplo, tarifas por uso comercial, tarifas de suscripción para los usuarios avanzados o tarifas de acceso de alta calidad), o

percepción de tarifas por los servicios relacionados (por ejemplo, tarifas por credenciales o prevalidación).

El RDS también puede generar un ahorro de costos para los registros y los registradores, que ya no se necesitarán facilitar acceso público o cumplir con estrictos tiempos de respuesta de nivel de servicio. Los ahorros de costos también los pueden aprovechar los solicitantes que buscan datos mediante la eliminación de ineficiencias causadas por proveedores que no cumplen (registradores, registros, validadores o proveedores acreditados de servicios de privacidad/representación).

b. Beneficios en comparación con el WHOIS actual bajo el RAA 2013

Las deficiencias de WHOIS se han documentado durante la última década en diversos informes y estudios, destacados en el Anexo B. Las mejoras a WHOIS, incluidas en el nuevo Acuerdo de Acreditación de Registradores (RAA) 2013 (RAA 2013), junto con otras mejoras que resulten de la evaluación por parte de la Junta Directiva de la ICANN de las recomendaciones del equipo de revisión de WHOIS, abordaron algunas deficiencias que se perciben en WHOIS.

Aunque el RAA 2013 introdujo varias obligaciones nuevas, sobre todo, los requisitos de validación y verificación para mejorar la precisión, hay otras importantes deficiencias que siguen existiendo. Estas deficiencias se resumen a continuación, asignadas por secciones de este informe que contiene recomendaciones para lograr mayores beneficios.

WHOIS bajo el RAA 2013	Abordado por el RDS en la Sección
El acceso público y anónimo de todos los elementos de datos crea un ambiente donde pueden tener lugar la minería y el abuso, con poca responsabilidad o capacidad de remediación.	III, Usuarios y propósitos IV, Mejora de la responsabilidad VI (d), Responsabilidad y auditoría
Capacidad limitada para proteger la privacidad de los individuos.	VI (a), Protección de los datos VII, Mejora de la privacidad del registratario
Capacidad limitada para asegurar la integridad de los datos de registración; los registratarios pueden fácilmente insertar detalles de contacto falsos, incluso de terceros.	V, Mejora de la calidad de los datos V (g), Capacidad de datos de contacto únicos

WHOIS bajo el RAA 2013	Abordado por el RDS en la Sección
Falta de funciones de seguridad.	IV (b), Acceso a datos restrictos y no autenticados IV (c), Acreditación de usuarios de RDS
Falta de características de auditoría.	VI (d), Responsabilidad y auditoría VIII (d), Almacenamiento de datos, custodia y registro
Acceso no vinculado directamente con propósitos legítimos establecidos.	III, Usuarios y propósitos III (e), Contactos con un propósito
Interfaces y respuestas de WHOIS inconsistentes.	IV (b), Acceso a datos restrictos y no autenticados VIII, Posibles modelos de RDS
Falta de soporte o estándares para la visualización de datos de registración internacionalizados.	IV (b), Acceso a datos restrictos y no autenticados V (e), Interacción con validadores
Capacidad limitada para aplicar diferentes reglas para ajustarse a los diferentes regímenes de privacidad de datos.	VI (a), Protección de datos
Niveles de precisión inaceptables crean ineficiencias para aquellos que buscan comunicarse con los registratarios.	V, Mejora de la calidad de los datos III (e), Contactos con un propósito
Procesos de gestión engorrosos para actualizar los contactos en varios nombres de dominio.	V, Mejora de la calidad de los datos V (c), Proceso de remediación, auditoría y precisión
Dificultades para identificar y comunicarse con clientes de servicios de privacidad y representación.	III (e), Contactos con un propósito VII (a), Servicios de privacidad/representación Anexo H, Modelo de revelación y retransmisión

WHOIS bajo el RAA 2013	Abordado por el RDS en la Sección
No hay regulación de los servicios de privacidad/representación, más allá de los requisitos de RAA 2013 que se aplican solamente a los registradores y sus afiliados.	VII (a), Servicios de privacidad/representación Anexo H, Modelo de revelación y retransmisión

c. Evaluación de riesgos e impacto

Como se ha señalado en la Sección IV, Mejora de la responsabilidad, el EWG recomienda realizar una evaluación de riesgos de amplio alcance para confirmar que los principios de RDS aquí recomendados pueden generar la recopilación y divulgación de datos apropiada para los propósitos definidos, lo que alcanza el equilibrio justo entre los riesgos y los beneficios.

El 14 de marzo, el EWG invitó a todas las partes que proporcionan o utilizan los datos de registración de nombres de dominio de gTLD a participar en una encuesta en línea del riesgo del RDS, incluidos los registratarios, registradores, registros y del amplio espectro de individuos, empresas y otras organizaciones que utilizan datos de WHOIS. Esta encuesta les ofrece a los encuestados la oportunidad de avisarle al EWG los riesgos y beneficios que un sistema de reemplazo de WHOIS para la próxima generación podría tener para ellos.

Antes de finalizar este informe, el EWG examinó una instantánea de los riesgos y beneficios identificados a través de esta encuesta con la esperanza de reducir los riesgos y no previstos e innecesarios. Hasta el 29 de mayo 2014, la versión en inglés de la encuesta obtuvo 180 respuestas parciales; unas 100 entidades respondieron la encuesta en su totalidad. Los encuestados procedían de América del Norte (68%), Europa (35%), Asia (20%), Latinoamérica (14%), África (11%) y Oceanía (10%), y estaban equilibradamente divididos entre los que USABAN y SUMINISTRABAN datos de registración. Las respuestas arrojan luz sobre los riesgos y los beneficios más probables e impactantes en las siguientes áreas: técnica, operativa, legal y financiera, de seguridad y privacidad. Alrededor de dos docenas de encuestados también comentaron sobre los riesgos inevitables y aceptables, y sobre maneras de cambiar o reducir el riesgo.

Para permitir aportes amplios de la comunidad sobre este tema, el EWG ha decidido dejar abierta la encuesta del riesgo del RDS hasta julio de 2014 y poner en marcha las versiones traducidas. Las respuestas se utilizarán para informar la revisión de la Junta

Directiva de la ICANN de este informe y como entrada para un futuro análisis formal de los costos, los riesgos y los beneficios para todas las partes interesadas que se verían afectados por la sustitución de WHOIS por RDS[37].

[37] También consulte la evaluación del riesgo del DNS (primera iteración) para consulta pública de la ICANN.

X. Conclusiones y próximos pasos

Después de considerar los puntos de vista de las muchas partes interesadas del ecosistema que dependen de datos de registración, el EWG recomienda por unanimidad abandonar el modelo actual de WHOIS, dar a cada usuario el mismo acceso público y anónimo a los datos de registración de gTLD, con un sistema de reemplazo, desarrollado desde cero.

El EWG cree que los principios y el RDS para la próxima generación recomendados en este informe final brindan una base más sólida que la actual, una base desde la cual la proteger la privacidad personal y garantizar mayor precisión, responsabilidad y transparencia de todo el ecosistema de la ICANN en los años venideros. El RDS se basa, pero va mucho más allá, en las mejoras realizadas en el marco del recientemente negociado RAA 2013, como se describe con más detalle en la Sección IX (b).

Aunque el informe final puede parecer excesivamente detallado, no abarca todo. Como se indica en el Anexo A, el informe trata cada una de las preguntas formuladas por la Junta Directiva. Sin embargo, varias cuestiones quedan para responder de manera más plena en el futuro, ya sea en algún seguimiento sobre el proceso de desarrollo de políticas (PDP) o en cualquier esfuerzo de implementación relacionado.

- **Organismos de acreditación y políticas para comunidades de usuarios del RDS.** Debido a que comunidades de usuarios específicas pueden tener acceso a los datos restrictos para un propósito aprobado, durante la etapa de implementación, se deben examinar las políticas para identificar quién califica como miembro de esa comunidad, además de los posibles organismos de acreditación y los modelos adecuados para cada comunidad.
- **Extensiones requeridas para EPP y RDAP.** Como se detalla en el Anexo G, el EWG recomienda que se utilicen los protocolos estándares para apoyar las necesidades del RDS, pero ha identificado determinadas extensiones que podrían ser necesarias para apoyar plenamente el modelo de RDS y los elementos de datos recomendados.
- **Evaluación de riesgos e impacto.** Como se debatió en la Sección IX, el EWG recomienda que se lleve a cabo una evaluación completa de riesgos y un análisis de costo/beneficio antes de implementar el RDS recomendado, y ya puso en marcha una encuesta para recopilar aportes sobre ese proceso.
- **Política de privacidad del RDS.** Como se debatió en la Sección VII, el EWG recomienda que se redacte una política básica de privacidad de la ICANN para el RDS, basada en las mejores prácticas estándar para protección de la privacidad, y

podrían elaborarse cláusulas contractuales tipo para dar efecto a esta política en todo el ecosistema del RDS.

- **Traducción/transliteración de los datos de contacto.** Como no existe un proceso de desarrollo de políticas (PDP) en curso sobre esta cuestión, el EWG decidió no duplicar esfuerzos más allá de los principios identificados en la Sección IV (b) y, en su lugar, sugiere que el resultado del PDP actual se examine en el futuro para determinar la forma de aplicar las nuevas políticas del RDS.
- **Servicios de privacidad y representación.** Los principios del EWG relacionados con proveedores de servicios de privacidad/representación acreditados se deberán considerar en combinación con el trabajo en curso de la GNSO en este tema, lo que puede conciliar el resultado del PDP actual con cualquier implementación del RDS.
- **Ecosistema de validadores.** La creación de un programa de acreditación para validadores y los procesos utilizados para validar datos de contacto de registratarios y contactos ubicados en todo el mundo se debe seguir estudiando durante la fase de implementación.

El RDS refleja compromisos cuidadosamente diseñados y equilibrados con elementos independientes que no se deben separar. Estos compromisos son informados por los aportes recibidos por el EWG en los muchos comentarios públicos, seminarios web y consultas recibidos en su trabajo hasta la fecha. Como resultado, el EWG alienta a la Junta Directiva a remitir el informe final de la GNSO para su aprobación en su conjunto. Elegir la adopción de solamente algunos de los principios de diseño de RDS socava los beneficios de todo el ecosistema. Al EWG le preocupa que el examen de los componentes de forma individual pueda dar lugar a un nuevo desacuerdo y el estancamiento en la comunidad que ha acompañado los intentos anteriores de mejorar a WHOIS.

El EWG envió este informe final al director ejecutivo y a la Junta Directiva de la ICANN, lo publicó en Internet y llevará a cabo varias sesiones en la reunión de junio de 2014 de la ICANN en Londres. También brindará seminarios web y habrá otras oportunidades para analizar el informe y responder preguntas de la comunidad de la ICANN relacionadas con él. El informe final está destinado a servir de base para el proceso de desarrollo de políticas (PDP) de la GNSO solicitado por la Junta Directiva para la asignación de datos de registración de gTLD y para negociaciones contractuales, según corresponda. En el marco de consideración de este informe final por parte de la Junta Directiva y la comunidad de la ICANN, el EWG recomienda centrarse en las preguntas siguientes:

- ¿Se prefiere el RDS en lugar del WHOIS actual?

- De lo contrario, ¿la comunidad de la ICANN cree que debe continuar el sistema de WHOIS actual y que este puede cumplir con las necesidades de la Internet global en evolución?

El EWG confía en que este informe final cumpla con la directriz de la Junta Directiva de la ICANN para ayudar a redefinir el propósito y la disposición de datos de registración de gTLD y que sirva de base para ayudar a la comunidad de la ICANN (a través de la GNSO) a crear una nueva política mundial sobre los servicios de directorio de gTLD.

ANEXO A: RESPUESTA A LAS PREGUNTAS DE LA JUNTA DIRECTIVA

La resolución de la Junta Directiva que dirigió el trabajo del EWG incluyó una serie de preguntas específicas que debían ser respondidas a medida que se realizaba el análisis. En este anexo, se hace referencia a las secciones del presente informe que abordan las preocupaciones de la Junta Directiva.

Preguntas de la Junta Directiva y orientación	Secciones del informe
El EWG debe redefinir el propósito de lo siguiente: • recopilación • mantenimiento • suministro de acceso a datos de registración de gTLD y • consideración de medios para proteger datos	Sección III, Usuarios y propósitos Sección IV, Mejora de la responsabilidad
¿Por qué se recopilan datos?	Sección III, Usuarios y propósitos Sección VI (a), Elementos de datos
¿Cuál es el propósito de los datos?	Anexo D, Propósitos y necesidades de datos
¿Quién recopila los datos?	Sección V, Mejora de la calidad de los datos Anexo I, Diagramas de flujo de procesos de RDS
¿Dónde se almacenan los datos y por cuánto tiempo?	Sección VIII, Posibles modelos de RDS Sección VIII (d), Almacenamiento de datos
¿Dónde se custodian los datos y por cuánto tiempo estarán custodiados?	Sección VIII (d), Principios de almacenamiento de datos, custodia y registro
¿Quién necesita los datos y por qué?	Sección III, Usuarios y propósitos
¿Quién necesita tener acceso a los registros de acceso de los datos y por qué?	Sección VI (d), Responsabilidad y auditoría
¿Se debe brindar acceso público a detalles sobre registración de nombres de dominio?	Sección IV (b), Acceso a datos restrictos y no autenticados Sección VI (a), Elementos de datos Sección VII, Mejora de la privacidad del registratario
¿Se debe brindar acceso mediante aplicación de la ley a detalles sobre registración de nombres de dominio?	Sección III, Usuarios y propósitos Sección VI (b), Principios para el acceso a datos mediante la aplicación de la ley

Preguntas de la Junta Directiva y orientación	Secciones del informe
¿Se debe brindar acceso al titular de propiedad intelectual a detalles sobre registración de nombres de dominio?	Sección III, Usuarios y propósitos
¿Se debe brindar acceso a profesionales de seguridad a detalles sobre registración de nombres de dominio?	Sección III, Usuarios y propósitos
¿Qué valor obtiene el público con acceso a los datos de registración?	Sección II (b), Propósito Sección III, Usuarios y propósitos
De todos los datos de registración disponibles, ¿a cuáles necesita acceso el público?	Sección VI (a), Elementos de datos
¿El protocolo de WHOIS es la mejor elección para brindar ese acceso?	Sección IV (b), Acceso a datos restrictos y no autenticados Anexo G, Capacidad de los protocolos EPP y RDAP para admitir RDS
Seguridad	
¿Qué compone una necesidad legítima de aplicación de la ley?	Sección III, Usuarios y propósitos Sección VI (b), Principios para el acceso a datos mediante la aplicación de la ley
¿Cómo se identifica un agente del orden público?	Sección IV (c), Principios de acreditación de usuarios de RDS Sección VI (b), Principios para el acceso a datos mediante la aplicación de la ley
¿Qué datos de registración y qué nivel de precisión componen la verdadera identidad de la parte responsable?	Sección V, Mejora de la calidad de los datos Sección VI (a), Elementos de datos Sección VII (b), Credenciales con protección de seguridad
¿Qué datos de registración y qué nivel de precisión componen información valiosa para un agente del orden público que busca la verdadera identidad de la parte responsable?	Sección III, Usuarios y propósitos Anexo D, Propósitos y necesidades de datos
¿El protocolo de WHOIS es la mejor elección para brindarlo?	Sección IV (b), Acceso a datos restrictos y no autenticados Anexo G, Capacidad de los protocolos EPP y RDAP para admitir RDS
Titulares de propiedad intelectual	
¿El acceso a datos de registración de nombre de	Sección III, Usuarios y propósitos

