Informe Inicial del Grupo de Trabajo de Expertos en Servicios de Directorio de Datos para la Siguiente Generación

ESTADO DE ESTE DOCUMENTO

El presente es un informe del Grupo de Trabajo de Expertos (EWG) en el cual se presentan recomendaciones para un Servicio de Directorio de Registración de gTLDs para la siguiente generación, en reemplazo del sistema de WHOIS actual.

I. RESUMEN EJECUTIVO

El Grupo de Trabajo de Expertos (EWG) en Servicios de Directorio de gTLDs 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, al cual se considera, en gran medida, "defectuoso". El mandato del EWG es reexaminar y definir el propósito de la recolección 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 grupo partió desde una tabula rasa, analizando y cuestionando supuestos fundamentales sobre los propósitos, los usos, la recolección, el mantenimiento y el suministro de datos de registración, como también la exactitud, el acceso, las necesidades de privacidad y las partes interesadas involucradas en los servicios de directorio de gTLD. Luego de analizar una amplia gama de casos concretos, y la gran cantidad de cuestiones que surgían a partir de dichos casos, el EWG llegó a la conclusión de que se debería abandonar el modelo actual de WHOIS - en el cual cada usuario tiene el mismo acceso público anónimo a datos de registración de gTLD - que suelen ser inexactos. En lugar de ello, 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 únicamente a solicitantes autorizados y responsables usarlos apropiadamente.

El EWG recomienda que, dentro de los fines permisibles, se incluyan:

- Control de nombre de dominio
- Búsqueda de nombre de dominio
- Protección de datos personales
- Acciones legales
- Cumplimiento efectivo de normas regulatorias/contratos
- Compra/venta de nombre de dominio
- Uso individual de Internet
- Mitigación de abusos

- Resolución de cuestiones técnicas
- Suministro de servicios de Internet

El EWG tuvo en cuenta a la gama de partes interesadas involucradas en la recolección, el almacenamiento, la divulgación y el uso de datos de registración de gTLD y realizó en mapeo de los mismos en base a fines relacionados. Luego, se identificaron áreas de interés común, las cuales fueron tenidas en cuenta a medida que el EWG desarrolló principios y características que sirvan de guía para diseñar un servicio de datos de registración (RDS) para la próxima generación.

Esto llevó al EWG a considerar varios diseños del sistema y acordar un nuevo modelo de servicio de datos de registración para recolectar, usar y divulgar elementos individuales de datos precisos para diversos fines. Cada actor dentro del ecosistema de RDS tiene distintas necesidades de obtención de datos, distintos riesgos y distintas responsabilidades potenciales. Históricamente, la mayoría de estas responsabilidades era transferida a los registradores, cuyo objetivo principal era proporcionar nombres de dominio en funcionamiento a los clientes que abonaran ese servicio. A medida que el ecosistema de Internet se torna más complejo, y con la introducción de cientos de nuevos gTLDs, es probable que se requiera a más actores adoptar las múltiples responsabilidades que implica cumplir con una gama tan amplia de propósitos de registración.

En la ilustración que figura a continuación, se muestra el modelo recomendado por el EWG para la próxima generación de RDS que, potencialmente, podría incorporar gran parte de los principios analizados en este informe. **Dentro de los elementos clave del modelo de RDS Agregado (ARDS), se incluye lo siguiente:**

- El ARDS sirve como un repositorio agregado que contiene una copia no autoritativa de todos los elementos de datos recolectados.
- Cada registro de gTLD continúa siendo una fuente autoritativa de datos.
- Los solicitantes (usuarios que desean obtener datos de registración de gTLD del sistema) solicitan credenciales de acceso al ARDS.

- Los registradores/registros quedan liberados de sus obligaciones de brindar acceso mediante Puerto 43, o de otros requisitos de acceso público.
- En la mayoría de los casos, el ARDS brinda acceso a datos de registración en memoria caché que es copiada de los registros de gTLD y mantenida mediante actualizaciones periódicas.
- El ARDS también puede brindar acceso a datos de registración obtenidos en tiempo real de los registros de gTLD, a pedido, y sujeto a controles para disuadir el uso excesivo o el abuso de esta opción.
- El ARDS (o un tercero que interactúe con el ARDS) sería responsable de efectuar los servicios de validación.
- El ARDS es responsable de auditar el acceso para minimizar el abuso e imponer penalidades y demás medidas para subsanar el acceso indebido.
- El ARDS maneja los reclamos por exactitud de datos.
- El ARDS maneja los acuerdos de licencia de acceso de datos.

La ICANN contrata a un proveedor internacional tercerizado que se encargue del desarrollo y la operación del ARDS y del monitoreo del cumplimiento de los requisitos.

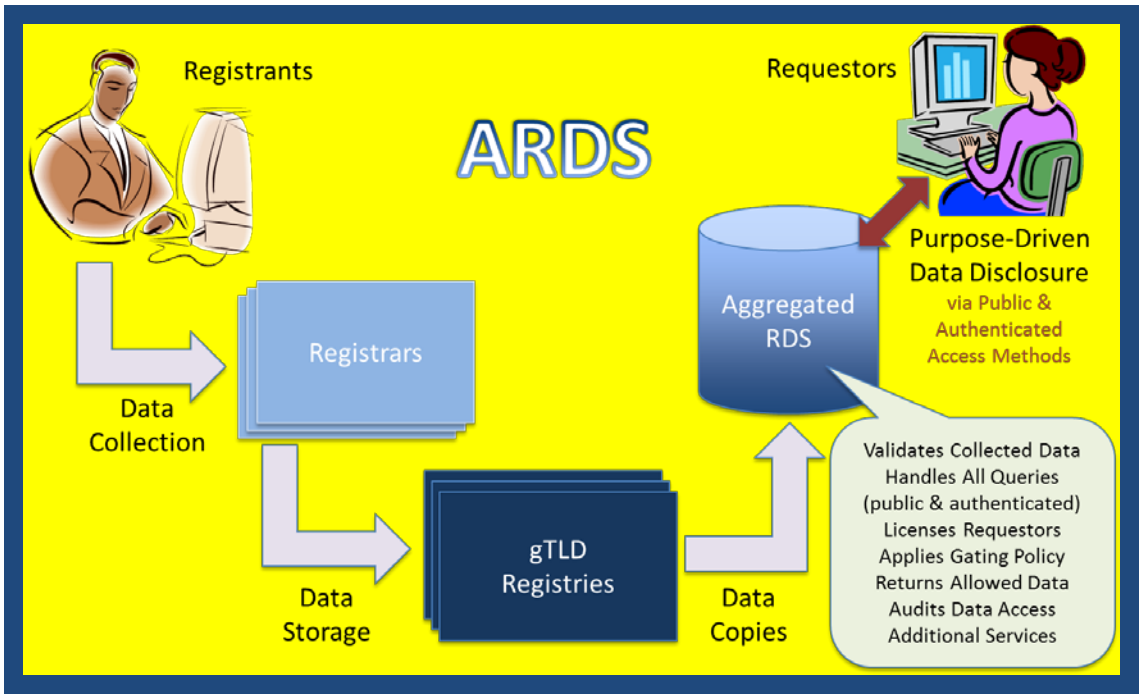

Figura 4. Modelo de RDS Agregado

El modelo cuenta con el acuerdo por consenso de los miembros del EWG dadas sus múltiples ventajas:

- Escala manejada por un único punto de contacto
- Posibles mejoras en el transporte y la entrega
- “Único sitio de consulta” para solicitantes de datos de registración
- Mayor responsabilidad en cuanto al acceso y la validación de datos de registración (medida anti-abuso).
- Capacidad de rastrear/auditar/penalizar a los solicitantes de igual modo en múltiples TLDs (medida anti-abuso)
- Puede reducir algunos costos actualmente afrontados por registradores y registros al brindar acceso a datos
- Se pueden brindar servicios de normalización o filtrado de datos
- Reduce los requisitos de ancho de banda para registros y registradores
- Facilita la estandarización de enfoques para atender inquietudes locales en materia de privacidad de datos
- Mejor capacidad de búsqueda en múltiples TLDs (por ejemplo, búsqueda inversa)
- Se minimizan costos de transición e implementación
- Permite la validación/acreditación de solicitantes que califican para fines especiales (por ejemplo, organismos a cargo del cumplimiento de la ley)
- Facilita una gestión más eficiente de inexactitud en informes
- Permite realizar verificaciones aleatorias de exactitud con mayor eficiencia
- Permite mostrar información en múltiples idiomas, códigos de escritura y caracteres en un portal de búsqueda fácil de usar

