ICANN | GNSO

Organización de Apoyo para Nombres Genéricos

Informe Final de la Fase 2 del Proceso Expeditivo de Desarrollo de Políticas sobre la Especificación Temporaria para los Datos de Registración de los gTLD

31 de julio de 2020

Estado de este documento

El presente documento constituye el Informe Final de Recomendaciones de la Fase 2 del Equipo responsable del Proceso Expeditivo de Desarrollo de Políticas (EPDP) de la GNSO de la Especificación Temporaria para los Datos de Registración de los gTLD (dominios genéricos de alto nivel), para presentarse al Consejo de la GNSO (Organización de Apoyo para Nombres Genéricos).

Preámbulo

El objetivo de este Informe Final es documentar los siguientes elementos del Equipo responsable del EPDP: (i) deliberaciones sobre las preguntas de la carta orgánica, (ii) aportes recibidos sobre el Informe Inicial de la Fase 2 del EPDP y el posterior análisis del Equipo responsable del EPDP, (iii) recomendaciones de

políticas y niveles de consenso asociados y (iv) pautas para la implementación para ser consideradas por el Consejo de la GNSO.

Índice

Este documento ha sido traducido a varios idiomas como información únicamente. El texto original y válido (en inglés) se puede obtener en: https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf

1 Resumen Ejecutivo

1.1 Información de referencia

El 17 de mayo de 2018, la Junta Directiva de la ICANN (Junta de la ICANN) adoptó la Especificación Temporaria para los Datos de Registración de Dominios Genéricos de Alto Nivel (gTLD) ("Especificación Temporaria"). La Especificación Temporaria proporciona modificaciones a los requisitos existentes en los Acuerdos de Registro y Acreditación de Registradores a fin de cumplir con el Reglamento General sobre la Protección de Datos de la Unión Europea ("GDPR").[1] De conformidad con los Estatutos de la ICANN, la Especificación Temporaria vencerá el 25 de mayo de 2019.

El 19 de julio de 2018, el Consejo de la GNSO inició un Proceso Expeditivo de Desarrollo de Políticas (EPDP) y creó la carta orgánica del equipo responsable del EPDP sobre la Especificación Temporaria para los Datos de Registración de los gTLD. De conformidad con la carta orgánica, los miembros del equipo responsable del EPDP fueron limitados expresamente. Sin embargo, todos los grupos de partes interesadas, unidades constitutivas y organizaciones de apoyo de la ICANN interesados en participar están representados en dicho equipo.

Durante la Fase 1 de su trabajo, el Equipo responsable del EPDP se encargó de determinar si la Especificación Temporaria para los Datos de Registración de los gTLD debería ser una política de consenso de la ICANN tal como está o con modificaciones. Este Informe Final corresponde a la carta orgánica del Equipo responsable de la Fase 2 del EPDP que incluye lo siguiente: (i) el análisis de un sistema para el acceso/divulgación estandarizados a los datos de registración sin carácter público, (ii) las cuestiones señaladas en el Anexo a la Especificación Temporaria para los Datos de Registración de los gTLD ("Cuestiones importantes para posterior acción de la comunidad"), y (iii) las cuestiones pendientes diferidas de la Fase 1, por ejemplo, personas jurídicas vs. personas físicas y la censura del campo que especifica la ciudad, entre otros. Para obtener más detalles, consulte aquí.

A fin de organizar su trabajo, el Equipo responsable del EPDP acordó dividir su trabajo en temas de prioridad 1 y prioridad 2. La prioridad 1 consiste en el SSAD y todas las preguntas directamente relacionadas. La prioridad 2 incluye los siguientes temas:

- Visualización de información de proveedores de servicios de privacidad/representación afiliados frente a los acreditados
- Personas jurídicas frente a personas físicas

[1] El GDPR puede consultarse en https://eur-lex.europa.eu/eli/reg/2016/679/oj; para obtener información sobre el GDPR, consulte https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/.

- Censura del campo que especifica la ciudad
- Retención de datos
- Posible objetivo de la Oficina del Jefe de Tecnologías de la ICANN
- Posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme
- Exactitud y Sistema de Informes sobre la Exactitud de WHOIS

El Equipo responsable del EPDP acordó que debía darse prioridad a la finalización de las deliberaciones sobre los temas de prioridad 1. Sin embargo, acordó que cuando fuera posible, el Equipo también se esforzaría por avanzar en los temas de prioridad 2 en paralelo.