Preguntas de la Junta Directiva y orientación	Secciones del informe
dominio es coherente con el acceso que tienen los titulares de propiedad intelectual a tipos similares de datos en otros sectores?	Sección IV (c), Principios de acreditación de usuarios de RDS
¿Cómo se identifica un titular de propiedad intelectual?	Sección IV (c), Principios de acreditación de usuarios de RDS
De todos los datos de registración disponibles, ¿a cuáles necesita acceso el titular de propiedad intelectual?	Sección III, Usuarios y propósitos Anexo D, Propósitos y necesidades de datos
¿Qué datos de registración sería adecuado poner a disponibilidad?	Sección VI (a), Elementos de datos
¿El protocolo de WHOIS es el método de acceso adecuado?	Sección IV (b), Acceso a datos restrictos y no autenticados Anexo G, Capacidad de los protocolos EPP y RDAP para admitir RDS

ANEXO B: ESTUDIOS PARA EVALUAR LAS DEFICIENCIAS DE WHOIS (EN INGLÉS)

- Informe del SSAC: SAC 051
- Informe del SSAC: SAC 054
- Informe del SSAC: SAC 055
- Principios de WHOIS del GAC
- Informe final del equipo de revisión de políticas de WHOIS
- Versión preliminar de procedimiento de la ICANN para el manejo de conflictos de WHOIS con la ley de privacidad
- Informe final de inventario de requisitos del servicio de WHOIS
- Informe inicial del grupo de trabajo 2 de WHOIS (2009)
- Informe final del grupo de trabajo sobre servicios de WHOIS (2007)
- Estudio para evaluar soluciones para la presentación y visualización de datos de contacto internacionalizados
- Informe final sobre el WHOIS amplio a cargo de la GNSO
- Informe provisional del EWG sobre datos de registración internacionalizados
- Revisión del procedimiento de la ICANN para el manejo de conflictos de WHOIS con la ley de privacidad
- Estudios sobre el WHOIS a cargo de la GNSO, incluso
    - Estudio sobre la precisión de la información de contacto de registratarios del WHOIS
    - Estudio sobre la prevalencia de nombres de dominio registrados usando servicios de privacidad/representación entre los cinco principales gTLD
    - Estudio del uso indebido de WHOIS
    - Estudio de identificación de registratarios de WHOIS
    - Estudio sobre el uso indebido de WHOIS mediante los servicios de privacidad/representación

- Encuesta de factibilidad de revelación y confianza de los servicios de privacidad/representación de WHOIS + Apéndices

ANEXO C: CASOS DE USO DE EJEMPLO

Como se describe en la Sección III, el EWG analizó los casos de uso reales que implican el sistema de WHOIS actual para identificar a los usuarios que desean acceder a los datos de registración de gTLD, sus propósitos para hacerlo y las partes interesadas y los datos involucrados. A continuación se proporciona una lista de casos de uso representativos considerados por el EWG.

Propósito	Casos de uso de ejemplo
Control de nombre de dominio	Creación de cuenta de registración de nombre de dominio
	Supervisión de modificación de datos de nombre de dominio
	Gestión de portfolio de nombres de dominio
	Iniciación de transferencia de nombre de dominio
	Supresiones de nombres de dominio
	Actualizaciones de DNS de nombres de dominio
	Renovaciones de nombres de dominio
	Validación de contacto del nombre de dominio
Protección de datos personales	Contacto con el proveedor de servicios de privacidad/representación
	Contacto con el aprobador de credencial segura
Resolución de cuestiones técnicas	Contacto con personal técnico de nombre de dominio
Certificación de nombres de dominio	Emisión de certificación de nombres de dominio
Uso individual de Internet	Contacto con el mundo real
	Protección del consumidor
Compra o venta de nombre de dominio comercial	Venta de nombre de dominio a través de un intermediario
	Información y protección (análisis de riesgo) respecto de una marca comercial de un nombre de dominio
	Adquisición de nombre de dominio
	Consulta por compra de nombre de dominio
	Historial de registración del nombre de dominio
	Nombres de dominio para un registratario especificado
Investigación de nombre de dominio de interés público/académico	Historial de registración del nombre de dominio
	Nombres de dominio para un contacto especificado
	Encuesta de registratarios de nombre de dominio o contacto designado

Propósito	Casos de uso de ejemplo
Acciones legales	Contacto del usuario del nombre de dominio
	Combatir el uso fraudulento de datos de registración
	Historial de registratario del nombre de dominio
	Nombres de dominio para un contacto especificado
Cumplimiento de normas regulatorias/contratos	Investigación impositiva en línea
	Procedimientos de UDRP
	Cumplimiento contractual del ecosistema del RDS
Mitigación de abusos relacionados con DNS e investigación criminal	Investigar nombres de dominio abusivos
	Investigación de actividades criminales fuera de línea
	Servicios de reputación de nombres de dominio
	Investigación de actividades criminales en línea
	Contacto en caso de abuso de un nombre de dominio afectado
Transparencia de DNS	Acceso público a los datos de registración
Actividades maliciosas en Internet	Secuestro de nombre de dominio
	Registración maliciosa de un nombre de dominio
	Extracción de datos de registración para usarlos en correos electrónicos no deseados o engañosos

Tabla 7: Casos de uso de ejemplo

Para ilustrar la metodología del EWG, a continuación se presenta un solo caso de uso. Consulte la Sección III para obtener descripciones adicionales de cada caso de uso y usuarios del RDS y necesidades de datos asociados.

Resolución de cuestiones técnicas. Contacto con personal técnico del nombre de dominio

Objetivo/escenario n.º 1:

Una persona experimenta un problema operativo o técnico con un nombre de dominio registrado. Quiere saber si hay alguien a quien pueda contactar para resolver el problema en tiempo real o casi en tiempo real, entonces usa el RDS para identificar a la persona adecuada, el rol o la identidad que cuente con la capacidad de resolver el problema. Una lista incompleta de ejemplos de cuestiones técnicas incluye el envío de correo electrónico y problemas de entrega, problemas de resolución de DNS y las cuestiones funcionales de sitios web.

Caso de uso en formato breve

Caso de uso: identificación de una persona, rol o entidad que puede ayudar a resolver una cuestión técnica con un nombre de dominio.

Casos de uso principal: Una persona accede al RDS para obtener información de contacto asociada con nombres de dominio registrados bajo uno o varios TLD. La persona envía un nombre de dominio al RDS para su procesamiento. El RDS devuelve información asociada con el nombre de dominio que identifica a una persona, rol o entidad que se puede contactar para

resolver cuestiones técnicas.

Caso de uso en formato informal

Título: identificación de una persona, rol o entidad que puede resolver una cuestión técnica con un nombre de dominio.

Actor principal: una persona experimenta un problema técnico con un nombre de dominio registrado.

Otras partes interesadas: operador del RDS (persona, rol o entidad asociada con el nombre de dominio que puede resolver cuestiones técnicas); registratario (quien puede saber sobre cuestiones operativas); validador (quien puede haber emitido el ID de contacto para el contacto técnico); registrador o proveedor de hosting (quien puede proporcionar un servicio operativo); proveedor acreditado de servicios de privacidad/representación (quien puede ayudar a contactar a la persona, rol o entidad asociada con el nombre de dominio que puede resolver la cuestión técnica).

Alcance: interacción con RDS

Nivel: tarea de usuario

Elementos de datos: los elementos de datos que permiten la comunicación en tiempo real o casi real son los más útiles en el contexto de este caso de uso. Entre estos, se incluye la dirección de correo electrónico, la dirección de mensajería instantánea, el número de teléfono y un indicador que identifica el método de contacto preferido especificado por el registratario. La sección 4 del RFC 2142 describe las recomendaciones para las direcciones de correo electrónico abuse@, noc@ y security@ para "proporcionarles un recurso para los clientes, proveedores y otras personas que están experimentando dificultades con el servicio de Internet de la organización", pero es importante tener en cuenta que el carácter público de estas direcciones a menudo las hace atractivas a remitentes de correo masivo no solicitado.

Historia: una persona (solicitante) que experimenta una cuestión técnica con un nombre de dominio registrado accede al RDS para obtener información asociada con nombres de dominio registrados bajo uno o varios TLD. Se puede acceder al RDS mediante un sitio web u otros medios de procesamiento electrónicos.

El solicitante envía un nombre de dominio registrado al sistema para su procesamiento.

El RDS procesa la solicitud y, o bien informa condiciones de error o consulta los datos de registración de gTLD para recuperar información relacionada con una persona, rol o entidad que haya sido previamente identificada como un recurso para ayudar a resolver cuestiones técnicas de este nombre de dominio.

El RDS devuelve los datos de registración asociados con el nombre de dominio o una condición de error que se encontró al recuperar los datos.

Figura 9: Caso de uso de ejemplo

ANEXO D: PROPÓSITOS Y NECESIDADES DE DATOS

El EWG analizó casos de uso para identificar a los usuarios que desean acceder a los datos de registración de gTLD, sus propósitos para hacerlo y las partes interesadas y los datos involucrados. En la tabla siguiente, se resumen los elementos de datos de RDS recomendados en la Sección IV y asignados a fines permisibles en la Sección III. Consulte la Sección IV para conocer recomendaciones de recopilación y divulgación para cada elemento de datos.

Elemento de datos	Propósitos
Nombre de dominio	Todos
Servidores de DNS	Control de nombre de dominio Resolución de cuestiones técnicas Certificación de nombres de dominio Compra o venta de nombre de dominio comercial Investigación de DNS de interés público/académico Cumplimiento efectivo de normas regulatorias/contratos Mitigación de abusos relacionados con DNS e investigación criminal
Nombre u organización de registratario Tipo de registratario ID de contacto del registratario Estado de validación de contacto de registratario Última marca de tiempo actualizada de contacto del registratario	Todos
Identificador de empresa de registratario	Control de nombre de dominio Certificación de nombres de dominio Uso individual de Internet Compra o venta de nombre de dominio comercial Acciones legales Investigación de DNS de interés público/académico Cumplimiento efectivo de normas regulatorias/contratos Mitigación de abusos relacionados con DNS e investigación criminal Transparencia de DNS

Elemento de datos	Propósitos
Dirección postal del registratario, incluso: Calle del registratario Ciudad del registratario Estado/provincia del registratario Código postal del registratario País del registratario	Control de nombre de dominio Certificación de nombres de dominio Compra o venta de nombre de dominio comercial* Investigación de DNS de interés público/académico* Acciones legales* Cumplimiento efectivo de normas regulatorias/contratos Mitigación de abusos relacionados con DNS e investigación criminal
Número de teléfono y extensión del registratario Número de teléfono alternativo y extensión del registratario	Control de nombre de dominio Resolución de cuestiones técnicas Certificación de nombres de dominio Compra o venta de nombre de dominio comercial* Investigación de DNS de interés público/académico* Acciones legales* Cumplimiento efectivo de normas regulatorias/contratos Mitigación de abusos relacionados con DNS e investigación criminal
Dirección de correo electrónico del registratario Correo electrónico alternativo del registratario	Todos
Fax y extensión del registratario	Control de nombre de dominio Certificación de nombres de dominio Compra o venta de nombre de dominio comercial* Investigación de DNS de interés público/académico* Acciones legales* Cumplimiento efectivo de normas regulatorias/contratos
Nuevos métodos de contacto que los registratarios pueden optar por publicar: SMS del registratario Mensajería instantánea del registratario Redes sociales del registratario Redes sociales alternativas del registratario URL de contacto del registratario URL para informe de abusos del registratario	Puede ser útil para cada fin permisible como alternativa a la dirección de correo electrónico del registratario
ID de contacto administrativo Elementos de datos de contacto administrativo	Control de nombre de dominio Certificación de nombres de dominio Compra o venta de nombre de dominio comercial Investigación de DNS de interés público/académico Transparencia de DNS

Elemento de datos	Propósitos
ID de contacto legal Elementos de datos de contacto legal	Control de nombre de dominio Certificación de nombres de dominio Investigación de DNS de interés público/académico Acciones legales Cumplimiento efectivo de normas regulatorias/contratos Transparencia de DNS
ID del contacto técnico Elementos de datos de contacto técnico	Control de nombre de dominio Resolución de cuestiones técnicas Certificación de nombres de dominio Investigación de DNS de interés público/académico Transparencia de DNS
ID de contacto para informe de abusos Elementos de datos de contacto para informe de abusos	Control de nombre de dominio Certificación de nombres de dominio Investigación de DNS de interés público/académico Mitigación de abusos relacionados con DNS e investigación criminal Transparencia de DNS
ID de contacto de proveedor de servicios de privacidad/representación Elementos de datos de contacto de proveedor de servicios de privacidad/representación	Control de nombre de dominio Protección de datos personales Certificación de nombres de dominio Investigación de DNS de interés público/académico Transparencia de DNS
ID de contacto comercial Elementos de datos de contacto comercial	Control de nombre de dominio Certificación de nombres de dominio Uso individual de Internet Investigación de DNS de interés público/académico Transparencia de DNS
Delegación de DNSSEC	Control de nombre de dominio Investigación de DNS de interés público/académico
Estado de registración Estado de cliente (registrador) Estado del servidor (registro)	Control de nombre de dominio Compra o venta de nombre de dominio comercial Investigación de DNS de interés público/académico Cumplimiento efectivo de normas regulatorias/contratos Mitigación de abusos relacionados con DNS e investigación criminal

Elemento de datos	Propósitos
Registrador Revendedor URL del registrador Número de IANA del registrador Dirección de correo electrónico para informe de abusos del registrador Número de teléfono de contacto para informe de abusos del registrador URL de sitio de reclamos de InterNIC	Control de nombre de dominio Compra o venta de nombre de dominio comercial Investigación de DNS de interés público/académico Cumplimiento efectivo de normas regulatorias/contratos Mitigación de abusos relacionados con DNS e investigación criminal Transparencia de DNS
Jurisdicción del registrador Jurisdicción del registro Idioma del acuerdo de registro	Todos
Fecha de registración original	Control de nombre de dominio Compra o venta de nombre de dominio comercial Investigación de DNS de interés público/académico Cumplimiento efectivo de normas regulatorias/contratos
Fecha de creación Fecha de actualización Fecha de vencimiento del registrador	Control de nombre de dominio Compra o venta de nombre de dominio comercial Investigación de DNS de interés público/académico Cumplimiento efectivo de normas regulatorias/contratos Mitigación de abusos relacionados con DNS e investigación criminal

Nota: El acceso a los elementos de datos restrictos del registratario a veces necesarios por propósitos marcados con * pueden implicar la aprobación de necesidad de saber; consulte la Sección III para conocer el debate sobre datos restrictos aprobados.