Por supuesto que nada es perfecto. El EWG también consideró las siguientes desventajas potenciales del modelo:

- Latencia de datos
- Creación de una fuente de "grandes datos" con datos sumamente valiosos que pueden ser usados indebidamente sin una auditoria y un mantenimiento apropiados
- Mayor riesgo de abusos internos y ataques externos, lo cual requiere prestar más atención a la implementación, el cumplimiento efectivo y la auditoria de políticas de seguridad
- Los registros/registradores ya controlan la entrega de los datos de registración

Al proponer este nuevo modelo, el EWG reconoce la necesidad de la exactitud, junto con la necesidad de proteger la privacidad de los registratarios que pueden requerir mayor protección de sus datos personales. El EWG analizó maneras en las cuales el RDS podría adecuarse a las necesidades de usuarios en riesgo en pos de servicios de registración con un nivel de protección máximo, mediante el uso de "credenciales con protección de seguridad". Una opción podría ser que la ICANN acreditase a un organismo independiente para que se desempeñe como un representante de confianza que, mediante un conjunto de criterios acordados, determinase si un registratario califica para recibir en máximo nivel de protección. El EWG espera considerar en mayor profundidad los posibles modelos de credenciales con protección de seguridad que puedan lograr un equilibrio efectivo e innovador entre la responsabilidad y las necesidades de protección de la privacidad de los usuarios de Internet en riesgo.

Próximos pasos

Sin perjuicio del progreso plasmado en estas recomendaciones, las deliberaciones del EWG no han finalizado. El grupo espera recibir aportes del público sobre estas recomendaciones preliminares, y continuará mejorando sus recomendaciones a medida que considere con atención los comentarios recibidos en línea, durante la reunión de la ICANN en Durban, y mediante otra instancia de consulta pública.

Asimismo, quedan por explorar varias cuestiones clave, a saber:

- Realizar un mapeo de los elementos de datos obligatorios/optativos para cada propósito
- Identificar áreas que requieran un análisis de riesgo e impacto
- Considerar costos e impactos, y las maneras en que se los podría afrontar
- Examinar métodos de acceso multi-modal, y la manera de habilitarlos en protocolos de acceso a datos de registración actuales o futuros

Luego de una consulta pública sobre este Informe inicial, el EWG publicará y entregará un Informe final al Director Ejecutivo y a la Junta Directiva de la ICANN para que sirva como base de las negociaciones contractuales y políticas de los nuevos gTLDs, según corresponda. Tal como especificara la Junta Directiva, un Informe de cuestiones basado en el Informe final será la base de un proceso de desarrollo de políticas (PDP) de la GNSO iniciado por la Junta Directiva y con un enfoque específico.

II. MANDATO Y PROPÓSITO DEL EWG

2.1 Mandato

El EWG fue creado como un primer paso en pos del cumplimiento de las instrucciones de la Junta Directiva de la ICANN[1] para ayudar a redefinir el propósito y el suministro de datos de registración de gTLD (tales como WHOIS), con el objeto explícito de sentar las bases para la creación de una nueva política global de servicios de directorio y negociaciones contractuales de gTLD. Los objetivos del EWG son 1) definir el propósito de la recolección y el mantenimiento de los datos de registro de gTLD, considerar cómo proteger los datos, y 2) proponer un modelo para la administración de los servicios de directorio de gTLD que aborde los problemas relacionados a la exactitud y acceso de los datos, mientras que, al mismo tiempo, se consideren medidas para la protección de datos. El EWG se basó en la información presentada en el Informe Final del Equipo de Revisión de WHOIS, en los Principios del GAC sobre WHOIS, como también en los aportes presentados previamente por la comunidad y en la labor de la GNSO durante la última década. Asimismo, se le solicitó al EWG que abordara preguntas clave planteadas por el Comité Asesor de Seguridad y Estabilidad (SSAC) en el informe SAC055, y que tuviera en cuenta las operaciones y los servicios de Internet actuales y futuros. El EWG también evaluó las preocupaciones de aquellas partes que brindan, recolectan, mantienen, publican o utilizan estos datos, ya que esto se encuentra relacionado al ámbito de competencia de la ICANN.

[1] La resolución de la Junta Directiva está publicada en el siguiente en enlace: http://www.icann.org/en/groups/board/documents/resolutions-08nov12-en.htm. **En el Anexo A** se destaca la respuesta del EWG a las preguntas específicas de la Junta Directiva.

2.2 Declaración de propósito orientativa de la labor del EWG

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:

- **Permita el acceso apropiado a datos de registración exactos, confiables y uniformes**
- **Proteja la privacidad de la información personal**
- **Permita un mecanismo confiable para identificar, establecer y mantener la capacidad de contactar a los registratarios**
- **Respalde un marco para abordar cuestiones que involucren a los registratarios, lo cual inlcuye, pero no se limita, a lo siguiente: protección del consumidor, investigación de delitos cibernéticos, y protección de propiedad intelectual.**
- **Proporcione una infraestructura para abordar las necesidades en materia de cumplimiento de la ley.**

III. METODOLOGÍA – IDENTIFICACIÓN DE USUARIOS Y PROPÓSITOS

3.1 Metodología de casos de uso

Se incentivó al EWG a, al trabajar en pos de la definición de la próxima generación de servicios de directorio de registración, 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 la nueva generación de RDS.

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 B**.

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 efectos deseados que deberían ser tenidos en cuenta en el RDS, 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.