1.2 Informe Inicial y Anexo al Informe Inicial

El 7 de Febrero de 2020, el Equipo responsable del EPDP publicó su Informe Inicial para comentario público. En el Informe Inicial se esbozaron las cuestiones básicas debatidas en relación con el Sistema Estandarizado de Acceso/Divulgación a datos de registración de gTLD sin carácter público ("SSAD") propuesto y las recomendaciones preliminares adjuntas.

El 26 de marzo de 2020, el Equipo responsable del EPDP publicó un Anexo al Informe Inicial para comentario público. El Anexo se refiere a las recomendaciones y/o conclusiones preliminares del Equipo responsable del EPDP sobre los temas de prioridad 2 enumerados anteriormente.

Tras la publicación del Informe Inicial y el Anexo al Informe Inicial, el Equipo responsable del EPDP: (i) continuó procurando pautas sobre cuestiones legales, (ii) examinó cuidadosamente los comentarios públicos recibidos en respuesta a la publicación del Informe Inicial y el Anexo, (iii) continuó con la revisión del trabajo en curso con los grupos comunitarios que los miembros del equipo representan, y (iv) continuó con las deliberaciones hacia la elaboración de este Informe Final que será analizado por el Consejo de la GNSO y, si es aprobado, será enviado a la Junta Directiva de la ICANN para su aprobación como una política de consenso de la ICANN. Las convocatorias al consenso sobre las recomendaciones contenidas en este Informe Final fueron llevadas a cabo por el Presidente del Equipo responsable del EPDP, conforme lo requerido por las Pautas para los Grupos de Trabajo de la GNSO y tal como se en el Anexo D. En resumen:

- Once (11) recomendaciones obtuvieron una designación de pleno consenso (1, 2, 3, 4, 11, 13, 15, 16, 17, 19 y 21)
- Tres (3) recomendaciones obtuvieron una designación de consenso (7, 20 y 21)
- Seis (6) recomendaciones obtuvieron un fuerte apoyo pero una designación de oposición significativa (5, 8, 9, 10, 12 y 18)

- Dos (2) recomendaciones obtuvieron una designación de divergencia (6 y 14)

Para obtener más detalles sobre estas designaciones, consulte el Anexo D y la sección 3.6 de las Pautas para los Grupos de Trabajo de la GNSO.

Recomendaciones para consideración del Consejo de la GNSO (véase el capítulo 3 para consultar el texto completo de las recomendaciones):

Recomendaciones del SSAD:

Recomendación #1.	**Acreditación**
Recomendación #2.	**Acreditación de entidades gubernamentales**
Recomendación #3.	**Criterios y contenido de las solicitudes**
Recomendación #4.	**Acuse de recibo**
Recomendación #5.	**Requisitos de respuesta**
Recomendación #6.	**Niveles de prioridad**
Recomendación #7.	**Propósitos del Solicitante**
Recomendación #8.	**Autorización de Partes Contratadas**
Recomendación #9.	**Automatización del procesamiento del SSAD**
Recomendación #10.	**Determinación de los SLA variables para los tiempos de respuesta para el SSAD**
Recomendación #11.	**Términos y condiciones del SSAD**
Recomendación #12.	**Requisito de divulgación**
Recomendación #13.	**Política de consultas**
Recomendación #14.	**Sostenibilidad financiera**
Recomendación #15.	**Registro**
Recomendación #16.	**Auditorías**
Recomendación #17.	**Requisitos de informes**

Recomendación #18. **Revisión de la implementación de las recomendaciones de políticas relativas al SSAD mediante un Comité Permanente de la GNSO**

Recomendaciones de prioridad 2:

Recomendación #19. **Visualización de información de proveedores de servicios de privacidad/representación afiliados y/o acreditados**

Recomendación #20. **Campo que especifica la ciudad**

Recomendación #21. **Retención de datos**

Recomendación #22. **Propósito 2**

Conclusiones de prioridad 2:

Conclusión 1. **Propósito de la OCTO**

Conclusión 2. **Exactitud y Sistema de Informes sobre la Exactitud de WHOIS**

Como resultado de las dependencias externas y las limitaciones de tiempo, el presente Informe Final no abordó todos los temas de prioridad 2. En concreto, no se abordan los siguientes puntos:

Personas jurídicas vs. personas físicas: aunque la cuestión fue objeto de cierta consideración en la Fase 2, no se llegó a un acuerdo sobre nuevas recomendaciones de políticas. El estudio solicitado sobre este tema se recibió demasiado tarde en el proceso para recibir la debida consideración. Por consiguiente, las recomendaciones de la Fase 1 del EPDP, los Registradores y Operadores de Registro tienen permitido diferenciar a las registraciones en base a si son personas físicas o jurídicas, aunque no están obligados a hacerlo. El Consejo de la GNSO está estudiando la posibilidad de continuar con el trabajo sobre este tema (incluida la consideración del Estudio sobre la diferenciación entre personas jurídicas y personas físicas en los Servicios de Directorio de Datos de Registración de Nombres de Dominio [RDDS] de la organización ICANN).

Posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme: El Equipo del EPDP recibió asesoramiento jurídico en el que se indicó que la publicación de direcciones de correo electrónico enmascaradas uniformes da lugar a la publicación de datos personales; lo cual indica que la publicación generalizada de direcciones de correo electrónico enmascaradas uniformes puede no ser actualmente factible en el marco del GDPR. El Consejo de la GNSO está estudiando la posibilidad de continuar con el trabajo sobre este tema.

El Equipo responsable del EPDP consultará al Consejo de la GNSO sobre cómo abordar los puntos restantes de prioridad 2.

1.3 Conclusiones y Próximos Pasos

Este Informe Final será presentado al Consejo de la GNSO para su consideración y aprobación.

1.4 Otras secciones relevantes de este informe

Para obtener una revisión completa de las cuestiones e interacciones relevantes de este Equipo responsable del EPDP, se incluyen las siguientes secciones dentro de este Informe Final:

- Información de referencia sobre las cuestiones que se están considerando.
- Documentación de quiénes participaron en las deliberaciones del Equipo responsable del EPDP, incluidos los registros de asistencia y enlaces a las Manifestaciones de Interés, según corresponda.
- Un anexo que incluye el mandato del Equipo responsable del EPDP tal como se define en la Carta orgánica adoptada por el Consejo de la GNSO.
- Documentación sobre la solicitud de aportes de la comunidad mediante canales formales de SO/AC y SG/C, incluidas las respuestas.

2 Enfoque del Equipo responsable del EPDP

Esta sección proporciona una descripción general de la metodología de trabajo y el enfoque del Equipo responsable del EPDP. Los puntos que se describen a continuación pretenden proporcionar al lector información de referencia relevante sobre las deliberaciones y procesos del Equipo responsable del EPDP y no deberían interpretarse como una representación de la totalidad de las iniciativas y deliberaciones del dicho equipo.

2.1 Metodología de trabajo

El Equipo responsable del EPDP comenzó sus deliberaciones para la fase 2 el 2 de mayo de 2019. El Equipo acordó continuar con su trabajo principalmente a través de teleconferencias programadas una o más veces por semana, además de intercambios de correo electrónico en su lista de correo. Además, el Equipo responsable del EPDP celebró cuatro reuniones presenciales: la primera serie de debates presenciales tuvo lugar en la reunión pública ICANN65 en Marrakech, Marruecos, dos reuniones presenciales específicas, la segunda y la cuarta reunión, se celebraron en la sede de la ICANN en Los Ángeles (LA) en septiembre de 2019 y enero de 2020, y el tercer debate presencial tuvo lugar en la reunión pública ICANN66 en Montreal, Canadá. Todas las reuniones del Equipo responsable del EPDP están documentadas en su espacio de trabajo wiki, que incluye su lista de correo electrónico, documentos preliminares, materiales de referencia y aportes recibidos de las Organizaciones de Apoyo y Comités Asesores de la ICANN, incluidas las unidades constitutivas y grupos de partes interesadas de la GNSO.

El Equipo responsable del EPDP también preparó un plan de trabajo, el cual fue revisado y actualizado de forma periódica. Para facilitar su labor, el Equipo responsable del EPDP utilizó una plantilla para tabular todos los aportes recibidos en respuesta a su solicitud de declaraciones de unidades constitutivas y grupos de partes interesadas (véase el Anexo D). Esta plantilla también se utilizó para registrar los aportes de otras organizaciones de apoyo y comités asesores de la ICANN y se puede encontrar en el Anexo D.

Dentro del marco de la Reunión pública ICANN66 realizada en Montreal, el Equipo responsable del EPDP celebró una sesión de la comunidad durante la cual presentó sus metodologías y hallazgos preliminares a la comunidad de la ICANN en su conjunto, para su debate y comentarios.