ANEXO E: ILUSTRACIÓN DE ACCESO A DATOS RESTRICTOS Y NO AUTENTICADOS

Los siguientes datos de registración amplían el ejemplo de WHOIS de RAA 2013 para reflejar los principios de RDS recomendados para la recopilación de datos y su divulgación.

La recopilación de los elementos grises es opcional; el resto son obligatorios.
Los elementos en negrita siempre son públicos; el resto puede ser restricto, a elección del registratario o del titular de contacto.

Estado de registración: X **Delegación de DNSSEC: delegación firmada (signedDelegation)** **Estado del cliente: eliminación prohibida (DeleteProhibited), renovación prohibida (RenewProhibited), transferencia prohibida (TransferProhibited)** **Estado del servidor: eliminación prohibida (DeleteProhibited), renovación prohibida (RenewProhibited), transferencia prohibida (TransferProhibited)** **Registrador: REGISTRADOR DE EJEMPLO LLC** **Revendedor: REVENDEDOR DE EJEMPLO** **Jurisdicción del registrador: JURISDICCIÓN DE EJEMPLO** **Jurisdicción del registro: JURISDICCIÓN DE EJEMPLO** **Idioma del acuerdo de registro: INGLÉS** **Fecha de creación: 2000-10-08T00:45:00Z** **Fecha de registración original: 2000-10-08T00:45:00Z** **Fecha de vencimiento de registración del registrador: 2010-10-08T00:44:59Z** **Fecha de actualización: 2009-05-29T20:13:00Z** **URL del registrador: http://www.registrador-ejemplo.tld** **Número de IANA del registrador: 5555555** **Correo electrónico para informe de abusos del registrador: email@registrar.tld** **Número de teléfono de contacto para informe de abusos del registrador: +1.1235551234** **URL de sitio de reclamos de InterNIC: http://wdprs.internic.net/**	Suministrado por registro o registrador
Nombre de dominio: EJEMPLO.TLD **Nombre del servidor: NS01.REGISTRADOR-EJEMPLO.TLD** Nombre del registratario: EJEMPLO DE REGISTRATARIO **Tipo de registratario: PERSONA JURÍDICA** **ID de contacto de registratario: xxxx-xxxx** (emitido por un validador acreditado por	Recopilados del registratario

RDS) **Estado de validación de contacto de registratario (del validador)** **Última marca de tiempo validada de contacto del registratario (del validador)** Organización del registratario: ORGANIZACIÓN DE EJEMPLO Identificador de empresa de registratario: DUNS 12345 (emitido por Dunn and Bradstreet) **Correo electrónico del registratario: CORREOELECTRÓNICO@EJEMPLO.TLD** Correo electrónico alternativo del registratario: EJEMPLO@OTRODN.TLD Calle del registratario: CALLE DE EJEMPLO 123 Ciudad del registratario: CUALQUIER CIUDAD Estado/provincia del registratario: AP Código postal del registratario: A1A1A1 **País del registratario**: AA Número de teléfono del registratario: +1.5555551212 Ext. telefónica del registratario: 1234 Número de teléfono alternativo del registratario: <númerocelular> Número de teléfono alternativo del registratario: 1234 Fax del registratario: +1.5555551213 Fax y extensión del registratario: 4321 SMS del registratario: <númerotextos> Mensajería instantánea del registratario: <identificadorMI> Redes sociales del registratario: <identificadorRS> Redes sociales alternativas del registratario: <otroidentificadorRS> URL de contacto del registratario: <enlace para formulario de contacto o instrucciones> URL de contacto del registratario: <enlace para formulario de informe de abusos o instrucciones>	
ID de contacto administrativo: xxxx-xxxx **(seguido de detalles de contacto administrativo de PBC*)**	El registratario debe publicar contactos con un propósito
ID de contacto técnico: xxxx-xxxx **(seguido de detalles de contacto técnico de PBC*)**	
ID de contacto legal: xxxx-xxxx **(seguido de detalles de contacto legal de PBC*)**	
ID de contacto para informe de abusos: xxxx-xxxx **(seguido de detalles de contacto para informe de abusos de PBC*)**	

ID de contacto técnico: xxxx-xxxx (solamente si el tipo de registratario = persona jurídica) (seguido de detalles de contacto de PBC comercial*)	
ID de contacto de proveedor de servicios de privacidad/representación: xxxx-xxxx (solamente si el tipo de registratario = proveedor de servicios de privacidad/representación) (seguido de detalles de contacto de PBC de proveedor de PP*)	

Leyenda: La recopilación de los elementos grises es opcional/condicional; el resto son obligatorios.

Los elementos en negrita siempre son públicos; el resto puede ser restricto, a elección del registratario o del titular de contacto. * Los elementos de datos de PBC no están completamente ilustrados aquí.

Ejemplo n.º 1: Consulta pública no autenticada para propósitos de resolución de cuestiones técnicas

1) El usuario envía la consulta de RDS no autenticada
(DN = MerchantZ.gtld; Propósito = resolución de cuestión técnica; Datos = todos)

2) El RDS evalúa la consulta:
Sin autenticación, porque la consulta no está autenticada
Sin autorización, así que se otorga acceso a datos públicos
El acceso está restringido a los datos públicos necesarios para la resolución de cuestiones técnicas
es decir, todos los datos públicos solicitados para el nombre de dominio + contacto técnico

3) El RDS recupera los elementos de datos solicitados:
Se recuperan datos de MerchantZ.gtld desde la caché de RDS (sincronizado) o del registro (federado) y envía solamente elementos de datos públicos definidos para este propósito, incluso

ID de contacto de registratario = 12345
Tipo de registratario = persona jurídica
Organización de registratario = MerchantZ, Inc.[38]
ID de contacto técnico = 67890

El ID de contacto técnico [67890] se recupera de la caché del RDS o del validador y solo obtiene los elementos de datos publicados expresamente por este contacto para este propósito, incluso

ID de PBC = 67890

Nombre de PBC = <*nombre de la entidad responsable de resolver los problemas técnicos del nombre de dominio MerchantZ.gtld*>

Dirección de correo electrónico de PBC = <*dirección de correo electrónico obligatoria de la entidad responsable de resolver los problemas técnicos del nombre de dominio MerchantZ.gtld*>

Dirección de correo electrónico alternativa de PBC = <*dirección de correo electrónico alternativa recomendada de la entidad responsable de resolver los problemas técnicos del nombre de dominio*>

[38] Los datos de la organización del registratario se recopilan de los registratarios que establecieron el tipo de registratario como persona jurídica o proveedor acreditado de servicios de privacidad/representación; pueden faltar cuando el tipo de registratario no se declara por defecto.

Número de teléfono de PBC = <*número de teléfono recomendado de la entidad responsable de resolver los problemas técnicos del nombre de dominio*>

URL de contacto de PBC = <*enlace de contacto recomendado publicado por la entidad responsable de resolver los problemas técnicos del nombre de dominio*>

<*cualquier elemento de datos públicos opcionales publicados por esta entidad*>

4) El RDS devuelve un error o una respuesta satisfactoria al usuario. Por ejemplo:

Nombre de dominio: MerchantZ.gtld *Estado de registración: x* *Estado del cliente: eliminación prohibida (DeleteProhibited), renovación prohibida (RenewProhibited), transferencia prohibida (TransferProhibited)* *Estado del servidor: eliminación prohibida (DeleteProhibited), renovación prohibida (RenewProhibited), transferencia prohibida (TransferProhibited)* *Registrador: REGISTRADOR DE EJEMPLO LLC* *Jurisdicción del registrador: JURISDICCIÓN DE EJEMPLO* *Jurisdicción del registro: JURISDICCIÓN DE EJEMPLO* *Idioma del acuerdo de registro: INGLÉS* *Fecha de creación: 2000-10-08T00:45:00Z* *Fecha de vencimiento de registración del registrador: 2010-10-08T00:44:59Z* *Fecha de actualización: 2009-05-29T20:13:00Z* *URL del registrador: http://www.ejemplo-registrador.tld* *Número de IANA del registrador: 5555555* *Correo electrónico para informe de abusos del registrador: email@registrar.tld* *Número de teléfono de contacto para informe de abusos del registrador: +1.1235551234* *URL de sitio de reclamos de InterNIC:http://wdprs.internic.net/*
Nombre del servidor: NS01.REGISTRADOR-EJEMPLO.TLD *ID de contacto de registratario = 12345* *Tipo de registratario = persona jurídica* *Organización de registratario = MerchantZ, Inc.* *Correo electrónico del registratario = 12345@MerchantZ.gtld* *Estado de validación de contacto de registratario = validado opcionalmente* *Última marca de tiempo validada de contacto del registratario = x* *<Otros elementos de datos públicos opcionales publicados por el registratario para este nombre de dominio>*
ID del contacto técnico = 67890 *ID de PBC = 67890*

Estado de validación de PBC = validado operativamente
Última marca de tiempo validada del PBC = x
Nombre del PBC: TÉCNICO DE EJEMPLO
Correo electrónico de PBC = 67890@SuperbHostingServices.gtld
Correo electrónico alternativo del PBC = SuperbHostingServices@OtherDN.gtld
Número de teléfono de PBC = +1.1235567890
URL de contacto de PBC = TechSupport@SuperbHostingServices.gtld
<Elementos de datos públicos opcionales publicados por este PBC>

Ejemplo n.º 2: Consulta restricta autenticada para propósitos de resolución de cuestiones técnicas

1) El usuario envía la consulta de RDS autenticada
(DN = PersonY.gtld; Propósito = resolución de cuestión técnica; Datos = todos)

2) El RDS evalúa la consulta:
   - Si "A" se autentica, se aprueba la consulta restricta
   - Si "A" es un ISP acreditado, se otorga acceso al propósito de resolución de la cuestión técnica
   - El acceso está restringido a los datos públicos y restrictos necesarios para la resolución de cuestiones técnicas
   - El acceso está restringido a los datos públicos y restrictos necesarios para la resolución de cuestiones técnicas, es decir, todos los datos públicos y restrictos solicitados para el nombre de dominio + contacto técnico

3) El RDS recupera los elementos de datos solicitados:
Se recuperan datos de PersonY.gtld desde la caché de RDS (sincronizado) o del registro (federado) y envía solamente elementos de datos públicos y restrictos definidos para este propósito, incluso
   ID de contacto de registratario = 12345
   Tipo de registratario = sin declarar
   <cualquier elemento de datos opcional público o restricto publicado por este registratario, por ejemplo, si el registratario lo elige, su nombre>
   ID del contacto técnico = 67890[39]

El ID de contacto técnico [67890] se recupera de la caché del RDS o del validador y solo obtiene los elementos de datos publicados y restrictos expresamente por este contacto para este propósito, incluso
   ID de PBC = 67890

   Dirección de correo electrónico de PBC = <*dirección de correo electrónico obligatoria de la entidad responsable de resolver los problemas técnicos del nombre de dominio PersonY.gtld*>

   Dirección de correo electrónico alternativa de PBC = <*dirección de correo electrónico alternativa recomendada de la entidad*

[39] Si el registratario no proporciona ningún ID de contacto durante la registración del nombre de dominio, podría ser informado de que su direcciones se publicarán como PBC principal y se le dará la oportunidad de dar su consentimiento, de proporcionar otro ID de PBC (por ejemplo, un ID de contacto de proveedor de servicios de privacidad) o de cancelar la registración.

responsable de resolver los problemas técnicos del nombre de dominio>

Número de teléfono de PBC = <*número de teléfono recomendado de la entidad responsable de resolver los problemas técnicos del nombre de dominio>*

URL de contacto de PBC = <*enlace de contacto recomendado publicado por la entidad responsable de resolver los problemas técnicos del nombre de dominio>*

<*cualquier elemento de datos opcional público o restricto publicado por esta entidad, por ejemplo, el número de SMS>*

4) El RDS devuelve un error o una respuesta satisfactoria al usuario. Por ejemplo:

Nombre de dominio: PersonY.gtld *Estado de registración: x* *Estado del cliente: eliminación prohibida (DeleteProhibited), renovación prohibida (RenewProhibited), transferencia prohibida (TransferProhibited)* *Estado del servidor: eliminación prohibida (DeleteProhibited), renovación prohibida (RenewProhibited), transferencia prohibida (TransferProhibited)* *Registrador: REGISTRADOR DE EJEMPLO LLC* *Jurisdicción del registrador: JURISDICCIÓN DE EJEMPLO* *Jurisdicción del registro: JURISDICCIÓN DE EJEMPLO* *Idioma del acuerdo de registro: INGLÉS* *Fecha de creación: 2000-10-08T00:45:00Z* *Fecha de vencimiento de registración del registrador: 2010-10-08T00:44:59Z* *Fecha de actualización: 2009-05-29T20:13:00Z* *URL del registrador: http://www.ejemplo-registrador.tld* *Número de IANA del registrador: 5555555* *Correo electrónico para informe de abusos del registrador: email@registrar.tld* *Número de teléfono de contacto para informe de abusos del registrador: +1.1235551234* *URL de sitio de reclamos de InterNIC:http://wdprs.internic.net/*
Nombre del servidor: NS01.REGISTRADOR-EJEMPLO.TLD *ID de contacto de registratario = 12345* *Tipo de registratario = sin declarar* *Correo electrónico del registratario = 12345@PersonY.gtld* *Estado de validación de contacto de registratario = validado opcionalmente* *Última marca de tiempo validada de contacto del registratario = x* *<Otros elementos de datos opcionales públicos o restrictos publicados por este registratario para el nombre de dominio, por ejemplo, el nombre del registratario, su SMS o su URL de contacto>*

ID del contacto técnico = 67890
ID de PBC = 67890
Estado de validación de PBC = validado operativamente
Última marca de tiempo validada del PBC = x
Nombre del PBC: TÉCNICO DE EJEMPLO
Correo electrónico de PBC = 67890@SuperbHostingServices.gtld
Correo electrónico alternativo del PBC = SuperbHostingServices@OtherDN.gtld
Número de teléfono de PBC = +1.1235567890
URL de contacto de PBC = TechSupport@SuperbHostingServices.gtld
<Elementos de datos públicos o restrictos opcionales publicados por este PBC>

Ejemplo n.º 3: Consultas sobre datos restrictos para propósitos de compra/venta de nombres de dominio o acciones legales

La investigación de posibles infracciones de marca se ilustra a continuación, pero se aplican puntos de partida y pasos similares a la compra de nombres de dominio, la fusión o adquisición, y otras investigaciones relacionadas con este y otros propósitos.