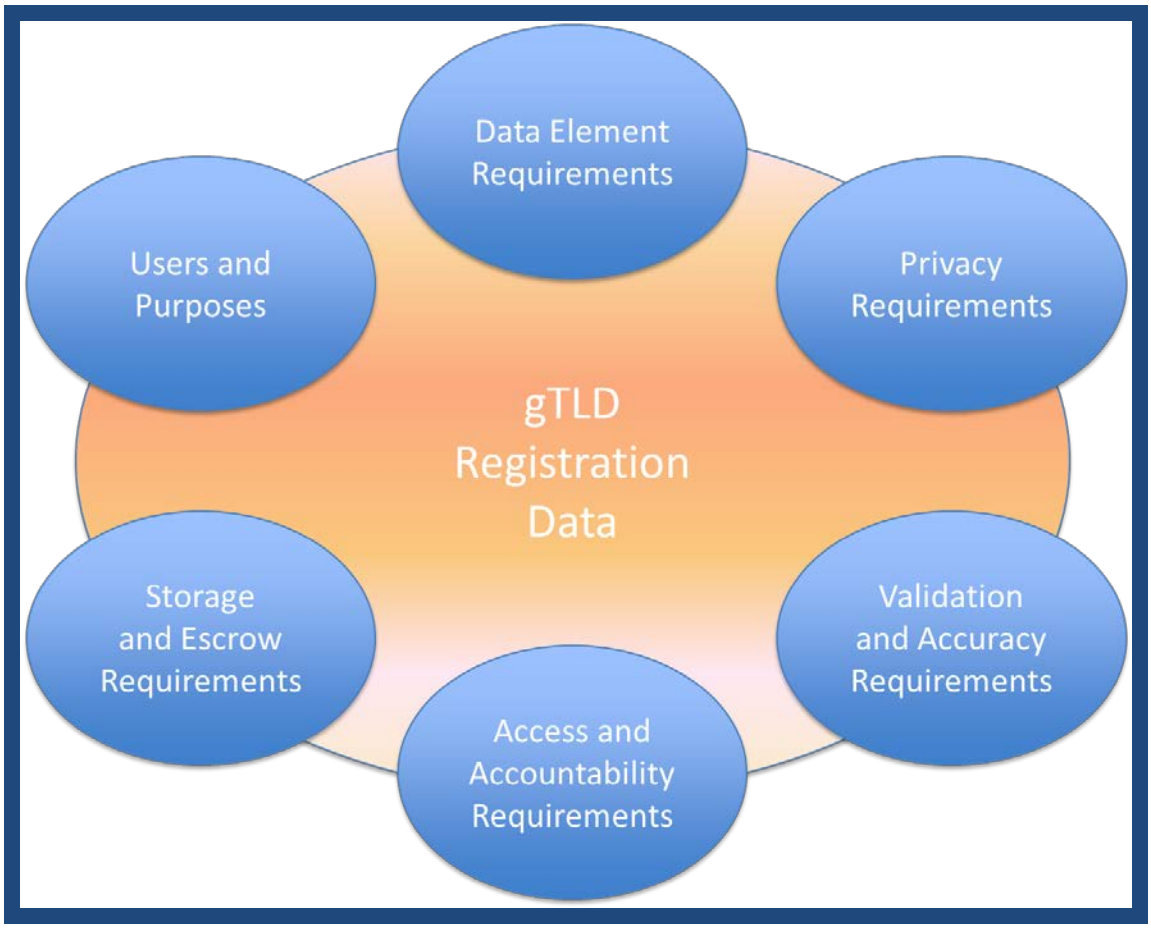

Gráfico 1: Análisis de necesidades

El EWG espera continuar con su labor analizando estos propósitos y necesidades para extraer elementos mínimos de datos, riesgos relacionados, implicancias en materia de legislación y políticas sobre privacidad, y preguntas

adicionales a ser exploradas en mayor detalle en la versión borrador final del presente informe.

3.2 Identificación de los usuarios del RDS

El EWG analizó cada uno de 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. Para más detalles sobre cada caso de uso y las interacciones de los usuarios con el RDS, consulte el **Anexo B**.

Usuario	Finalidad	Ejemplo de casos de uso	Fundamento para acceder a los datos de registración
All **Todos los registratarios** (personas físicas, personas jurídicas, proveedores de servicios de privacidad/proxy)	Control de nombre de dominio	Creación de cuenta de registración de nombre de dominio	Permitir la registración de nombres de dominio por parte de todo registratario mediante la creación de una nueva cuenta con un registrador
		Monitoreo 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
		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
		Transferencias de nombres 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 del DNS a causa de un nombre de dominio	Permitir que un registratario inicie un cambio del DNS en virtud de un nombre de dominio
		Transferencias de nombres de dominio	Permitir la renovación de un nombre de dominio registrado por parte de su contacto administrativo designado (persona física, rol o entidad)
		Validación de contacto del nombre de dominio	Facilitar la validación inicial y continua de los datos de registración del nombre de dominio (por ejemplo, contactos designados, direcciones)
Registratarios Protegidos	Protección de datos personales	Mejorar la protección de la registración	Permitir el uso de servicios acreditados de privacidad o proxy por parte de todo registratario que procure minimizar el

Usuario	Finalidad	Ejemplo de casos de uso	Fundamento para acceder a los datos de registración
(por ejemplo, clientes de servicios de privacidad/proxy)			acceso público a nombres y direcciones personales
		Registración con protección máxima	Permitir el uso de servicios acreditados de registración mediante representación por parte de individuos o grupos que se encuentran amenazados, utilizando credenciales anónimas emitidas por un tercero confiable
Personal técnico de Internet (por ejemplo, admin. de DNS y sitios web)	Resolución de cuestiones técnicas	Contacto con personal técnico del 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)
Proveedores de servicios en línea (por ejemplo, ISPs, proveedores de servicios de alojamiento web, CAs, servicios de reputación)	Suministro de servicios de Internet	Contacto con el registratario del nombre de dominio	Permitir el re-establecimiento del contacto con un cliente (individuo, rol o entidad) para tratar cuestiones comerciales de un nombre de dominio cuando fallan los métodos de contacto usuales de un proveedor
		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
		Servicios de certificación de nombres de dominio	Ayudar a una autoridad de certificación (CA) a identificar al registratario de un nombre de dominio que estará 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 ejemplo, domicilio comercial)
		Protección del consumidor	Costear un mecanismo de bajo perfil para que los consumidores se contacten con registratarios de nombres de dominio (por ejemplo, minoristas *online*) para resolver cuestiones con rapidez, sin la intervención de LE/OpSec
		Acción legal/civil	Ayudar a las víctimas individuales a identificar al registratario de un nombre de dominio involucrado en una actividad potencialmente ilícita para permitir una mayor investigación por parte de LE/OpSec

Usuario	Finalidad	Ejemplo de casos de uso	Fundamento para acceder a los datos de registración
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 de su registratario actual (si lo hubiere)
		Historial de registración de un nombre de dominio	Proporcionar el historial de la registración de un nombre de dominio para identificar registratarios y fechas anteriores
		Nombres de dominio para un registratario especificado	Permitir la determinación de todos los nombres de dominio registrados por una entidad específica (por ejemplo, verificación de fusiones/derivaciones de activos)
Investigadores de Internet	Búsqueda de nombre de dominio	Historial de registración de un nombre de dominio	Permite la investigación y el análisis estadístico de registraciones de nombres de dominio (necesario también para los usuarios comerciales de Internet)
		Nombres de dominio para un registratario especificado	Permite la investigación y el análisis estadístico de registratarios de nombres de dominio (necesario también para los usuarios comerciales de Internet)
		Contacto del registratario del nombre de dominio	Permite realizar relevamientos de los registratarios de nombres de dominio (necesario también para los proveedores de servicios en línea)
Titulares de propiedad intelectual (por ejemplo, titulares de marcas comerciales, propietarios de	Acciones legales	Identificación de clientes de proveedores de servicios de proxy	Permite identificar clientes de servicios de proxy/representación asociados a un nombre de dominio que está siendo investigado por un posible incumplimiento o robo de propiedad intelectual (revelación)
		Contacto del usuario del nombre de dominio	Permite contactar a la parte que utiliza un nombre de dominio que está siendo investigado por incumplimiento en

Usuario	Finalidad	Ejemplo de casos de uso	Fundamento para acceder a los datos de registración
marcas comerciales, titulares de propiedad intelectual)			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, domicilio) que pertenecen a otro registratario, y la respuesta a dicho uso fraudulento
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 contractual y regulatorio efectivo	Investigación impositiva en línea	Facilitar la identificación de un 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 para evitar ser demandado (*cyberflight*)
		Cumplimiento contractual del RAA	Permitir que el Departamento de Cumplimiento Contractual de la ICANN audite y responda a los reclamos sobre la conducta de los registradores (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 ejemplos, organismos que se encargan del cumplimiento de la ley, equipos de respuesta ante incidentes)	Mitigación de abusos	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
		Contacto en caso de abuso 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/ISP designado para lidiar con el abuso
Delincuentes (por ejemplo, los que participan en el envío de	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 el/los nombre(s) de dominio de ese

Usuario	Finalidad	Ejemplo de casos de uso	Fundamento para acceder a los datos de registración
correo electrónico no deseado, DDoS, suplantación de identidad, robo de identidad, secuestro de nombre de dominio)			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 no deseados o engañosos	Recolectar datos del registratario de un nombre de dominio para uso maliciosos por parte de quienes envían correos electrónicos no deseados, engañosos y demás delincuentes

Tabla 1. Usuarios

En la Figura 2, se presenta un resumen no ejecutivo de usuarios del sistema de WHOIS existente, tanto con fines constructivos como 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 la Sección IV, el EWG recomienda abandonar el modelo actual de WHOIS (y su protocolo) que le otorga a cada usuario el mismo acceso público y anónimo a datos de registración de gTLD (frecuentemente inexactos). En lugar de ello, 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 únicamente a solicitantes autorizados y responsables usarlos apropiadamente.

3.3 Identificación de los fines a ser aceptados y los fines a ser prohibidos

El EWG procure priorizar los fines enumerados en la sección 3.2 con el fin de focalizarse en el desarrollo de casos 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 resultado llevó al EWG a recomendar que todas las finalidades identificadas en la sección 3.2 fuesen incorporadas al RDS de algún modo, con excepción de actividades maliciosas conocidas en Internet que debieran ser disuadidas. Las finalidades permisibles recomendadas por el EWG se resumen a continuación.