Paso 1. El usuario de RDS inicia sesión en un organismo de acreditación (definido en la Sección IV (c), Acreditación de usuarios de RDS) y certifica que no solo la acción legal es su propósito, sino que además busca obtener los datos para investigar posibles infracciones de marcas del asunto "X". El usuario suministra el nombre y la información de contacto de la persona/organización que es el tema de interés. Las consultas de RDS relacionadas con este propósito están inherentemente limitadas a los datos de registración asociados con este asunto.

Paso 2. El usuario de RDS puede realizar una consulta inversa de los valores ya conocidos sobre el tema, buscando en el RDS una lista de los nombres de dominio que incluyen algunos valores como:

- Registratario o nombre/organización del PBC
- Registratario o teléfono/teléfono alternativo del PBC
- Registratario o dirección postal del PBC, o
- Registratario o correo electrónico/correo electrónico alternativo del PBC

Algunos de estos elementos de datos pueden ser restrictos. La consulta inversa busca en estos elementos de datos restrictos aprobados, pero solamente el valor dado y el propósito establecido, según se detalla en el certificado.

Paso 3. Con la lista de nombres de dominio investigados que puedan estar involucrados en una infracción de marca, el usuario de RDS puede realizar consultas en RDS sobre esos nombres de dominio a fin de obtener los datos necesarios para evaluar los casos, por ejemplo:

- ID del contacto
- Fechas de registración
- Jurisdicción del registrador
- Jurisdicción del registro
- País del registratario (jurisdicción del registratario)
- Organización del registratario, e
- Identificador de empresa de registratario

Se puede solicitar la misma información mediante consultas en WhoWas de estos nombres de dominio. En este paso, todos los elementos de datos son públicos menos uno; el único dato restricto es el país del registratario.

Paso 4. Habiendo concluido que sería inadecuado realizar acciones adicionales, el usuario de RDS puede realizar una consulta en RDS para recuperar el ID de contacto legal público y los datos de contacto asociados (incluso el nombre/organización, teléfono y dirección postal del PBC). Estos resultados se pueden utilizar para intentar contactarse con el contacto legal designado del registratario o para presentar una demanda o un reclamo de UDRP o efectuar alguna otra acción legal.

Paso 5. Si el contacto legal niega ser responsable del nombre de dominio, pueden ser necesarios los datos de contacto completos del registratario para efectuar acciones legales. Es posible que muchos datos sean conocidos del paso 1, no obtenidos del RDS. Sin embargo, pueden existir algunas brechas que deben llenarse en este punto.

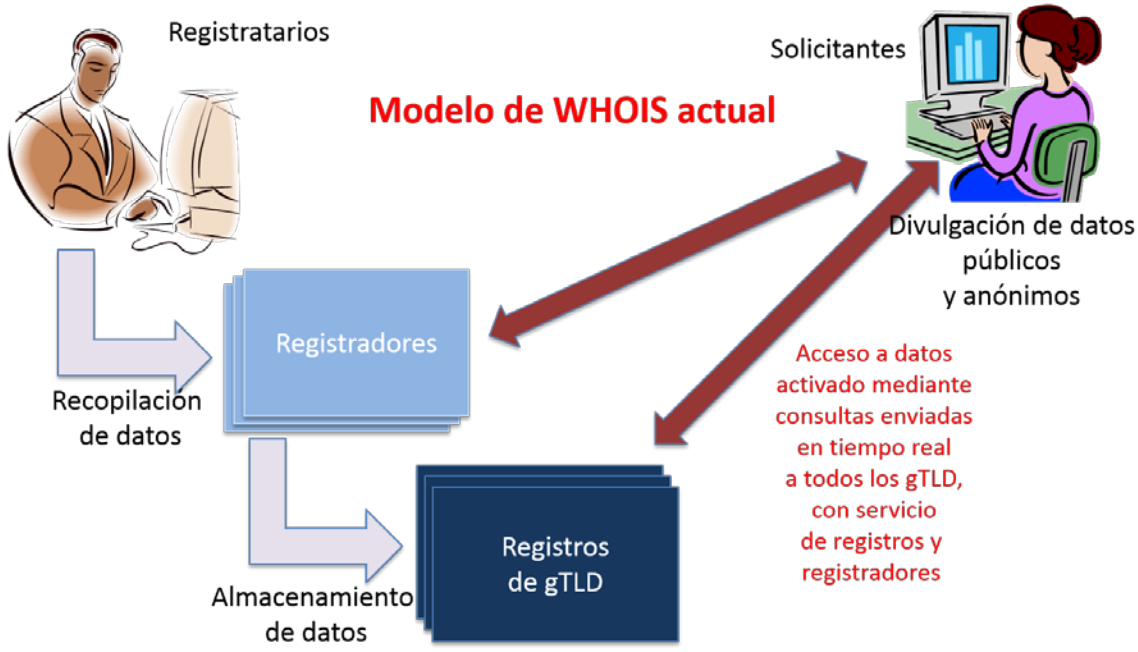
Este ejemplo ilustra las interacciones de RDS que podrían implicar investigaciones y posibles acciones legales relativas a la infracción de marca. No obstante, se puede llevar a cabo una serie similar de pasos en otros tipos de acciones legales y al investigar activos de nombres de dominio en una compra/venta. En los casos de los datos restrictos aprobados, el acreditador debe ser responsable de la auditoría del acceso para detectar solicitudes que probablemente vayan más allá del alcance limitado y de tomar medidas para prevenir el abuso y hacer cumplir los términos de servicio. Tener el certificado del usuario de RDS en archivo facilitará la auditoría que efectuará el acreditador del acceso y la investigación de posibles abusos. Asimismo, servirá para disuadir investigaciones aleatorias.

ANEXO F: MODELOS DE SISTEMA CONSIDERADOS Y METODOLOGÍA

Además de los modelos descritos anteriormente en Posibles modelos de RDS, el EWG consideró las siguientes alternativas, pero las encontró menos viables que el modelo federado y el modelo sincronizado, por razones que se resumen a continuación.

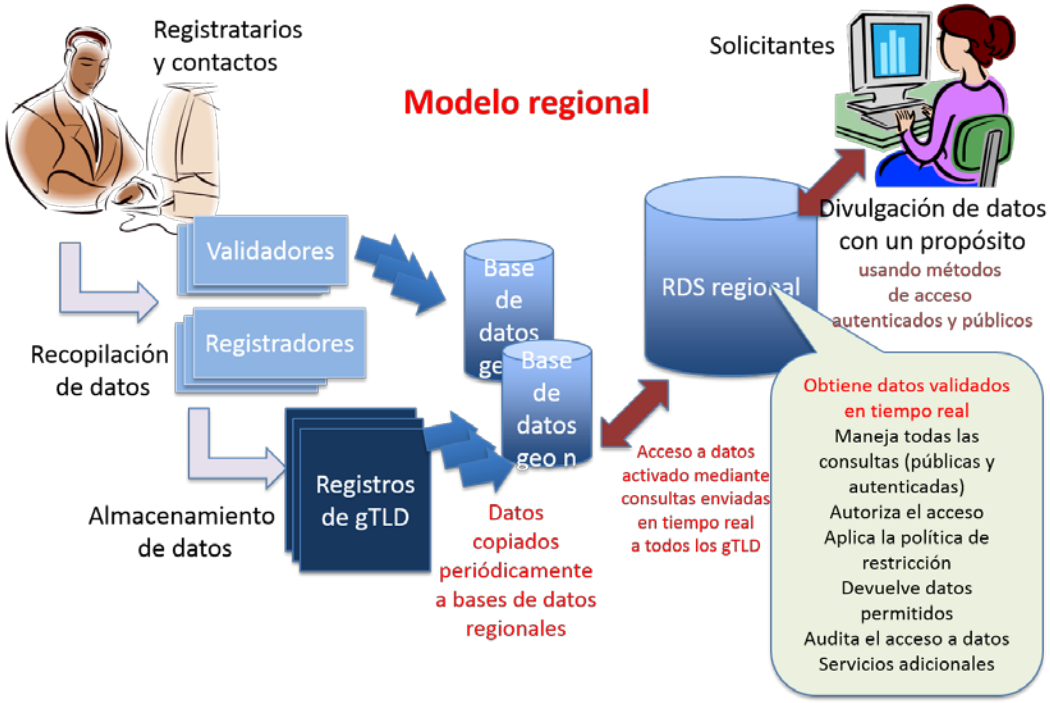
WHOIS actual

Este modelo describe el enfoque autónomo totalmente distribuido empleado por el sistema de WHOIS, en el cual cada registro y registrador ofrece sus propios servicios de WHOIS sin integración en todos los gTLD. Aunque se podría crear un portal centralizado para permitir el acceso a WHOIS en todos los gTLD, cada registro proporcionaría sus propios datos de almacenamiento y acceso gestionados de forma independiente, sea directamente (amplio) o mediante delegación a registradores (breve).



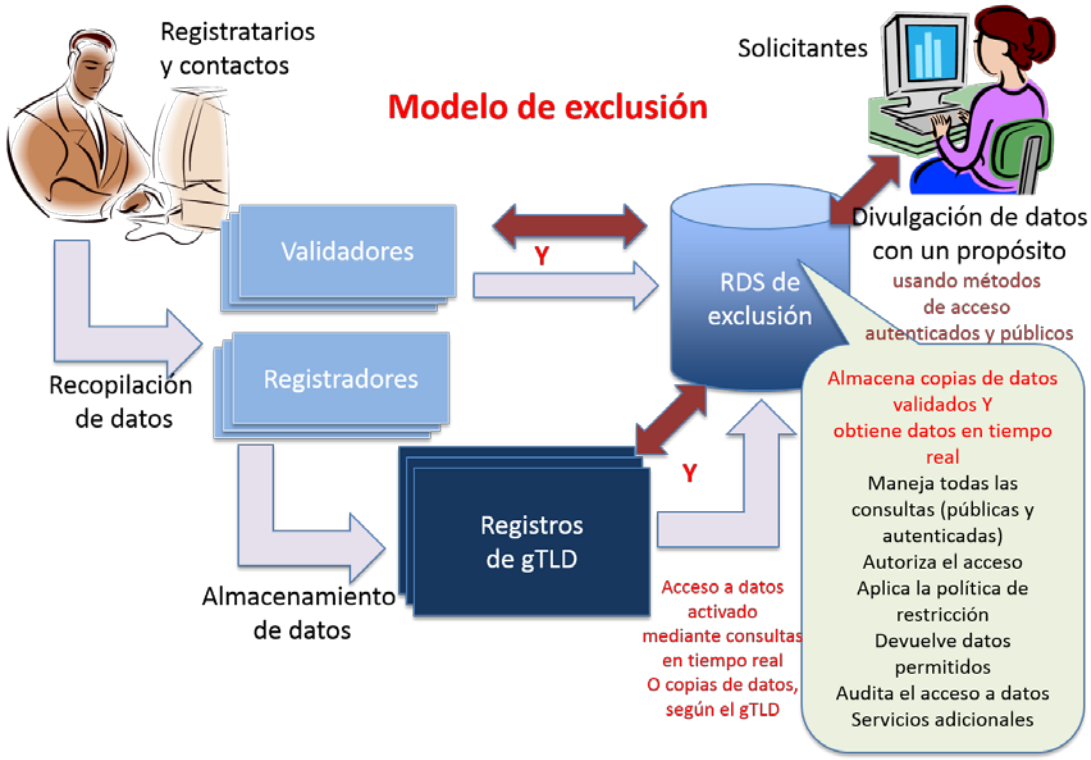
Modelo regional

Este modelo describe un RDS que copia periódicamente datos recibidos de áreas de almacenamiento distribuido operadas por registros y validadores en un almacenamiento regional distribuido por el mundo. Los registros y los validadores continúan almacenando datos, pero el RDS puede usar copias regionales para procesar solicitudes de acceso con mayor efectividad. El RDS opera las áreas de almacenamiento regional, pero están sujetas a las leyes de la jurisdicción en la que se ubican.



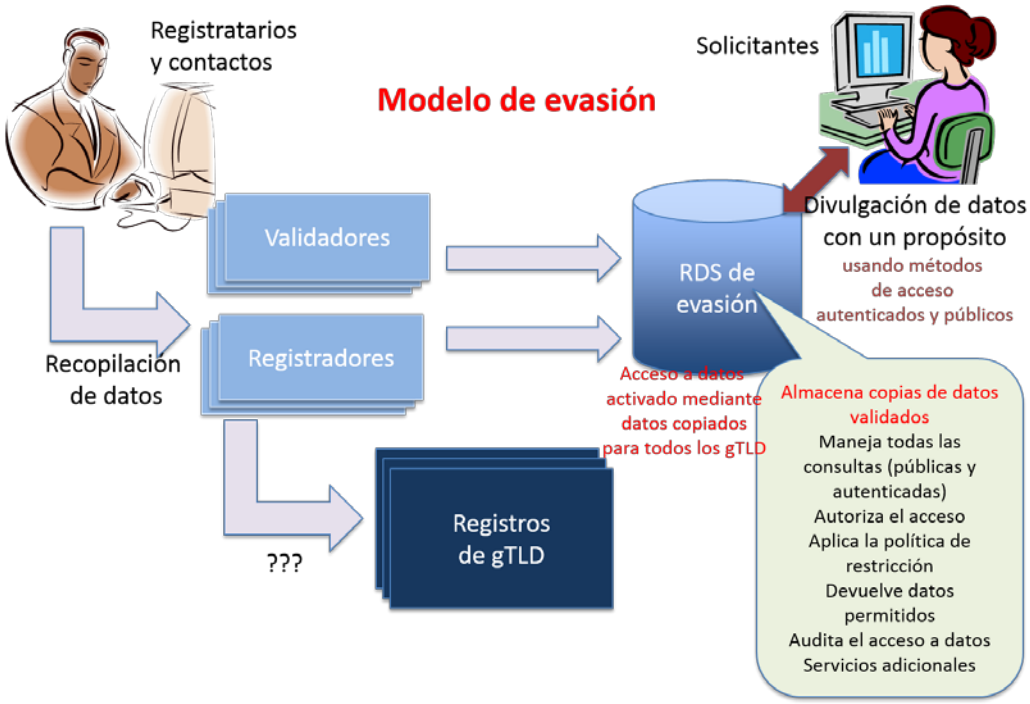
Modelo de exclusión

Este modelo describe un RDS que copia periódicamente datos recibidos de áreas de almacenamiento distribuido operadas por registros en un almacenamiento sincronizado operado por el RDS. En este modelo, cualquier registro puede excluir almacenamiento sincronizado siempre y cuando acepte proporcionar la infraestructura necesaria para manejar una cantidad de consultas significativas, requerido según los acuerdos de nivel de servicio (SLA) de disponibilidad y desempeño.



Modelo de evasión

Este modelo describe un RDS que copia periódicamente datos recibidos de áreas de almacenamiento distribuido operadas por registradores en un almacenamiento sincronizado operado por el RDS. En este modelo, se evitan los registros como fuente de información de registración. En su lugar, el RDS se ocupa de las consultas usando datos de registración sincronizados, copiados directamente de fuentes autorizadas.