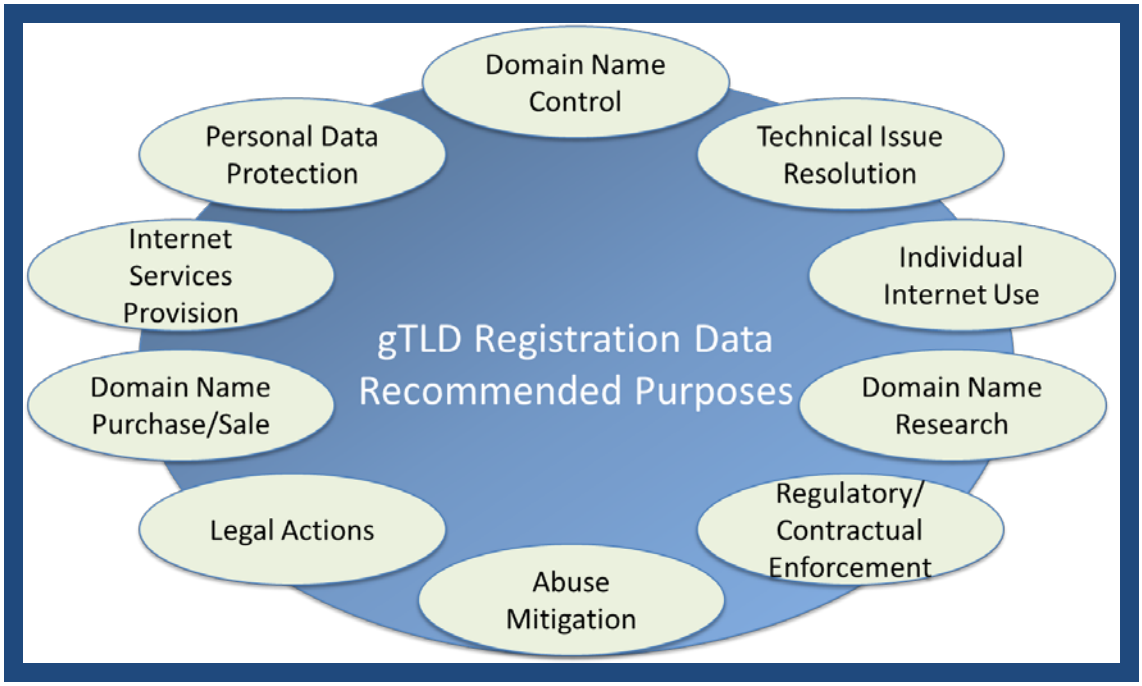

Figura 3: Finalidades

Cabe señalar que, dentro de cada finalidad, hay un número infinito de casos de uso existentes y potenciales. Si bien el EWG no intentó identificar todas las finalidades de uso posibles, hizo su mayor esfuerzo por explorar una muestra representativa con la esperanza de efectuar una identificación rigurosa de las clases de usuarios y sus finalidades al procurar el acceso a los datos de registración de gTLD. Sin embargo, el RDS debería ser diseñado con la capacidad de incorporar nuevos usuarios y finalidades permisibles que probablemente surjan con el transcurso del tiempo.

3.4 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, mapeadas en base a fines relacionados. Algunas partes interesadas suministran datos (por ejemplo, los registratarios), mientras que otras recolectan/almacenan datos (por ejemplo, registradores, registros) o los divulgan (por ejemplo, operador del RDS, proveedores de servicios de privacidad o

proxy/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 en caso de abuso 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	Finalidades
Contacto designado en caso de abuso del nombre de dominio	Mitigación de abusos
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	Suministro de servicios de Internet
Reclamante/demandante	Cumplimiento efectivo de normas regulatorias/contratos
Consumidores que usan 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
Departamento de Cumplimiento Contractual de la ICANN	Cumplimiento efectivo de normas regulatorias/contratos
Proveedores de Servicios de Internet	Mitigación de abusos
Investigador	Uso individual de Internet
Personal de organismos encargados del cumplimiento de la ley	Mitigación de abusos Acciones legales
Contactos listados	Suministro de servicios de Internet
Proveedor de servicios en línea	Suministro de servicios de Internet
Proveedores de servicios de seguridad operativa	Mitigación de abusos

Organismo que patrocina un estudio	Búsqueda de nombre de dominio
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 Control de nombre de dominio Suministro de servicios de Internet Cumplimiento efectivo de normas regulatorias/contratos Protección de datos personales
Proveedor de servicios de privacidad/representación	Mitigación de abusos Compra o venta comercial de nombre de dominio Control de nombre de dominio Investigación de nombre de dominio Suministro de servicios de Internet Acciones legales Protección de datos personales Cumplimiento efectivo de normas regulatorias/contratos Resolución de cuestiones técnicas
Operador del RDS	Todas las finalidades
Registratario	Todas las finalidades
Agente/mandatario del registratario	Compra o venta comercial de nombre de dominio Suministro de servicios de Internet Cumplimiento efectivo de normas regulatorias/contratos
Registrador	Compra o venta comercial de nombre de dominio Control de nombre de dominio Investigación de nombre de dominio Uso individual de Internet Suministro de servicios de Internet Acciones legales Protección de datos personales Cumplimiento efectivo de normas regulatorias/contratos Resolución de cuestiones técnicas Mitigación de abusos
Registro	Todas las finalidades
Informante de un problema	Resolución de cuestiones técnicas
Investigador	Búsqueda de nombre de dominio
Revendedor	Mitigación de abusos
Resolutor de un problema	Resolución de cuestiones técnicas
Destinatario de acciones legales/civiles	Uso individual de Internet
Contacto técnico	Resolución de cuestiones técnicas
Terceros que buscan contacto	Acciones legales Protección de datos personales
Agente/mandatario de confianza	Protección de datos personales
Panelistas de UDRP	Cumplimiento efectivo de normas regulatorias/contratos
Proveedor de UDRP	Cumplimiento efectivo de normas regulatorias/contratos
Validador del aumento de necesidad de protección	Protección de datos personales

Víctima de abuso	Mitigación de abusos
Proveedor de servicios de alojamiento en la Web	Resolución de cuestiones técnicas

Tabla 2. Resumen representativo de las partes interesadas

3.5 Áreas en común

A medida que el EWG analizó los casos de uso, fue quedando claro que muchos usuarios tienen necesidades de obtener elementos de datos similares, pero con finalidades distintas. 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

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
- La capacidad de determinar cuando un nombre de dominio fue registrado por primera vez

El EWG tuvo en cuenta estas necesidades en común al desarrollar los principios recomendados para orientar el diseño del RDS. Sin embargo, dado que es probable que se identifiquen más necesidades en común con el transcurso del tiempo, el sistema debería ser diseñado teniendo en cuenta la posibilidad de su ampliación.

3.6 Coincidencia de elementos de datos con finalidades aceptables

En el **Anexo C** se describen los elementos de datos relevantes para cada finalidad aceptable. En última instancia, algunos de estos elementos de datos deberían ser recolectados para cada nombre de dominio, mientras que otros

pueden ser recolectados de manera optativa para un sub-grupo de nombres de dominio. Asimismo, los elementos de datos recolectados pueden o no estar disponibles para los solicitantes mediante el RDS. El EWG espera considerar en mayor profundidad estas cuestiones para arribar a recomendaciones iniciales al respecto, pero recomienda que se efectúe un análisis de riesgo e impacto más exhaustivo de cada elemento de datos para completar esta categorización. Sería de utilidad recibir comentarios públicos para identificar como debería efectuarse el análisis de riesgo e impacto, quien debería realizarlo, los criterios de cada elemento de datos a ser identificados como obligatorios u optativos, para su recolección o divulgación mediante acceso público o restricto.

IV. CARACTERÍSTICAS DESEADAS & PRINCIPIOS DE DISEÑO

Con sujeción a futuros análisis apropiados de riesgo e impacto en múltiples área, el EWG cree que la próxima generación de Servicios de Directorio de Registración (RDS) debería incluir los siguientes principios y características:

	Característica	Principios de diseño del EWG
4.1	**Aplicabilidad**	
	4.1.1	• Es necesario que el RDS se aplique a todos los registros de gTLD, tanto existentes como nuevos. No debería permitirse ninguna cláusula de derechos adquiridos o excepción especial.
4.2	**Consideraciones Internacionales**	
	4.2.1 4.2.2	• Cada una de las partes interesadas que participen del RDS deberían establecer una o más políticas respecto del acceso a los datos, el uso de los datos, la retención de los datos y el debido proceso. o Dichas políticas pueden variar según cada jurisdicción o Estas políticas deben permitir el cumplimiento de las leyes locales o Los expertos del EWG deben analizar estas cuestiones en mayor profundidad • Para ser verdaderamente global, el RDS debería mostrar los datos de registración en múltiples idiomas, códigos de escritura y conjuntos de caracteres o Es necesario un mayor análisis por parte de los expertos en materia de IDN para definir estos requisitos
4.3	**Responsabilidad**	
	4.3.1 **4.3.2** **4.3.3**	• Todas las partes del ecosistema de nombres de dominio tienen responsabilidades mutuas. • Los registratarios son responsables de proveer y mantener datos de registración actuales, precisos y puntuales en el RDS. • Los registratarios son responsables de

	4.3.4 4.3.5 4.3.6	asegurar que alguien esté disponible para facilitar la resolución oportuna de cualquier problema que pueda surgir en relación con sus nombres de dominio. • Los registratarios asumen la responsabilidad de la registración y el uso de su nombre de dominio. • Los registradores son responsables de proveer el servicio a los registratarios según se especifica en sus contratos, lo cual incluye el suministro de datos de registración actuales y precisos. • Debería haber repercusiones por la falta de suministro y mantenimiento de información precisa. o El EWG espera analizar estas cuestiones en mayor profundidad
4.4	**Consideraciones de privacidad**	
	4.4.1 4.4.2 4.4.3 4.4.4	• El RDS debería incorporar las necesidades de privacidad, entre las que se incluyen: o Un Servicio Mejorado de Registración Protegida para satisfacer las necesidades generales de privacidad de datos personales; y o Un Servicio de Máxima Registración Protegida que ofrezca el servicio de credenciales con protección de seguridad para usuarios en riesgo, o finalidades de libertad de expresión. • Debería haber una acreditación para los proveedores de servicios de privacidad/representación y reglas para el suministro y uso de servicios de privacidad/representación acreditados. • 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. • El EWG espera analizar estas cuestiones en mayor profundidad, incluyendo: o Procesos estandarizados a ser implementados por todos los

		proveedores de servicios de privacidad y representación acreditados. o Procesos específicos relacionados con el manejo de solicitudes cursadas por organismos de cumplimiento de la ley acreditados. o Procesos específicos relacionados con el manejo de solicitudes cursadas por otros solicitantes autorizados (por ejemplo, titulares de propiedad intelectual).
4.5	**Finalidades permisibles**	
	4.5.1 **4.5.2**	• Los usos permisibles/no permisibles del sistema deberían estar claramente identificados. • **En la Sección 3** se incluyen una descripción general de los usos aceptables identificados por el EWG.
4.6	**Divulgación de datos**	
	4.6.1 4.6.2 4.6.3 4.6.4 4.6.5 4.6.6	• El RDS debería incorporar la divulgación de elementos de datos con una finalidad • No todos los datos recolectados han de ser públicos; las opciones de divulgación deberían depender del solicitante y la finalidad • Debería permitirse el acceso público a un conjunto mínimo de datos identificados, con restricciones para limitar la recolección masiva de datos. • Los elementos de datos considerados de alta sensibilidad una vez efectuado el análisis de riesgo e impacto deberían estar protegidos mediante acceso restricto, en base a lo siguiente: ▪ Identificación de una finalidad permisible ▪ Divulgación fidedigna del solicitante/ la finalidad ▪ Auditoría/cumplimiento contractual para garantizar que no se haga uso abusivo del acceso restricto • Se podría acceder a ciertos elementos de datos considerados de alta

	4.6.7	sensibilidad (tras el análisis de riesgo e impacto) mediante un proceso legal (por ejemplo, citación judicial) • Solamente deberían divulgarse los elementos de datos permisibles para el fin declarado • En el **Anexo C** se describen los elementos de datos considerados relevantes para los usos aceptables específicos identificados en el **Anexo B**.
4.7	**Elementos de datos**	
	4.7.1 **4.7.2** **4.7.3** **4.7.4** **4.7.5**	• Los únicos elementos de datos que deberían ser recolectados son los que tienen al menos una finalidad permisible • Cada elemento de datos debería estar asociado a fines permisibles, en base a los usos permisibles identificados. • La lista de elementos de datos mínimos a ser recolectados, almacenados y divulgados públicamente debería basarse en una evaluación de riesgo. • Con el fin de permitir la ampliación, el sistema debería incorporar todos los elementos de datos adicionales recolectados por los registros, haciendo que estén disponibles a través de los métodos e interfaces de acceso común • Todo el conjunto de elementos de datos debería ser almacenado por los registros.
4.8	**Métodos de acceso**	
	4.8.1 **4.8.2**	• El acceso debería ser no-discriminatorio (es decir, el proceso debería crear reglas de participación parejas para todos los solicitantes, dentro de la misma finalidad) • Con el fin de disuadir el uso indebido y promover la responsabilidad: o Todo acceso debería estar autenticado dentro del nivel apropiado, y o Los solicitantes que necesiten acceder a elementos de datos deberían poder solicitar y recibir

	4.8.3 4.8.4 4.8.5 4.8.6 4.8.7	credenciales de uso a ser utilizadas en futuras solicitudes autenticadas de acceso a datos. • Se debería solicitar cierto tipo de acreditación a los solicitantes de acceso restricto o Cuando los solicitantes acreditados consulten datos, ¿su finalidad debería estar [alternativa a] implícita, o [alternativa b] declarada cada vez que se cursa una solicitud?[2] o Podrán aplicarse distintos términos y condiciones a las distintas finalidades. o Se deberían aplicar penalidades ante un incumplimiento de los términos y las condiciones por parte de los solicitantes acreditados. • Todas las consultas/respuestas deberían proteger la confidencialidad e integridad de los datos en tránsito. • Se podrán ofrecer servicios Premium de acceso a datos (por ejemplo, WHOIS inverso, WhoWas), sujetos a cierto tipo de régimen de acreditación. • Todas las divulgaciones deberían efectuarse a través de métodos de acceso definidos. No se debería exportar todo el conjunto d de datos en forma masiva con el fin de permitir un acceso no controlado. • La divulgación puede incluir la exhibición y otros métodos de publicación. o Con el fin de que los datos se encuentren más fácilmente y de manera uniforme, se debería ofrecer un punto de acceso centralizado (por ejemplo, un portal en la web). o Todos los solicitantes deberían poder acceder a los datos públicos a través de un método de consulta

[2] El EWG deben analizar estas dos alternativas en mayor profundidad

		anónimo (como mínimo, mediante un sitio web). o El acceso restricto a datos sensibles debería contar con soporte en la web y en otros métodos y formatos de acceso (por ejemplo, respuestas XML, SMS, correo electrónico), en base a la finalidad y el propósito del solicitante. o Los solicitantes deberían poder obtener datos autoritativos en tiempo real cuando lo necesiten.
4.9	**Validación y exactitud**	
	4.9.1 4.9.2 4.9.3	• Con el fin de mejorar la calidad de los datos, se debería realizar la validación sintáctica de los datos del registratario (es decir, se debería verificar su formato correcto [según el documento SAC58]) al momento de su recolección. • Con el fin de mejorar la usabilidad, se debería realizar una validación operativa de los datos de contacto/el nombre del registratario. (es decir, se debería verificar que se los pueda contactar). • Con el fin de reducir el fraude: o Los registratarios deberían poder ser pre-validados mediante el suministro de un nombre/una organización de registratario y un contacto asociado, únicos a nivel global, antes de la registración inicial del nombre de dominio. o Una vez que se haya verificado la precisión y la singularidad de los datos pre-validados, se le debería entregar un código de autorización (por ejemplo, un PIN) a dicho registratario. No se deberían registrar nombres de dominio con