Metodología aplicada para comparar modelos de sistemas

El EWG consideró los gastos de asistencia y las vulnerabilidades de seguridad inherentes al sistema actual de WHOIS, muchos de los cuales se abordan en los informes que figuran en el Anexo B, que documenta las deficiencias de WHOIS. Se compararon los costos y las vulnerabilidades del sistema de WHOIS actual y se contrastaron con los modelos posibles. Además, el EWG comparó las ventajas y las desventajas de seguridad de cada uno de los posibles modelos con los criterios siguientes:

Implicaciones de seguridad

- **Punto único de falla:** teniendo en cuenta el uso de una arquitectura distribuida y un proveedor de servicios principal, ¿cuán vulnerable es el modelo si un sistema falla? ¿La falla de algún sistema impediría temporalmente el acceso a toda la información de registración o a parte de ella? **Nota:** Se deben utilizar prácticas operativas y de diseño razonables para proporcionar redundancia interna y respaldo de datos; por lo tanto, se trata de la disponibilidad de los datos en caso de una falla.
- **Sujeto a abuso interno:** ¿cuán vulnerable es el modelo al abuso interno de acceso administrativo/operativo a la información de registración almacenada en el sistema o transferida mediante él de los sistemas que conforman el modelo? ¿El abuso interno podría generar acceso no autorizado a algunos datos o todos ellos? ¿Con qué facilidad se podrían aplicar controles para detectar/disuadir el abuso interno?
- **Sujeto a ataques externos:** ¿cuán vulnerables el modelo respecto de ataques externos contra cualquiera de los sistema que conforman el modelo? ¿Podría un ataque externo causar una brecha de privacidad para todos o algunos de los registratarios? ¿Con qué facilidad se podrían aplicar controles para detectar/disuadir ataques externos?
- **Consistencia de seguridad:** ¿cuán vulnerable es el modelo respecto de una implementación de seguridad inconsistente y la aplicación de políticas? ¿Es posible que todas las partes responsables de los componentes operativos cumplan con los resultados de seguridad de manera uniforme? ¿O la seguridad se vería gravemente impactada por diferencias en la experiencia y la inversión de registradores, registros y validadores?

Jurisdicción e implicaciones de privacidad

- **Almacenamiento de datos en jurisdicciones locales:** ¿el modelo permite almacenar información de registración en una de varias jurisdicciones? ¿Hasta qué punto los registratarios o los registradores/validadores eligen almacenar información de

registración en una jurisdicción con leyes de protección de datos compatibles con la jurisdicción local del registratario?

- **Aplicación de leyes locales a la vista:** ¿el modelo permite acceder a información de registración de manera compatible con una de varias jurisdicciones? ¿Hasta qué punto el RDS puede aplicar las leyes de protección de datos de la jurisdicción local del registratario a la información de registración que se accede mediante el RDS?
- **Cumplimiento con leyes locales de protección de datos:** ¿el modelo ayuda o dificulta el cumplimiento del registrador y del registro con las leyes locales de protección de datos que se aplican a ellos? ¿Cuánto podría dificultar el modelo la obtención de excepciones para permitir el cumplimiento? ¿Cómo se podría garantizar el cumplimiento con los procedimientos legales requeridos por la ley local del registratario?

Acreditación

- **Acreditación de solicitantes:** ¿el modelo les permite a los usuarios que deseen obtener acceso con un propósito a datos restrictos solicitar acreditación, ser evaluados, recibir credenciales de acceso y usarlas para obtener el acceso adecuadamente autorizado a los datos? ¿Hasta qué punto el modelo ayuda o dificulta la solicitud uniforme y sólida de semejante proceso de acreditación de solicitantes?

  Validación: ¿la facilita? ¿La hace menos costosa? ¿Existe algún sistema que permita que las credenciales seguras sean más fáciles o más económicas?
- **Rastrear o penalizar a solicitantes:** ¿con qué nivel de efectividad y confianza puede el modelo registrar solicitudes de acceso a datos y respuestas a los efectos de detectar el abuso de acceso acreditado (es decir, acciones que violan los términos y condiciones de acceso)? ¿Hasta qué punto el modelo ayuda o dificulta las acciones de aplicación de cumplimiento (es decir, sanciones aplicadas a usuarios que no cumplen para evitar futuros abusos)?
- **Auditoría:** ¿el modelo permite auditar solicitudes de acceso a datos y sus respuestas, y las operaciones relacionadas, para evaluar la eficacia del proceso de acreditación y la autorización de acceso a los datos?

Funcionamiento

- **Portal fácil de usar:** ¿el modelo permite presentar fácilmente la información de registración mostrada mediante un portal web o devuelta en respuesta a consultas de protocolo? ¿Hasta qué punto el modelo admite principios de internacionalización

(por ejemplo, soporte de conjuntos de caracteres locales, traducción de respuestas)? ¿Hasta qué punto el modelo facilita la visualización consistente en todos los gTLD?

- **Auditorías aleatorias de datos e informes de precisión:** ¿el modelo admite auditorías periódicas de precisión y la elaboración de informes de precisión en todos los gTLD? ¿Hasta qué punto el modelo facilita la detección y la actualización eficientes y consistentes de la información de registración inadecuada y la aplicación uniforme de políticas de precisión?
- **Latencia de datos (desempeño):** ¿el modelo presenta ineficiencias inherentes respecto del manejo de datos que probablemente afecten el desempeño y no se puedan afrontar mediante la implementación de una plataforma escalable? ¿Cuál es la magnitud relativa de estas ineficiencias (en comparación con otros modelos) respecto de la velocidad de manejo de solicitudes y las demoras percibidas por los usuarios que consultan la información de registración?
- **Sincronización de datos:** ¿el modelo requiere que los datos se copien desde cualquier sistema para sincronizarlos con otros sistemas? ¿Cuál es la amplitud de estas necesidades de sincronización de datos y cuán problemática puede ser la falta de sincronización (en comparación con otros modelos)?
- **Acceso de los registratarios a sus propios datos:** ¿el modelo admite o impide el acceso de registratarios a sus propios datos de registración?
- **Requisitos de almacenamiento y custodia:** ¿el modelo presenta diversas áreas de almacenamiento que aumentan el número o la complejidad de los requisitos de almacenamiento y custodia?
- **Medidas de prevalidación:** ¿el modelo admite la prevalidación de información de registratarios o contactos con un propósito en todos los gTLD? ¿Hasta qué punto el modelo facilita la creación y el mantenimiento eficientes y consistentes de la información de contacto prevalidada y la aplicación uniforme de políticas de carácter único?

Implementación

- **Infraestructura compleja:** en términos generales, ¿el modelo es menos complejo que otros modelos? Por ejemplo, un modelo más complejo (más débil) podría tener muchos más sistemas e interfaces que requerirán una inversión inicial y de mantenimiento continuo.

- **Facilidad de implementación:** ¿es probable que el modelo sea más fácil de implementar que otros modelos? Por ejemplo, un modelo más difícil (más débil) podría requerir cambios a más sistemas.
- **Facilidad de transición:** ¿con qué efectividad el modelo permite una transición fluida del WHOIS actual al RDS para la próxima generación en comparación con otros modelos? Aquí, un modelo más débil es aquel que dificulta que los usuarios, los registradores y los registros efectúen la transición desde procesos existentes.

Costo

- **Reducción de los costos operativos del WHOIS para registradores y registros:** ¿el modelo podrá reducir el costo continuo de mantenimiento y de funcionamiento para los registradores y los registros, en comparación con el sistema de WHOIS actual? Aquí, un modelo que reduce los costos es considerado más fuerte.
- **Costo más bajo de la implementación:** ¿el modelo requerirá una inversión inicial general más o menos alta para infraestructuras y procesos nuevos o modificados, en comparación con otros modelos? Aquí, un modelo con un costo general de inversión de implementación más bajo es considerado más fuerte.
- **Consulta inversa y en historial de WhoWas:** ¿el modelo requerirá una inversión adicional para admitir consultas inversas y búsquedas en historial de WhoWas por parte de solicitantes autorizados? En este caso, un modelo que requiere un menor costo total para ofrecer estos servicios se considera fuerte.

Caso de uso

Comparación de la capacidad de estos posibles modelos para admitir a todos los usuarios y propósitos identificados en el informe inicial, incluso (pero sin limitarse) los siguientes casos de uso:

- Adquisición de nombre de dominio
- Historial de registración de nombre de dominio (incluso el seguimiento del historial de registración de cualquier nombre de dominio [WhoWas])
- Nombres de dominio para registratarios especificados (incluso la búsqueda de nombres de dominio registrados por un registratario específico [consulta inversa de RDS])
- Procedimientos de UDRP
- Investigar nombres de dominio abusivos
- Disuadir actividades maliciosas en Internet

Modelo de análisis de costos

Para examinar la viabilidad y los costos de implementación asociados con los modelos de SRDS y FRDS, la ICANN contrató a IBM para elaborar un análisis detallado centrado en las diferencias de costos entre estos dos posibles modelos de implementación. IMB elaboró un informe final titulado "*Análisis de costos del modelo de implementación del servicio de directorio de registración (RDS)*" (Registration Directory Service [RDS] Implementation Model Cost Analysis)[40]. A continuación, se incluye una parte del informe con los hallazgos de IBM para mayor referencia.

Enfoque

En febrero/marzo de 2014, se llevó a cabo un análisis de costos presupuestarios en el cual se comparó la implementación de RDS[41] sincronizado y federado. Se utilizó un enfoque por etapas:

- *Paso 1: Recopilar los requisitos básicos de cada uno de los modelos de implementación.*
- *Paso 2: Definir y acordar supuestos de mediciones volumétricas clave proporcionados por la ICANN y basados, en gran medida, en los informes de consultas de WHOIS mensuales suministrados por los registros de gTLD. Se usaron estos supuestos para derivar la carga de trabajo esperada del sistema y para definir un esbozo de la solución básica de alto nivel de ambos modelos de implementación.*
- *Paso 3: Crear un modelo de costos y medir los costos presupuestarios de cada esbozo de solución básica.*
- *Paso 4: Formular conclusiones.*

Puntos de partida de participación

- *Se elabora una estimación de costos presupuestarios para el "proveedor/sistema de RDS". No se calculan los costos del operador de registro.*
- *Se crea un modelo de costos de servicios administrados y una estimación. Es decir, se asume la configuración y el funcionamiento continuo del servicio administrado del RDS y se estiman los costos relacionados.*
- *Para los fines de comparación de costos, la solución y los costos se basan, en gran medida, en el portfolio de IBM (principalmente la oferta de IaasS SoftLayer de IBM), usando componentes de un solución de terceros solamente cuando no existe alternativa*

[40] https://community.icann.org/display/WG/EWG+Public+Research+Page

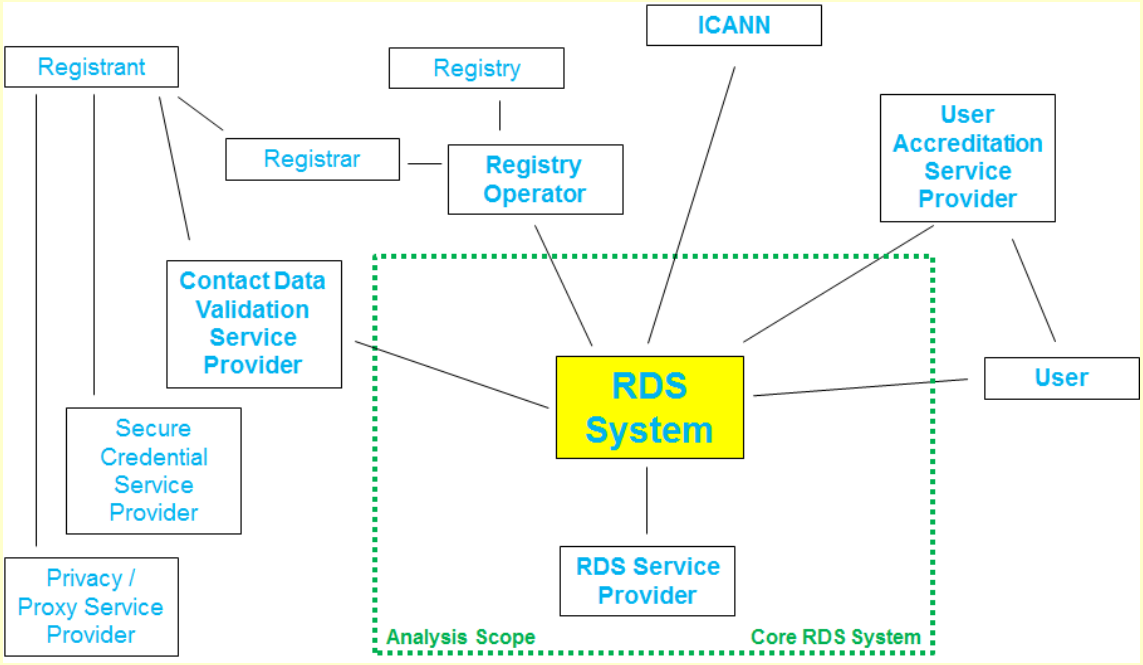
[41] Para estar en consonancia con el informe final del EWG, en este informe se hace referencia al RDS sincronizado (SRDS), el modelo descrito en informes anteriores del EWG como RDS agregado (ARDS).

en el portfolio de IBM.

- *Las estimaciones de costos se elaboran solamente para el esbozo de solución/requisito básico, no para las variantes. No se realiza ningún análisis detallado de generadores de costos.*

Alcance del análisis de costos y mediciones volumétricas

El foco del análisis de costos fue el "sistema RDS central", como se muestra a continuación



.

Se definieron los casos de uso principales para apoyar cada modelo (sincronizado y federado).