	4.9.4 4.9.5 4.9.6 4.9.7 4.9.8 4.9.9 4.9.10	una organización o un nombre idéntico[3] sin que se proporcione este código de autorización. o La ICANN debería celebrar un contrato apropiado con un proveedor externo que proporcione este servicio de pre-validación y emita los códigos de autorización. • Con el fin de promover la consistencia y la uniformidad, y de simplificar el mantenimiento: o Los elementos de datos pre-validados deberían ser reutilizables – es decir, se los debería poder aplicar a futuras registraciones, con la opción de circunscribir dichas pre-validaciones por defecto caso a caso, según cada dominio. o Toda actualización de elementos de datos pre-validados podrían ser aplicados automáticamente a todos los nombres de dominio relacionados. • Con el fin de mejorar la calidad, el nombre/los datos de contacto del registratario que no se encuentren pre-validados deberían ser validados de algún modo (por ejemplo, en forma implícita mediante un pago exitoso con tarjeta de crédito con el nombre/o los datos de contacto). • Con el fin de preservar la activación rápida sin dejar de fomentar la calidad, el retraso de la validación del nombre/los datos de contacto del registratario no deberían evitar la registración exitosa y la inclusión en el lista del DNS. Sin embargo, dichos nombres de dominio podrían ser marcados y suspendidos/eliminados, si no se los valida dentro de un plazo especificado. • Con el fin de permitir la validación global exitosa del nombre/los datos de contacto

[3] El EWG espera analizar este tema en mayor profundidad

		del registratario, los métodos de validación operativa no deberían basarse exclusivamente en un único método de contacto (por ejemplo, el domicilio postal). • Con el fin de mantener la calidad de los datos con el transcurso del tiempo, los elementos de datos validados deberían ser vueltos a validar periódicamente - por ejemplo, cada vez que se realicen actualizaciones de nombres/datos de contacto o que se transfieran nombres de dominio vinculados un nombre/contacto previamente validado. • El sistema no debería registrar si cada elemento de datos fue validado, ni cuando se efectuó dicha validación, incluso en el caso de elementos de datos que nunca sean divulgados. • Con el fin de promover la registración exitosa de nombres de dominio vinculados con nombres/datos de contacto de alta calidad, se debe educar a los registratarios sobre este proceso y sus políticas asociadas.
4.10.	**Servicio de validación estándar**	
	4.10.1 **4.10.2**	• El uso de un servicio de validación estándar es preferible por los siguientes motivos: o Reduce costos/molestias para registradores y registros o Permite una autorización más eficiente de bases de datos de validación como la verificación cruzada de domicilios de UPS, las páginas amarillas, los datos corporativos/de gobierno, los registros gubernamentales, los padrones electorales, los informes crediticios, etc. o Estandariza la validación de procedimientos apropiados para un país o una jurisdicción específicos. o Reduce el número de consultas por cumplimiento que reciben los registros/registradores.

		• La ICANN debería celebrar un contrato apropiado con un proveedor externo que brinde los servicios de validación estándar en forma tal que permita el cumplimiento en materia de exactitud, auditoría y disponibilidad de los datos.
4.11	**Relaciones contractuales**	
	4.11.1 4.11.2 4.11.3 4.11.4	• El RDS debería estar operado por un proveedor externo verdaderamente internacional. • La ICANN debería celebrar un contrato apropiado con un proveedor externo de RDS para permitir el cumplimiento, la auditoría y la disponibilidad. • La ICANN debería celebrar contratos apropiados con un proveedor de servicios de validación estándar, proveedores de servicios de privacidad/representación, proveedores de credenciales con protección de seguridad, y demás proveedores que puedan interactuar con el RDS. • La ICANN debería modificar los acuerdos existentes (RAA, acuerdos de registro) para incorporar el RDS y eliminar los requisitos legados.
4.12	**Requisitos de almacenamiento y custodia**	
	4.12.1 **4.12.2** **4.12.3**	• Con el fin de mantener sistemas redundantes y eliminar el punto único de fallas, los datos deberían estar alojados en múltiples ubicaciones (por ejemplo, registrador, registro, custodia de datos y RDS). • Se deberían efectuar auditorias de datos en custodia para evaluar su formato e integridad, y que sean completos. • El RDS debería mantener los elementos de datos en forma segura, protegiendo la confidencialidad y la integridad de los elementos de datos en riesgo, y preservándolos el uso no autorizado.
4.13	**Costos operativos y de acceso al RDS**	

	4.13.1	• La cuestión del costo es un aspecto importante del RDS. El EWG espera analizar esta cuestión en mayor profundidad, incluyendo un análisis de costos de desarrollo y operativos, y las formas posibles de afrontar dichos gastos (por ejemplo, siendo absorbidos por fondos del RDS, o compensados por honorarios de servicios con valor agregado).

V. MODELO SUGERIDO

La necesidad de recolectar, almacenar y divulgar elementos de datos precisos con diversas finalidades llevó al EWG a proponer un modelo general para la próxima generación de RDS que cumpla con los principios identificados en la Sección 4. Cada actor en el ecosistema del RDS tiene distintas necesidades de obtener datos, distintos riesgos y distintas responsabilidades potenciales. Históricamente, la mayoría de estas responsabilidades era transferida a los registradores, cuyo objetivo principal era proporcionar nombres de dominio en funcionamiento a los clientes, y mantener a los clientes que abonaran ese servicio. El EWG reconoce que, a medida que el ecosistema de Internet se torna más complejo, y con la introducción de cientos de nuevos gTLDs, es probable que se requiera a más actores adoptar las múltiples responsabilidades que implica cumplir con una gama tan amplia de finalidades de los datos de registración.

En base a las características y a los principios de diseño establecidos en la Sección 4, en la Figura 4 se incluye el modelo recomendado por el EWG para la próxima generación de RDS que podría incluir a muchos de estos principios.