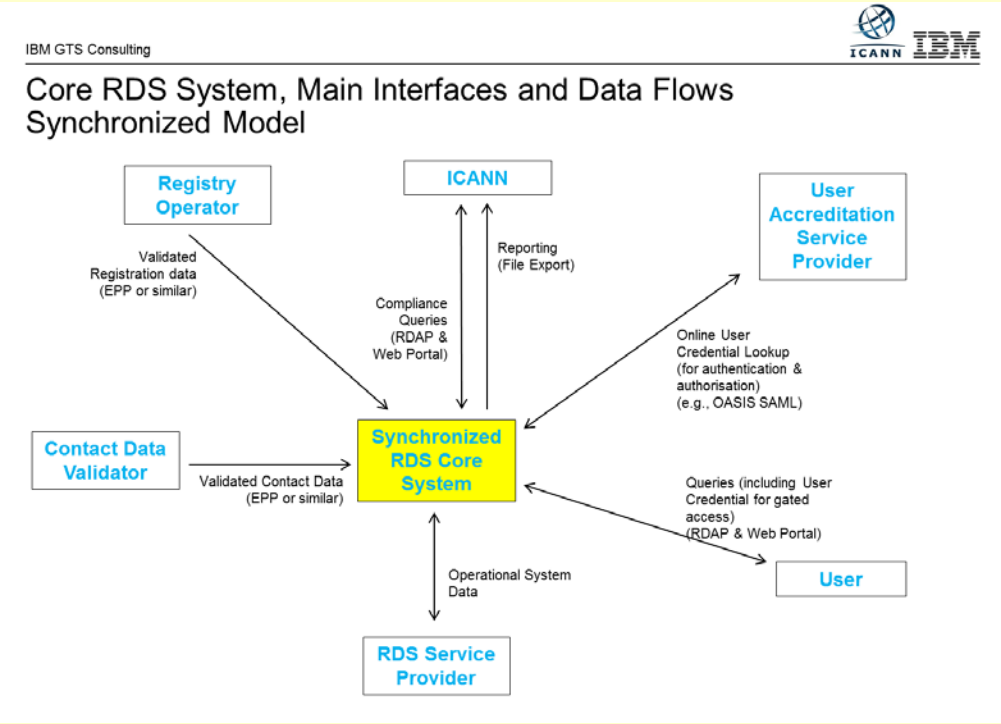
Además, se establecieron supuestos de mediciones volumétricas clave:

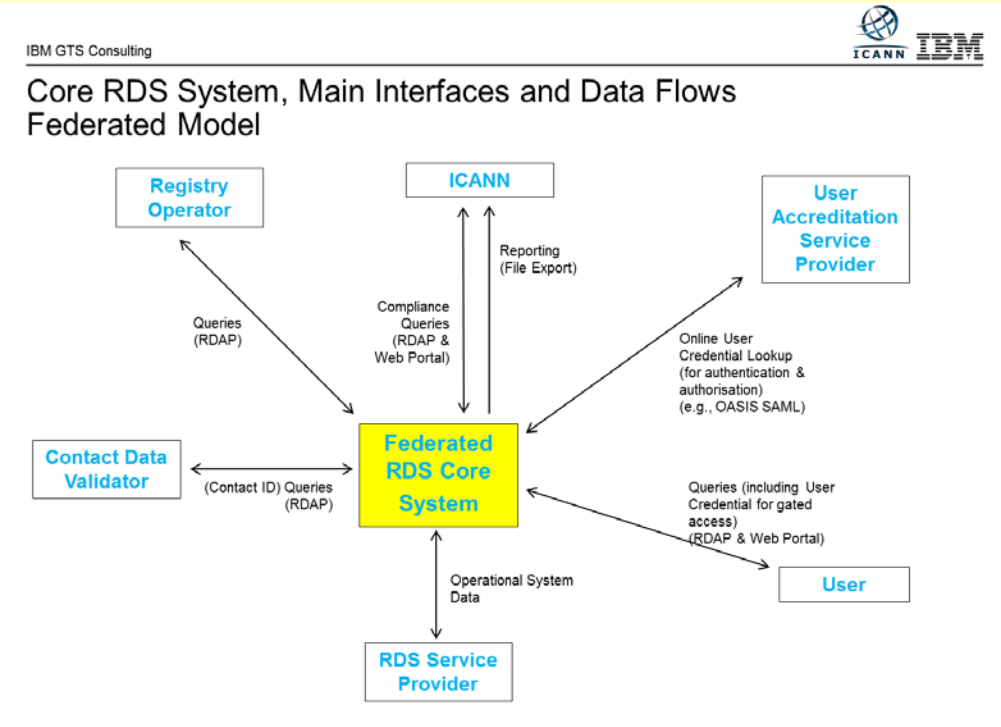
YEARLY GROWTH RATE	22%	nr of DN records added in a year, assumed to include the growth in the nr of gTLDs					
Nr of DN RECORDS, YEARLY UPDATE RATE	100%	nr of DN records updated in a year					
		start yr1 (2015)	start yr2 (2016)	start yr3 (2017)	start yr4 (2018)	start yr5 (2019)	end yr 5 (2020)
Nr of gTLDs		2000	3000	4000	5000	6000	7000
growth rate			50%	33%	25%	20%	17%
	December 2013, ICANN input	start yr1 (2015)	start yr2 (2016)	start yr3 (2017)	start yr4 (2018)	start yr5 (2019)	end yr 5 (2020)
NR OF DOMAIN NAMES	151.196.101	184.459.243	225.040.277	274.549.138	334.949.948	408.638.936	498.539.502
NR OF QUERIES/MONTH	9.031.522.529	11.018.457.485	13.442.518.132	16.399.872.121	20.007.843.988	24.409.569.665	29.779.674.992
AVERAGE NR OF QUERIES/SEC	3.484	4.251	5.186	6.327	7.719	9.417	11.489
NR OF QUERIES/PEAK SEC		42.509	51.862	63.271	77.191	94.173	114.891
AVERAGE NR OF QUERIES/HOUR	12.543.781	15.303.413	18.670.164	22.777.600	27.788.672	33.902.180	41.360.660
NR OF QUERIES IN PEAK HOUR	25.087.563	30.606.826	37.340.328	45.555.200	55.577.344	67.804.360	82.721.319
USER VISITS IN PEAK HOUR	16.892.292	20.608.596	25.142.488	30.673.835	37.422.079	45.654.936	55.699.022
CONCURRENT VISITS IN PEAK HOUR	563.076	686.953	838.083	1.022.461	1.247.403	1.521.831	1.856.634
NEW VISITS IN PEAK SEC		28.623	34.920	42.603	51.975	63.410	77.360

% of reverse queries	1,0%

Modelos de implementación del RDS

Los siguientes modelos de implementación derivaron de los informes de actualización iniciales y de estado del EWG para fines de análisis de costos:



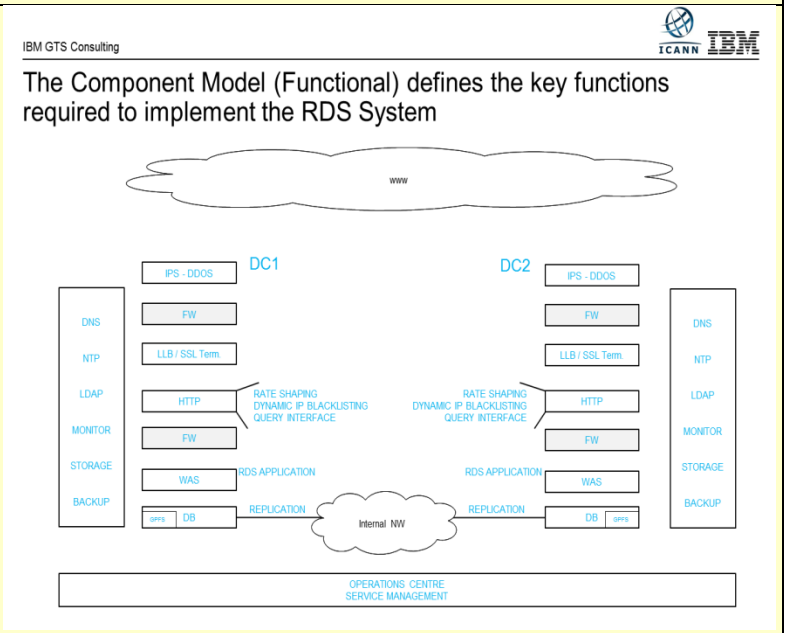


Componentes funcionales del RDS

El siguiente modelo de componentes fue creado para fines de análisis de costos e incorpora todas las funciones clave que se requieren para implementar el sistema de RDS. Se siguieron supuestos de mejores prácticas estándar de diseño de sistemas al calcular los costos de SRDS y de FRDS, como la replicación de la base de datos y del sistema principal de RDS en dos centros de datos geográficamente dispersos, con balanceo de carga y conmutación por error para garantizar la redundancia y la disponibilidad, e IPS para desviar DDoS. Se debe entender que estos componentes funcionales CORRESPONDEN A AMBOS MODELOS DE IMPLEMENTACIÓN.

Componentes funcionales:

- *Balanceo de carga y enrutamiento inter-DC*
- *Mitigación de DDoS de IPS*
- *Balanceo de carga y SSL intra-DC*
- *Servidor web (HTTP)*
- *Servidor de aplicaciones web (WAS)*
- *Nodo de administración de WAS*
- *Sistema de memoria caché de la base de datos*
- *Sistema de miembro de base de datos*
- *Servidor de almacenamiento*
- *Supervisión de sistemas*
- *DNS*
- *NTP*
- *LDSP*
- *Repositorio Syslog*
- *Servidor de respaldo*
- *Servidor de almacenamiento de respaldo*
- *Sistema de respaldo de base de datos cliente*
- *Zonificación de red, cortafuegos/IPS*
- *Conectividad de Internet y DC*



Por ejemplo, se asumió una configuración de dos centros de datos para el sistema de RDS principal, tanto en SRDS como en FRDS, utilizando un diseño activo-activo, donde cada RDS principal es capaz de manejar el 50% de la carga máxima. En este análisis de costos, no se incluyó la agrupación en clústeres para alta disponibilidad en los centros de datos. Se puede agregar sin cambiar los costos relativos de los dos modelos de RDS.

Estimación de costos (suponiendo 1% de consultas inversas)

Los costos detallados a continuación no constituyen de ninguna manera una propuesta de implementación de IBM. El cálculo de costos se creó con el único propósito de solamente ser usado y considerado como parte de un análisis de costos presupuestarios destinado a la comparación de dos modelos de implementación de RDS. Sobre la base de las medidas volumétricas clave, los requisitos de carga de trabajo y el esbozo de solución dado

*anteriormente, el costo por cada nombre de dominio por año de los **sistemas FRDS y SRDS principales solamente** se estima de la siguiente manera:*

Estimación de costos presupuestarios de SRDS

€ 0,0183	average cost/domain/year			
cost per domain name				
yr1	yr2	yr3	yr4	yr5
€ 0,041	€ 0,023	€ 0,017	€ 0,020	€ 0,019

Estimación de costos presupuestarios de FRDS

€ 0,0173	average cost/domain/year			
cost per domain name				
yr1	yr2	yr3	yr4	yr5
€ 0,041	€ 0,018	€ 0,017	€ 0,021	€ 0,017

Las diferencias en costos se analizaron y se compararon de la siguiente manera:

FRDS – SRDS Budgetary Cost Estimate Differences

SETUP COSTS		**5,9%**		10,5%	
INFRASTRUCTURE SETUP COSTS	ARCHITECTURE & DESIGN	**1,5%**	0,2%	15,6%	0,0%
	PROVISION & CONFIGURE		1,2%		19,2%
	INFRASTRUCTURE TESTING		0,1%		18,4%
APPLICATION SETUP COSTS	ANALYSIS, DESIGN, CODE, UNIT TEST	**1,2%**	1,2%	0,0%	0,0%
TESTING	INTEGRATION TESTING & DEPLOYMENT	**1,7%**	0,8%	7,8%	0,0%
	E2E SYSTEM TESTING		0,2%		38,2%
	PERFORMANCE		0,2%		33,3%
	SECURITY (ETHICAL HACK)		0,5%		0,0%
TRANSITION TO BAU	TRANSITION TO BAU	**0,6%**	0,5%	26,6%	37,7%
	SERVICE DESK SETUP		0,1%		0,0%
MANAGEMENT	PROJECT MANAGEMENT	**0,9%**	0,9%	13,4%	13,4%

The FRDS model implies a higher computing power requirement (more systems required to handle the envisaged load) in the web and web application server layer.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve more testing effort

FRDS – SRDS Budgetary Cost Estimate Differences

COST MODEL FRDS		SHARE IN TOTAL		DIFFERENCE WITH ARDS	
		100,0%		-5,4%	
RUN COSTS		**94,1%**		-6,3%	
INFRASTRUCTURE COSTS	PUBLIC NW	**30,5%**	8,1%	-22,4%	-55,9%
	DC NW, GLB, LLB, IPS/DDOS		5,7%		10,7%
	HTTP SERVERS		2,2%		236,0%
	WAS SERVERS		3,7%		218,5%
	DB SERVERS		2,2%		-52,0%
	STORAGE		6,3%		-3,8%
	BACKUP		1,9%		-19,0%
	GENERIC SYSTEMS		0,3%		0,0%
SW LICENCE & MAINTENANCE COSTS	DB	**32,7%**	13,7%	-17,5%	-59,5%
	WAS		18,8%		234,6%
	BACKUP		0,3%		0,0%
OPERATIONS AND MANAGEMENT COSTS	INFRA OPERATIONS & MAINTENANCE	**30,9%**	19,4%	44,0%	63,6%
	APPLICATION OPERATIONS		2,6%		20,0%
	APPLICATION MAINTENANCE		1,3%		27,3%
	SERVICE GOVERNANCE		5,2%		0,0%
	SERVICE DESK		2,4%		100,0%

The Public NW cost is lower in the FRDS case due to the IBM SoftLayer NW charging model: incoming traffic is free; per server 20 TB/month outgoing traffic is free, i.e. you get a total free outgoing volume of #servers x 20 TB per month. As the number of servers increases in the FRDS model, the total amount of free TB outgoing NW volume/month increases.

The FDRS model implies a higher NW throughput requirement. Impact on Firewall and Intrusion Prevention Component.

The FRDS model implies a higher computing power requirement in the web and web application server layer.

The FRDS model implies less storage and backup storage capacity as less data is stored centrally.

The DB compute requirement is estimated to be higher in the SRDS model.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve a higher application operations, support & maintenance release testing workload

Conclusiones principales

Con los supuestos utilizados, el sistema del RDS principal es un poco más económico en el modelo de RDS federado (FRDS) que el modelo de RDS sincronizado (SRDS).

El modelo de FRDS es altamente sensible a las variaciones en la carga consulta inversa. Con una mayor cantidad de consultas inversas, el modelo de FRDS se vuelve sustancialmente más costoso que el SRDS. Con una carga de consultas inversas del 3 % en lugar del 1 %, se estima que el costo del modelo de FRDS pasa a ser un 35 % más alto. Este es un factor importante de incertidumbre y riesgo asociado con el modelo de FRDS. Por el contrario, el modelo de SRDS se cree que es menos sensible a la cantidad de consultas inversas.

Se calcula que el modelo de FDRS requerirá más operaciones de aplicaciones, soporte, mantenimiento y esfuerzos de prueba, ya que se espera una mayor interacción con los operadores de registro.

Además, el modelo de FRDS tiene más impacto en los operadores de registro. En el modelo de FRDS, cada operador de registro tendrá que implementar soporte —en virtud del SLA— para consultas en línea, incluso consultas inversas y consultas históricas de propiedad (WhoWas). En el último caso, los datos históricos tendrían que ser mantenidos por los operadores de registro.