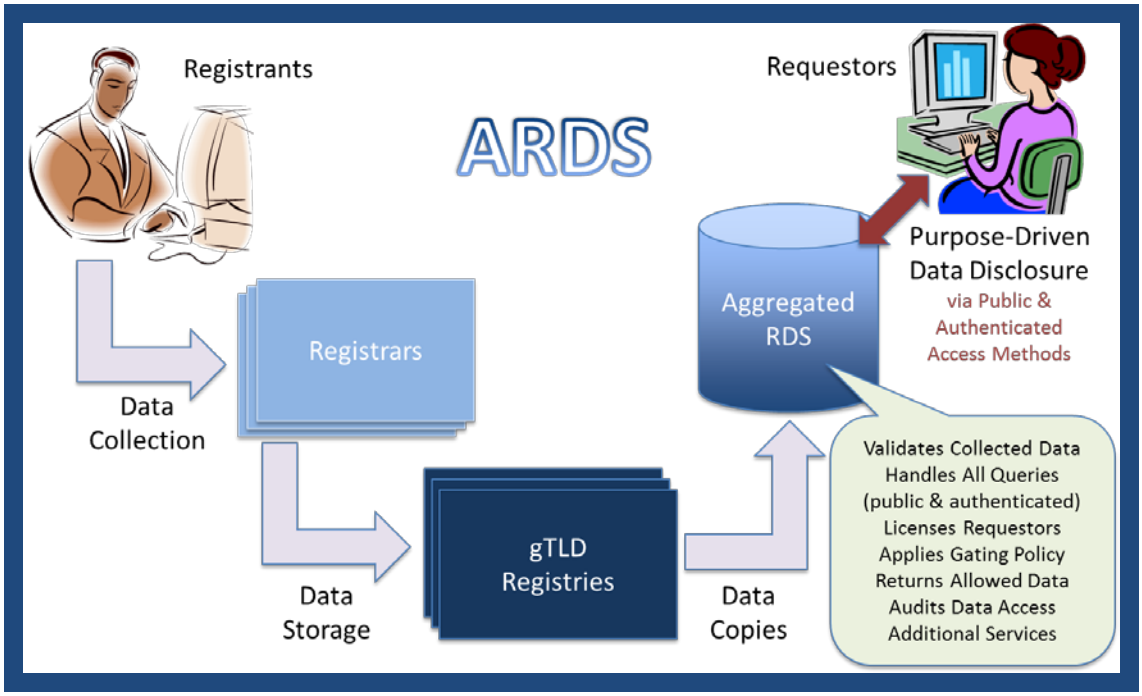

Figura 4. Modelo de RDS Agregado

5.1 Análisis de diversos diseños del sistema

Luego de identificar los principios recomendados y las características deseadas de un nuevo RDS, el EWG consideró varios modelos alternativos para determinar la forma en que cada modelo podría abordar las necesidades identificadas en materia de registración de datos. El EWG evaluó sistemas distribuidos, como los que se emplean hoy en día en el sistema de WHOIS, como también sistemas agregados. Asimismo, el EWG consideró un sistema de tipo representativo, en el cual un tercero sería el intermediario que permita el acceso a los datos consultados, pero no se desempeñaría como repositorio de dichos datos. El trabajo del Grupo Asesor sobre Acceso al Archivo de Zona (ZFA)[4] que consideró cuestiones similares en el contexto de del Programa de los nuevos gTLD fue valioso en tanto que brindó información a la cual el EWG recurrió para entender esta cuestión.

[4] Para mayor información, consulte los archivos del Grupo Asesor sobre el Acceso al Archivo de Zona en el siguiente enlace: http://archive.icann.org/en/topics/new-gtlds/zone-file-access-en.htm

Los sistemas distribuidos presentan desventajas que se verían abordadas de mejor manera mediante modelos alternativos. Ante la potencial inclusión en línea de miles de registros, el EWG reconoció que la continuidad de los sistemas distribuidos actuales introduce ineficiencias y costos adicionales ya es posible que los consumidores de esta información tengan que lidiar con distintos formatos, credenciales, puntos de acceso, condiciones de otorgamiento de licencia, y demás obstáculos que puedan ser creados por el registro o registrador. Tal como lo señalara el Grupo Asesor sobre el ZFA, cuando "se utilizan sistemas dispares, los procesos o la automatización implementados por consumidores de archivos de zona son más proclives a fallar. Cuando se producen errores el resultado es la pérdida de acceso, y la resolución del problema es engorrosa para los consumidores de datos debido a que el consumidor debe participar en sistemas únicos de presentación de informes para resolver el inconveniente."[5] Estas cuestiones serían igualmente aplicables al RDS.

Asimismo, los costos asociados con requerir que cada registro y/o registrador modifique sus sistemas para crear un nuevo sistema distribuido para implementar un nueva generación de RDS probablemente limiten la innovación y la adopción, dado que no hay un incentivo financiero u operativo aparente para respaldar los cambios al método por el cual se accede a estos datos. Tal como lo indicara el Grupo Asesor sobre el ZFA:

> "En general, el proporcionar un acceso fiable a los datos del archivo de zona impone costos operativos y responsabilidades para los registros de Dominios Genéricos de Alto Nivel (gTLD), sin existir una compensación directa. Si bien esto ha sido aceptado por los operadores del registro como un costo asociado con la operación de uno de los espacios de nombres principales de Internet, sería lógico para los registros que se

[5] Véase el Documento sobre el Concepto de Archivo de Zona, publicado en: http://archive.icann.org/en/topics/new-gtlds/zfa-concept-paper-18feb10-en.pdf

> reduzcan estos costos si existiese una manera más eficiente de ofrecer ese acceso. Por ejemplo, se requiere que los registros brinden acceso continuo a todos los solicitantes, sin existir ninguna especificación respecto a los Acuerdos de Nivel de Servicio (SLAs). Claramente, el operar de esta manera cuesta dinero si el registro también es responsable de proporcionar una conexión segura y archivos de datos limpios a los consumidores de datos, lo cual crea importantes requisitos de seguridad para los registros."[6]

Asimismo, tanto los sistemas distribuidos como los sistemas de representación dificultan o hacen imposible el ofrecimiento de características necesarias en común, tales como búsqueda cruzada de registratarios de TLD, búsqueda inversa de registratario-dominio o incluso un tipo de registro de titularidad histórica. Todas estas características podrían ser posibles mediante una base de datos agregada en la cual se realice la recolección y el mantenimiento de los datos aplicables.

5.2 RDS agregado sugerido

Un modelo de RDS agregado (ARDS), tal como se lo ilustró anteriormente, fue respaldado por consenso en el EWG, como una manera de abordar las características deseadas y los principios de diseño identificados en la Sección 4.

En el modelo propuesto:

- El ARDS sirve como un repositorio agregado que contiene una copia no autoritativa de todos los elementos de datos recolectados.
- Cada registro de gTLD continúa siendo una fuente autoritativa de datos.
- Los solicitantes solicitan las credenciales de acceso al ARDS

[6] Véase el Documento sobre el Concepto de Acceso de Archivo para mayores consideraciones.

- Los registradores/registros quedan liberados de sus obligaciones de brindar acceso mediante Puerto 43, o de otros requisitos de acceso público.
- En la mayoría de los casos, el ARDS brinda acceso a datos de registración en memoria caché que copiados de los registros de gTLD, con actualizaciones periódicas.
- El ARDS también puede permitir el acceso a datos de registración obtenidos en tiempo real de los registros de gTLD, a pedido. El ARDS (o un tercero que interactúe con el ARDS) sería responsable de efectuar los servicios de validación.
- El ARDS es responsable de auditar el acceso para minimizar el abuso e imponer penalidades y demás medidas para subsanar el acceso indebido.
- El ARDS maneja los reclamos por exactitud de datos.
- El ARDS maneja los acuerdos de licencia de acceso de datos.
- La ICANN contrata a un proveedor internacional tercerizado que se encargue del desarrollo y la operación del ARDS, y del monitoreo del cumplimiento de los requisitos.

	Modelo de RDS Agregado
Ventajas	• Escala manejada por un único punto de contacto • Posibles mejoras en el transporte y la entrega • "Único sitio de consulta" para solicitantes de datos de registración • Mayor responsabilidad en cuanto al acceso y la validación de datos de registración (medida anti-abuso). • Capacidad de rastrear/auditar/penalizar a los solicitantes de igual modo en múltiples TLDs (medida anti-abuso) • Puede reducir algunos costos actualmente afrontados por registradores y registros al brindar acceso a datos • Se pueden brindar servicios de normalización o filtrado de datos • Reduce los requisitos de ancho de banda para registros y

	Modelo de RDS Agregado
	registradores • Facilita la estandarización de enfoques para atender inquietudes locales en materia de privacidad de datos • Mejor capacidad de búsqueda en múltiples TLDs (por ejemplo, búsqueda inversa) • Se minimizan costos de transición e implementación • Permite la validación/acreditación de solicitantes que califican para fines especiales (por ejemplo, organismos a cargo del cumplimiento de la ley) • Facilita una gestión más eficiente de inexactitud en informes • Permite realizar verificaciones aleatorias de exactitud con mayor eficiencia • Permite mostrar información en múltiples idiomas, códigos de escritura y caracteres en un portal de búsqueda fácil de usar
Desventajas	• Latencia de datos • Creación de una fuente de "grandes datos" con datos sumamente valiosos que pueden ser usados indebidamente sin una auditoria y un mantenimiento apropiados • Mayor riesgo de abusos internos y ataques externos, lo cual requiere prestar más atención a la implementación, el cumplimiento efectivo y la auditoria de políticas de seguridad • Los registros/registradores ya controlan la entrega de los datos de registración

VI. TRATAMIENTO DE CUESTIONES RELATIVAS A LA PRIVACIDAD

La cuestión de la exactitud de los datos de registración es central dentro del ámbito de incumbencia del EWG. Si la próxima generación de RDS requiere una exactitud mucho mayor de los datos de registración, entonces surgen varias cuestiones de inmediato y, probablemente, una de las cuestiones más polémicas sea la cuestión de la privacidad.