ANEXO G: CAPACIDAD DE LOS PROTOCOLOS EPP Y RDAP PARA ADMITIR RDS

Elemento de datos	Soporte de EPP para recopilación	Soporte de RDAP para acceso
Nombre de dominio	S	S
Estado de registración	S	S
Servidores de DNS	S	S
Delegación de DNSSEC	S	S
Estado del cliente	S	S
Estado del servidor	S	S
Registrador	S	S
Revendedor	S	S
Jurisdicción del registrador	N	N
Jurisdicción del registro	N	N
Idioma del acuerdo de registro	N	S
Fecha de creación	S	S
Fecha de registración original	S	S
Fecha de vencimiento del registrador	S	S
Tipo de registratario	N	S*
Nombre del PBC	S	S
ID de PBC	S	S
Estado de validación de PBC	N	N
Última marca de tiempo validada del PBC	N	N
Organización del PBC	S	S
Calle del PBC	S	S
Ciudad del PBC	S	S
Estado/provincia del PBC	S	S
Código postal del PBC	S	S
País del PBC	S	S
Correo electrónico del PBC	S	S
Correo electrónico alternativo del PBC	N	S
Número de teléfono y extensión del PBC	S	S
Número de teléfono alternativo y extensión del PBC	N	S
Fax y extensión del PBC	S	S
SMS del PBC	N	S
Mensajería instantánea del PBC	N	S
Redes sociales del PBC, redes sociales	N	S

Elemento de datos	Soporte de EPP para recopilación	Soporte de RDAP para acceso
alternativas		
URL de contacto o para informe de abusos del PBC	N	S
Fecha de actualización	S	S
Nombre del registratario	S	S
ID de contacto del registratario	S	S
Estado de validación de contacto de registratario	N	N
Última marca de tiempo validada de contacto del registratario	N	N
Organización del registratario	S	S
Identificador de empresa de registratario	S	S
Calle del registratario	S	S
Ciudad del registratario	S	S
Estado/provincia del registratario	S	S
Código postal del registratario	S	S
País del registratario	S	S
Número de teléfono y extensión del registratario	S	S
Fax y extensión del registratario	S	S
Correo electrónico del registratario, correo electrónico alternativo	S	S
SMS del registratario	N	S
Mensajería instantánea del registratario	N	S
Redes sociales del registratario, redes sociales alternativas	N	S
URL de contacto o para informe de abusos del registratario	N	S
URL del registrador	N	S
Número de IANA del registrador	N	S*
Dirección de correo electrónico	N	S

Elemento de datos	Soporte de EPP para recopilación	Soporte de RDAP para acceso
para informe de abusos del registrador		
Número de teléfono de contacto para informe de abusos del registrador	N	S
URL de sitio de reclamos de InterNIC	N	S

* Estos elementos de datos no están definidos explícitamente en RDAP. Se pueden obtener usando los campos de "observaciones" o una extensión del protocolo.

Extensiones del protocolo o adiciones

Jurisdicción del registrador y registro: se debería agregar a EPP o derivar de la información actual de ubicación del registrador. Se puede obtener usando los campos de "observaciones" de entidad de RDS o una extensión del protocolo.

Idioma del acuerdo de registro: se debería agregar a EPP por extensión del protocolo.

Tipo de registratario: se debería agregar a EPP por extensión del protocolo.

Estado de validación del registratario/PBC, última marca de tiempo validada, correo electrónico alternativo, teléfono alternativo y extensión, SMS, mensajería instantánea, redes sociales, redes sociales alternativas, URL de contacto, URL para informe de abusos: se debería agregar a EPP por extensión del protocolo. RDAP puede manejar identificadores de redes sociales, pero se debería crear una especificación para definir su formato.

Tipo de contacto: actualmente, están disponibles los contactos administrativos, técnicos y de facturación. Todo contacto adicional requerirá una extensión para RDAP.

Propósito declarado en consulta de RDAP: se debería agregar a RDAP por extensión del protocolo.

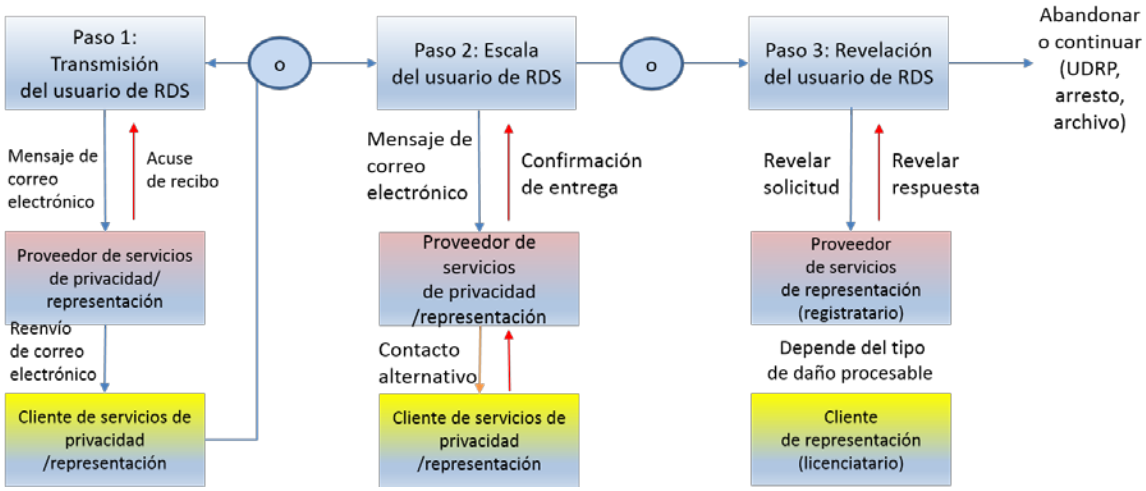
Nivel de acceso en EPP: EPP incluye un mecanismo sencillo para recopilar y transmitir preferencias de divulgación de elemento de contacto de registratario del registrador al registro, donde pueden ser utilizados para informar el comportamiento de respuesta de RDAP. Sin embargo, este mecanismo no es lo suficientemente granular para capturar las preferencias en el nivel de cada elemento de datos individual. Por lo tanto, se requiere una extensión de EPP o una asignación de contacto para indicar la elección de contacto o registratario para anular los valores predeterminados de cada elemento de datos (por ejemplo, elegir publicar un elemento restringido por defecto).

ANEXO H: MODELO Y PRINCIPIOS DE REVELACIÓN Y RETRANSMISIÓN

Como se ha señalado en la Sección VI (b), el EWG recomienda servicios acreditados de privacidad/representación para retransmitir todo el correo electrónico recibido por la dirección de correo electrónico de reenvío. El objetivo es proporcionarles a los clientes de servicios de privacidad/representación y los usuarios de RDS que quieran ponerse en contacto con ellos una ruta de comunicación estándar, siempre disponible y casi en tiempo real.

Además, el EWG recomienda solicitarles a los proveedores acreditados de servicios de privacidad/representación que respondan a solicitudes de revelación de manera oportuna (consulte los detalles a continuación). El objetivo es proporcionarles a los usuarios que experimentan serios problemas con los dominios registrados mediante servicios de representación un proceso eficiente, estándar y siempre disponible para buscar una solución efectiva de problemas.

Al analizar estas necesidades de los usuarios, el EWG señaló otro déficit en las prácticas de hoy en día: la ausencia de un método de escalamiento disponible y eficiente en caso de fallo de comunicación. Muchos usuarios reaccionan rápidamente para revelar porque no tienen otro recurso. El EWG recomienda la introducción de un proceso de escalamiento que podría ser menos costoso para todas las partes y reduciría el número de problemas que conducen a solicitudes de revelación más costosas y que consumen mucho tiempo. A continuación, se ilustra el proceso de tres pasos:



Paso 1: Retransmisión

a) El usuario de RDS solicita datos de contacto de un dominio y obtiene:

- El ID de contacto del registratario (es decir, el ID de contacto del proveedor de servicios de representación o cliente de privacidad)

- Los ID de contacto de todos los contactos con un propósito (PBC) obligatorios y las direcciones de PBC publicadas (incluso direcciones de correo electrónico)

- Una indicación de que la registración del dominio se efectuó mediante servicios de privacidad/representación, y

- Nombre y dirección del proveedor de servicios de privacidad/representación, suministrados como PBC de proveedor de servicios de privacidad/representación, lo que incluye URL de formulario de revelación y escala de retransmisión publicados.

b) El usuario de RDS, al notar que se trata de una registración por parte de un proveedor acreditado de servicios de privacidad/representación, intenta enviarle un correo electrónico al cliente, a la dirección de reenvío. Opcionalmente, los proveedores pueden permitirles a los clientes brindar más direcciones de reenvío (por ejemplo, dirección postal, teléfono, SMS).

c) El proveedor acreditado de servicios de privacidad/representación debe reenviar y acusar recibo del mensaje demorado (por ejemplo, acusar recibo de un correo electrónico de todos los mensajes recibidos en la dirección de correo electrónico de reenvío). En casos de error (por ejemplo, no existe ese buzón de correo), se puede recibir un acuse de recibo negativo y se puede establecer un umbral para limitar los acuses de recibo al mismo remitente a fin de evitar el abuso de retransmisión.

d) El usuario de RDS que recibe el acuse de recibo ahora cuenta con confirmación de que el mensaje fue reenviado al cliente de servicios de privacidad/representación. Sin embargo, el cliente puede optar por no responder o puede descartar el mensaje transmitido sin leerlo (por ejemplo, tratarlo como correo no deseado).

Paso 2: Escala

El usuario de RDS se cansa de esperar que el cliente de servicios de privacidad/representación responda y decide escalar el contacto antes intentado mediante lo siguiente:

a) Visitar el sitio web del proveedor acreditado de servicios de privacidad/representación identificado en el Paso 1 y completar un formulario de escalada que contiene:

- ID del usuario de RDS (posiblemente reutilice la credencial de consultas de RDS)
- El motivo de contacto del usuario de RDS (puede ser una lista desplegable de motivos definidos)
- Nombre de dominio registrado mediante servicios de privacidad/representación
- Mensaje cargado para reenviar al cliente (posiblemente cifrado)
- Marca de tiempo de primer intento de reenvío

b) El proveedor acreditado de servicios de privacidad/representación debe intentar ponerse en contacto con el cliente directamente, si es posible, usando la información de contacto o métodos que no puede utilizar el usuario de RDS, y debe devolver un mensaje de "confirmación de entrega" en N*[42] días. Aquí también es posible obtener confirmaciones negativas en casos de error (por ejemplo, usuario no autenticado, tiempo de espera agotado) y es posible registrar los envíos y establecer un umbral como límite para impedir el abuso.

c) El usuario de RDS que recibe la confirmación ahora cuenta con una prueba documentada de que el mensaje fue entregado al cliente de servicios de privacidad/representación. De todas maneras, el cliente puede optar por no responder, pero la escala puede ayudar a superar fallas básicas de comunicación sin requerir ninguna revelación.

Paso 3: Revelación (solamente se aplica a los dominios registrados mediante servicios de representación)

El tiempo del usuario de RDS se agota a la espera de que el cliente de servicios acreditados de representación (licenciatario) responda y decida si el problema es lo suficientemente importante como para emprender acciones legales o civiles y realiza lo siguiente:

[42] * El tiempo de espera agotado puede depender de la identidad autenticada y el motivo declarado de contacto. Por ejemplo, 1 día para la aplicación de la ley/investigación de un crimen de OpSec/abuso; 7 días para propietarios de marcas que investigan infracciones de marca; 7 días para los consumidores de Internet que intentan llegar a los comerciantes en línea.

a) Visitar el sitio web o llamar o enviarle un correo electrónico al proveedor acreditado de servicios de representación identificado en el Paso 1 y enviar una solicitud de revelación que contiene:

- ID del usuario de RDS
- Motivo de contacto del usuario de RDS (limitado a los daños procesables)
- Nombre de dominio registrado mediante servicios de representación
- Documentación del daño (información de registración de la marca, denuncias de abuso)
- Marca de tiempo del intento de retransmisión/escala (número de caso de la escala)

d) El proveedor acreditado de servicios de privacidad/representación debe investigar y tomar las medidas apropiadas (consulte el punto d), y devolver un mensaje de "respuesta de revelación" en N*[43] días. Las solicitudes de revelación se pueden registrar y limitar a los daños procesables denunciados por usuarios de RDS en efecto,[44] para impedir el abuso.

c) El proveedor acreditado de servicios de representación, con documentación para evaluar el caso, puede:

- Notificar al cliente y transferirle el dominio (es decir, suspender el servicio de representación)
- Suspender temporalmente el dominio durante una investigación criminal
- Revelar al usuario la identidad o el contacto de un licenciatario envuelto en actividades ilegítimas
- Rechazar la revelación; confirmar la responsabilidad del proveedor de servicios de representación para más uso del dominio

[43] * El tiempo de espera agotado puede depender del solicitante y el motivo declarado de contacto. Los agentes de seguridad pueden ir directamente al Paso 3 (Revelación) para investigaciones en las cuales el tiempo es un tema sensible. Los plazos de tiempo y los esfuerzos del Paso 2 deben ser lo suficientemente bajo para desalentar a las personas a ir directamente al Paso 3.

[44] ** Cualquier usuario que solicite una revelación debe demostrar que es una parte que sufre daños procesables o un representante de la parte afectada. Por ejemplo, los titulares de marca o los agentes que denuncian infracciones de marca pueden mostrar que poseen nombres de dominio similares al dominio registrado mediante servicios de representación. Se debe analizar más este tema para asignar tipos de usuarios a tipos de daños. Consulte la lista de GoDaddy de opciones del formulario de reclamos de dominios registrados mediante servicio de representación como ejemplo.

Se debe elaborar una política para detallar qué constituye documentación suficiente y cuándo debe ser notificado el licenciatario. Además, tiene que haber políticas claras en relación con el impacto de la ley local y de los factores que deben considerarse. Todo lo mencionado anteriormente sucede hoy en día, sin ningún tipo de supervisión, orientación política ni consecuencias por rechazar/ignorar una revelación.