El EWG reconoce la necesidad de la exactitud, junto con la necesidad de proteger la privacidad de los registratarios que puedan requerir una mayor protección de su información personal. Los ejemplos de registratarios que podrían calificar para recibir estas protecciones mayores incluyen a individuos o grupos bajo amenaza, los que quieren ejercer los derechos a la libertad de expresión en Internet – los cuales se consideran protegidos en gran medida – o en las instancias en las que la identificación de los oradores podría significar una amenaza para sus vidas o las de sus familias.

De conformidad con los principios recomendados que se enumeran en la Sección 4.4, el EWG ha debatido maneras en las cuales el RDS podría incorporar las necesidades de los usuarios en riesgo de recibir servicios con protección máxima con “credenciales con protección de seguridad”. Una opción podría ser que la ICANN acreditase a un organismo independiente para que se desempeñe como un representante de confianza que, mediante un conjunto de criterios acordados, determinase si un registratario califica para recibir en máximo nivel de protección. El EWG espera considerar en mayor profundidad los posibles modelos de credenciales con protección de seguridad que puedan lograr un equilibrio efectivo e innovador entre la responsabilidad y las necesidades de protección de la privacidad de los usuarios de Internet en riesgo.

VII. ILUSTRACIÓN DE LAS CARACTERÍSTICAS DEL ACCESO RESTRICTO

El modelo de acceso restricto propuesto (ilustrado en la Figura 5) puede resumirse de la siguiente manera:

- Un subconjunto de elementos de datos cuidadosamente seleccionados estaría accesible públicamente a los solicitantes anónimos mediante una le interfaz[7] web para de acceso al RDS.
- Los elementos de datos restantes serían accesibles a los solicitantes autorizados únicamente a través de métodos de acceso restricto multi-modales con soporte por parte del RDS.
- El acceso restricto estaría disponible únicamente para los solicitantes que hayan solicitado y recibido credenciales a ser utilizadas en al autenticación de consultas al RDS. El proceso mediante el cual se emitirían las credenciales no se define en este documento, pero el EWG recomienda que este proceso tenga en cuenta la finalidad de cada solicitante para querer acceder a los datos de registración.
- En cada consulta de acceso restricto se identificaría la finalidad del solicitante autenticado (en forma implícita o explícita) y una lista deseada de elementos de datos. Se retornarían únicamente los elementos de datos disponibles para el nombre de dominio y accesibles al solicitante para la finalidad declarada.

El EWG espera examinar métodos de acceso multi-modal, y la manera de habilitarlos en protocolos de acceso a datos de registración actuales o futuros

[7] El EWG espera explorar en mayor profundidad la posibilidad de que ciertos elementos de datos de registración asociados con el nombre de dominio de un sitio web visitado estén disponibles mediante la integración del navegador.

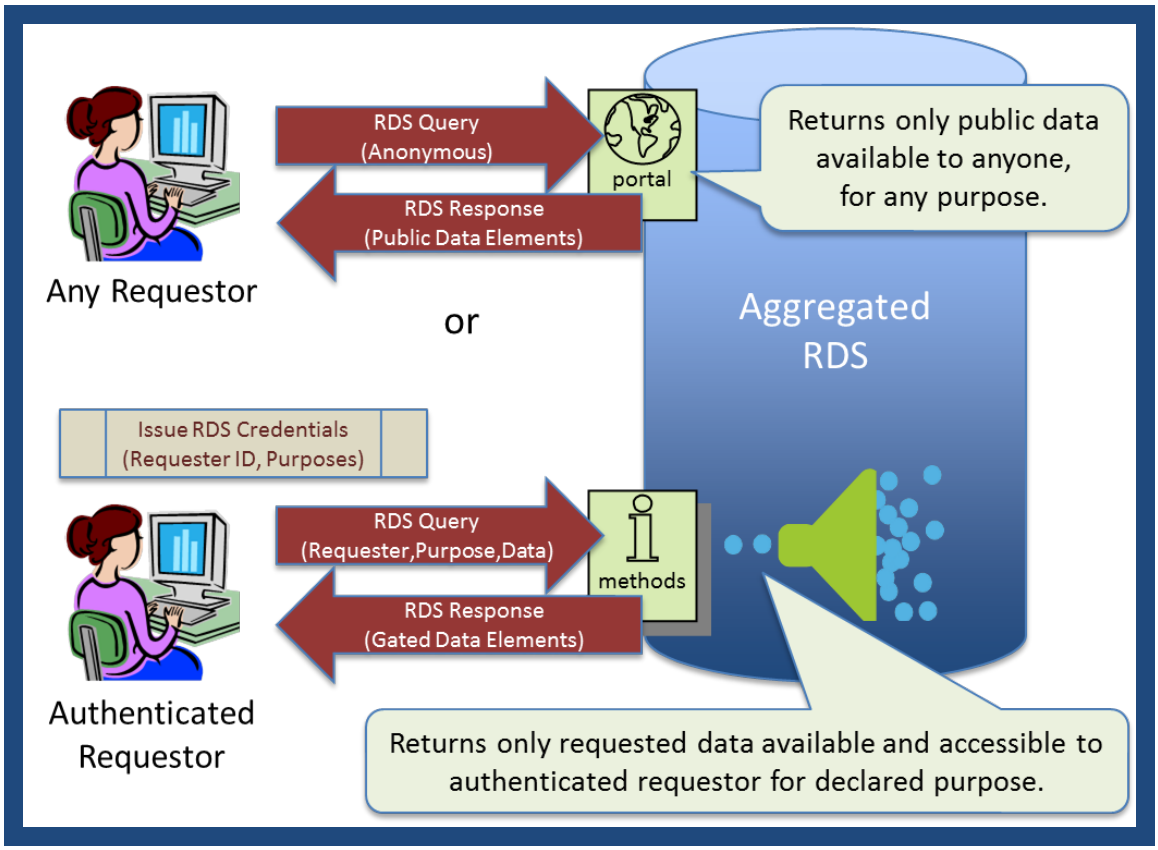

Figura 5. Modelo de acceso restricto

VIII. CONCLUSIÓN Y PRÓXIMOS PASOS

El EWG sugiere la adopción de un RDS agregado en reemplazo del sistema de WHOIS actual para cumplir con los principios de diseño y las características que identificó el EWG y que se describen más exhaustivamente en el presente informe. Esto contempla el respaldo de una característica de “credenciales con protección de seguridad” que permita una mayor protección de la privacidad para los registratarios considerados en riesgo, como los que ejercen sus derechos a la libertad de expresión. Asimismo, el grupo propone recomendaciones para validar los datos de registración recolectados con el fin de incrementar la exactitud, junto con una mayor responsabilidad mediante controles de "acceso restricto” que permitan que los solicitantes que necesitan recibir información adicional soliciten credenciales de acceso limitado, en base a la finalidad declarada. El modelo propuesto incorpora la responsabilidad y las capacidades de auditoría cuyo objetivo es penalizar el uso indebido por parte de los solicitantes que procuren ir más allá de su nivel de acceso autorizado.

Es importante reconocer que el modelo propuesto refleja acuerdos que se lograron tras un arduo trabajo entre los diversos miembros del EWG, y que seguramente no satisfará a todas las partes interesadas afectadas por el RDS. Sin embargo, el EWG espera que estas recomendaciones, en su conjunto, puedan ser reconocidas como una mejora significativa en relación al sistema de WHOIS actual.

El EWG recibirá con agrado el comentario público en línea y el debate dentro de la comunidad de la ICANN en la reunión de la ICANN en Durban sobre preguntas específicas identificadas en el foro, como también todo comentario sobre este informe, que servirán como información para sus próximas deliberaciones. Luego de una consulta pública sobre este informe, el EWG se reunirá nuevamente para reflexionar sobre los comentarios recibidos, y para efectuar las revisiones pertinentes a sus recomendaciones. Una vez finalizadas las deliberaciones del EWG, se publicará un informe final, el cual será entregado

al Director Ejecutivo y a la Junta Directiva de la ICANN para servir como base de la política y las negociaciones contractuales de los nuevos gTLD, según corresponda. Tal como especificara la Junta Directiva, un Informe de cuestiones basado en el Informe final será la base de un proceso de desarrollo de políticas (PDP) de la GNSO iniciado por la Junta Directiva y con un enfoque específico.