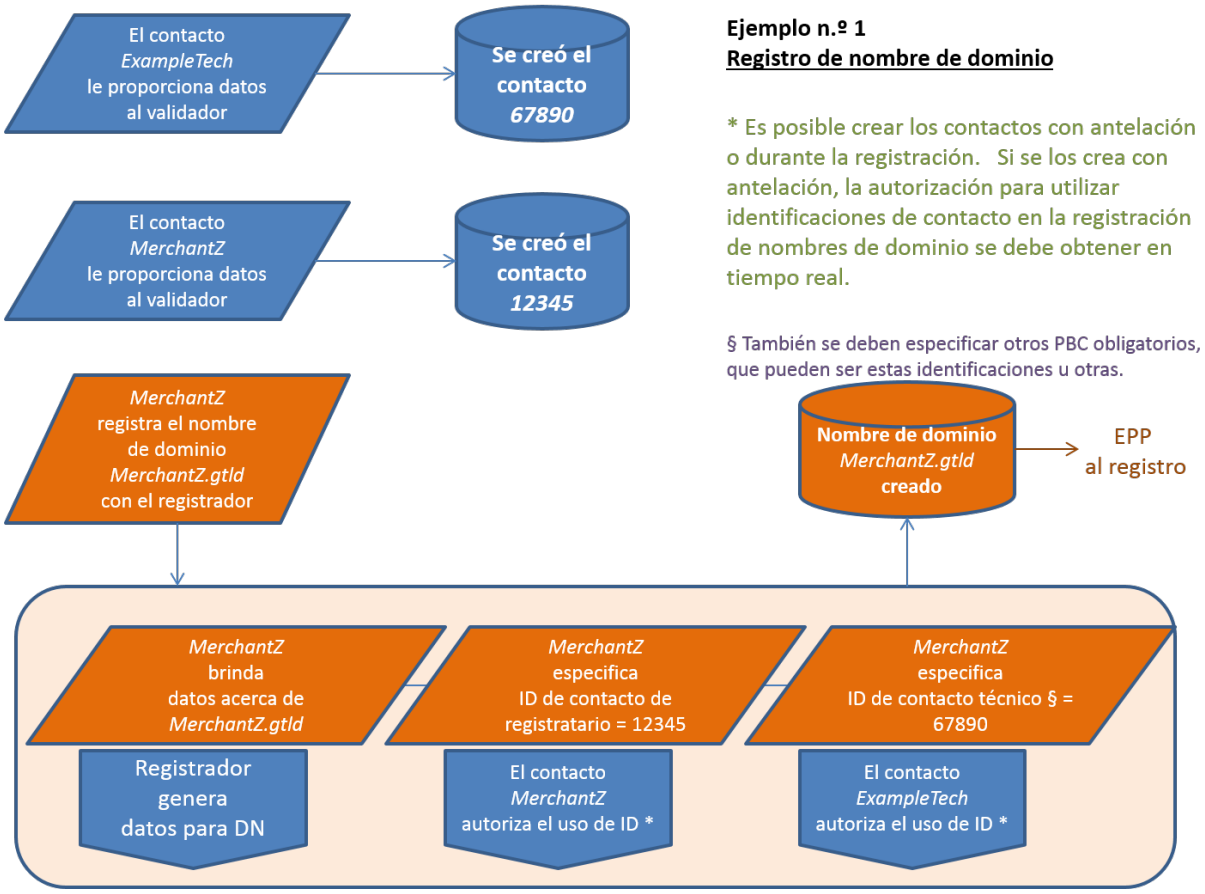
d) El usuario de RDS que recibe la respuesta de la revelación ahora cuenta con la información necesaria para desechar el asunto o llevar adelante acciones civiles/legales. Por ejemplo, la infracción de marca puede dar lugar a la presentación de un reclamo de UDRP, mientras que una investigación criminal de un organismo de aplicación de la ley podría llevar a la detención de un sospechoso. Si se rechaza la revelación (o no se recibe una respuesta oportuna), el usuario de RDS ahora también puede optar por llevar a cabo acciones civiles/legales con el proveedor acreditado de servicios de representación.

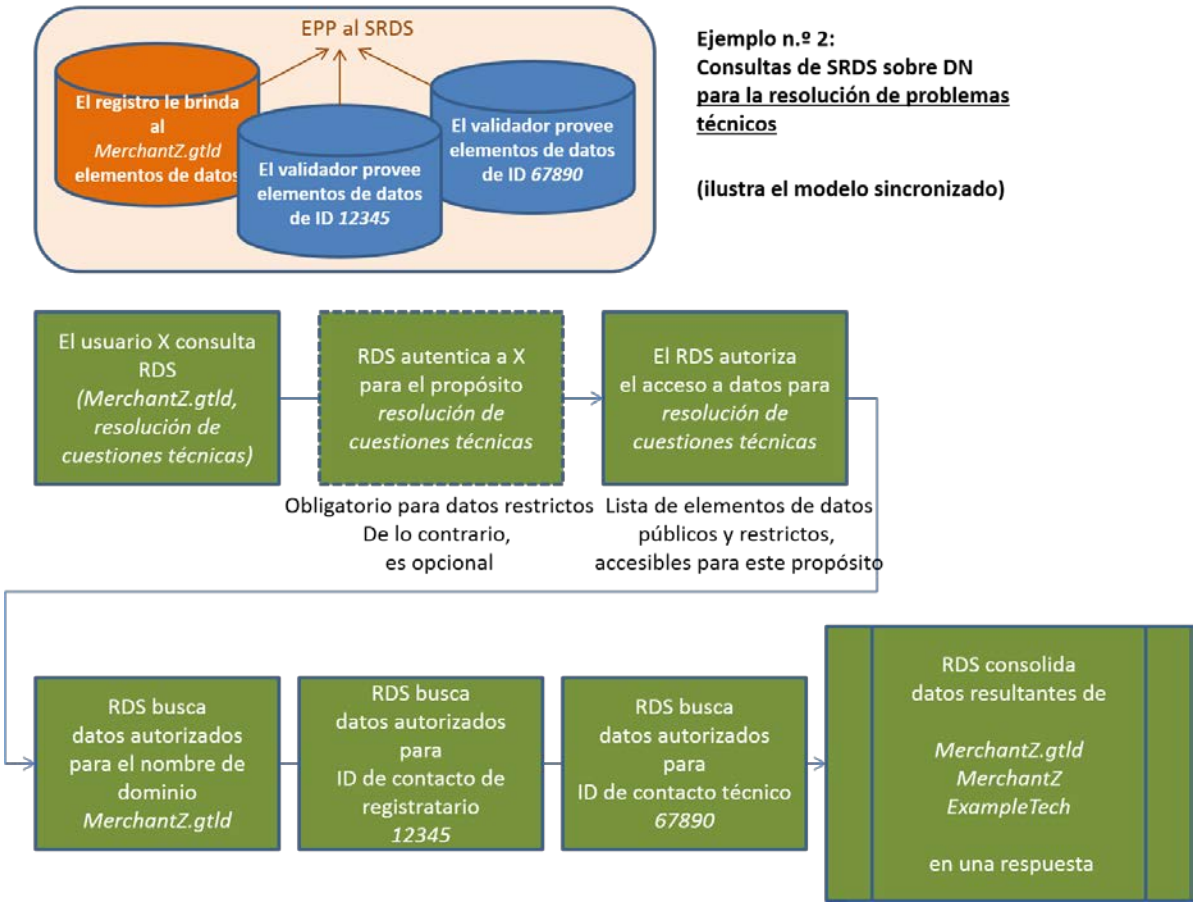
Tenga en cuenta que los procesos descritos anteriormente no resuelven cuándo una registración mediante servicios de privacidad/representación debe ser "desenmascarada" para el público en lugar de simplemente "revelarla" para el solicitante.

El grupo de trabajo de PPSAI de la GNSO debe refinar estos modelos y procesos sugeridos sobre la base de su consideración de las necesidades de la comunidad de la ICANN y con conocimiento de las mejores prácticas identificadas por las respuestas a la encuesta en línea de proveedores de servicios de privacidad/representación del EWG.

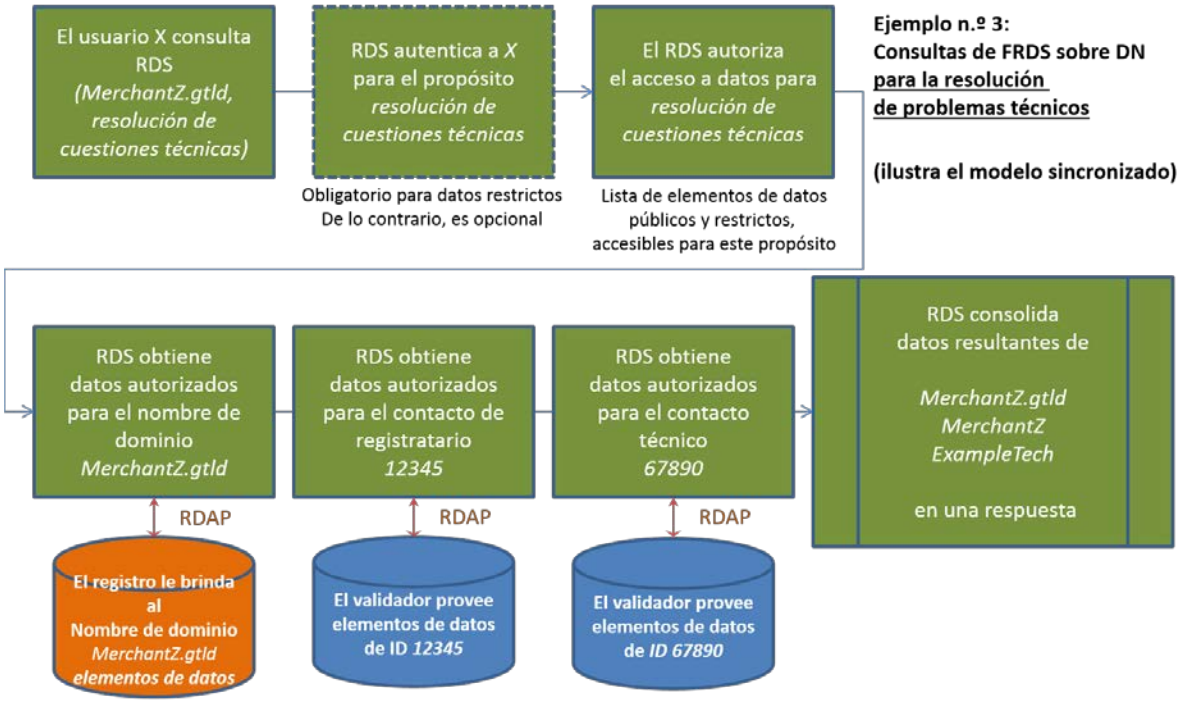
ANEXO I: DIAGRAMAS DE FLUJO DE PROCESOS DE RDS

Los siguientes diagramas de flujo ilustran los flujos de datos clave entre los actores del ecosistema de RDS durante la registración del nombre de dominio y las consultas de los solicitantes a RDS para obtener información sobre ese nombre de dominio para la resolución de problemas técnicos.





Para facilitar la comparación de modelos, este mismo ejemplo se repite a continuación para FRDS.



ANEXO J: ACERCA DEL EWG

Proceso de selección y visión

Al convocar al EWG, la Junta Directiva de la ICANN adoptó un nuevo enfoque para resolver un problema difícil que ha estado marcado por los desacuerdos y el estancamiento en el pasado. La Junta Directiva convocó a individuos que representan una amplia variedad de perspectivas y partes interesadas con la esperanza de que, al compartir su experiencia, pudieran tener éxito donde otros habían fracasado. Con la

entrega de este informe final y sus 180 principios con consenso, la visión de la Junta Directiva se ha materializado.

Los miembros del EWG fueron cuidadosamente seleccionados con la ayuda de un facilitador experimentado y neutral, Jean-Francois Baril. Fue elegido por su experiencia en el desarrollo de estándares del sector de la electrónica de consumo. Se analizaron docenas de solicitantes del EWG sobre la base de varios criterios, incluso las habilidades de liderazgo, la experiencia, la diversidad geográfica, la creación de consenso, la aptitud para innovar y, en algunos casos, la neutralidad. Se consideró que las personas de fuera de la comunidad de la ICANN podrían traer una nueva perspectiva, despegada de los intentos anteriores de abordar la cuestión de WHOIS.

Composición del EWG
El EWG consta de individuos, coordinadores de enlace de la Junta Directiva y personal de Australia, Canadá, China, la Comisión Europea, Irlanda, Jamaica, Nigeria, Noruega, Suiza, el Reino Unido y los Estados Unidos. Esta diversidad geográfica resultó fundamental para la comprensión de los muchos desafíos jurisdiccionales relacionados con el trabajo del EWG.

Entre los miembros del EWG, había empresarios y líderes internacionales experimentados (Ajayi, Ala-Pietilä, Neylon, Rasmussen y Shah). Su experiencia colectiva para equilibrar riesgos y su estilo de resolución de problemas orientada a los resultados allanó el camino para llegar a un consenso rápido en el EWG.

Debido a que el mandato del EWG incluyó el examen de políticas públicas, en particular, cuestiones de privacidad, la experiencia específica en el sector gubernamental fue clave para el éxito. Perrin y Niebel aportaron experiencia desde la perspectiva de Canadá y Europa, lo que garantizó que estos temas tuvieran prioridad en el diseño del sistema para la próxima generación. Es significativo que durante sus deliberaciones, el EWG tuvo conocimiento de los cambios recientes en la legislación de protección de datos de la Unión Europea y trató de tenerlo en cuenta.

Otro aspecto fundamental de la labor del EWG fue asegurar que sus recomendaciones fueran razonablemente viables en el ecosistema de DNS actual. La experiencia de miembros registradores de gTLD (Neylon), registros de gTLD (Hollenbeck-.com y .net) y ccTLD (.cn-Jian, .uk-Nanayakkara, .ng- Ajayi y .au-Disspain) aclaró temas como los enfoques de validación, las registraciones de servicios de privacidad/representación, compatibilidad con protocolos, como EPP y el nuevo RDAP en desarrollando en IETF, así como la incorporación de conceptos como el "acceso restricto" para la visualización de

elementos de datos confidenciales.

También se examinaron problemas de seguridad y estabilidad, aprovechando la visión de los miembros actuales y anteriores de SSAC (Crocker y Rasmussen), aportando su gran comprensión de las necesidades de aplicación de la ley en la lucha contra el abuso malicioso relacionado con DNS.

Es imposible diseñar un nuevo sistema sin considerar las necesidades de los muchos usuarios del RDS para la próxima generación. El EWG incluyó a miembros con un gran conocimiento de cuestiones de propiedad intelectual (Kawaguchi, Vayra y Shah) que se basan en gran medida en el sistema actual de WHOIS para luchar contra la ocupación ilegal de dominios, el fraude y la falsificación en línea, así como los puntos de vista compartidos por los usuarios finales (Samuels y Phifer). Estas diversas perspectivas ayudaron a garantizar que los propósitos legítimos para obtener acceso desde RDS a los datos de registración se adopten, lo que reduce al mínimo las ineficiencias y los abusos de los procesos actuales de registración siempre que sea posible.

Para complementar el EWG, los miembros del personal de la ICANN (Michel, Milam) trajeron una visión ejecutiva y el conocimiento del marco contractual de la ICANN. Un consultor (Phifer) también proporcionó datos de los extensos estudios sobre WHOIS de la GNSO realizados en los últimos cinco años para ayudar al EWG a formular recomendaciones basadas en los hechos.

Metodología de trabajo

El EWG inició su trabajo con una serie de actividades de conocimiento de compañeros, destinadas a construir una buena relación, confianza y, lo más importante, un sentido de pertenencia a un equipo. El EWG estableció un conjunto de valores de equipo para superar los obstáculos a la búsqueda de soluciones innovadoras para este complejo problema. Ellos son:

- Somos miembros de un equipo
- Hable con libertad
- No hay atribuciones de redes sociales
- Honestidad intelectual
- Autorregulación del sector
- Diseño desde cero
- Factores en realidades difíciles (tecnología y gobiernos)

Estos valores ayudaron a guiar al EWG a tener el compromiso necesario para diseñar el RDS y a elaborar los principios descritos en este informe final.

Para obtener más información y conocer las biografías de los miembros del EWG, consulte este anuncio.