2.2 Mapa conceptual, hojas de trabajo y bloques de base

A fin de asegurar un entendimiento común de los temas que se abordarán como parte de sus deliberaciones de la fase 2, el Equipo responsable del EPDP delineó los temas mediante los siguientes mapas conceptuales, que permitieron reagrupar y consolidar

los temas (véase mapa conceptual). Esto constituyó la base para la elaboración posterior de las hojas de trabajo de prioridad 1 y prioridad 2 (ver hojas de trabajo) que el Equipo responsable del EPDP utilizó para capturar:

- Descripción de cuestiones / preguntas relacionadas con la carta orgánica
- Entregable previsto
- Lectura requerida
- Sesiones informativas a proporcionar
- Preguntas legales
- Dependencias
- Cronograma y enfoque propuestos

El Presidente del Equipo responsable del EPDP también presentó varias definiciones de trabajo para garantizar la coherencia de la terminología y una comprensión compartida de los términos utilizados durante las deliberaciones del Equipo responsable del EPDP (ver definiciones de trabajo).

Tras la revisión de varios casos de uso en la vida real, el Equipo responsable del EPDP estableció un conjunto de bloques de base en el cual consistiría el Sistema Estandarizado de Acceso/Divulgación ("SSAD"), reconociendo que en la decisión sobre las funciones y responsabilidades de las distintas partes interesadas que participan pueden influir tanto el asesoramiento jurídico como la orientación del Comité Europeo de Protección de Datos (“EDPB”).

2.3 Temas de prioridad 1 y prioridad 2

A fin de organizar su trabajo, el Equipo responsable del EPDP acordó dividir su trabajo en temas de prioridad 1 y prioridad 2. La prioridad 1 consiste en el SSAD y todas las preguntas directamente relacionadas. La prioridad 2 incluye los siguientes temas:

- Visualización de información de proveedores de servicios de privacidad/representación afiliados frente a los acreditados
- Personas jurídicas frente a personas físicas
- Censura del campo que especifica la ciudad
- Retención de datos
- Posible objetivo de la Oficina del Jefe de Tecnologías de la ICANN
- Posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme
- Exactitud y Sistema de Informes sobre la Exactitud de WHOIS

El Equipo responsable del EPDP acordó que debía darse prioridad a la finalización de las deliberaciones sobre los temas de prioridad 1. Sin embargo, acordó que cuando fuera posible, el Equipo también se esforzaría por avanzar en los temas de prioridad 2 en paralelo.

Como resultado de las dependencias externas y las limitaciones de tiempo, el presente Informe Final no abordó todos los temas de prioridad 2. En concreto, no se abordan los siguientes puntos:

Personas jurídicas vs. personas físicas: aunque la cuestión fue objeto de cierta consideración en la Fase 2, no se llegó a un acuerdo sobre nuevas recomendaciones de políticas. El estudio solicitado sobre este tema se recibió demasiado tarde en el proceso para recibir la debida consideración. Por consiguiente, las recomendaciones de la Fase 1 del EPDP, los Registradores y Operadores de Registro tienen permitido diferenciar a las registraciones en base a si son personas físicas o jurídicas, aunque no están obligados a hacerlo. El Consejo de la GNSO está estudiando la posibilidad de continuar con el trabajo sobre este tema (incluida la consideración del Estudio sobre la diferenciación entre personas jurídicas y personas físicas en los Servicios de Directorio de Datos de Registración de Nombres de Dominio [RDDS] de la organización ICANN).

Posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme: El Equipo del EPDP recibió asesoramiento jurídico en el que se indicó que la publicación de direcciones de correo electrónico enmascaradas uniformes da lugar a la publicación de datos personales; lo cual indica que la publicación generalizada de direcciones de correo electrónico enmascaradas uniformes puede no ser actualmente factible en el marco del GDPR. El Consejo de la GNSO está estudiando la posibilidad de continuar con el trabajo sobre este tema.

2.4 Comité jurídico

En reconocimiento de la complejidad de muchos temas que se encargaron al Equipo responsable del EPDP para que los tratara en la Fase 2, el Equipo responsable del EPDP solicitó recursos para el asesor jurídico externo de Bird & Bird. Para ayudar en la preparación de las preguntas jurídicas preliminares para Bird & Bird, los líderes del EPDP optaron por reunir un Comité jurídico, formado por miembros del Equipo responsable del EPDP con experiencia jurídica.

El Comité jurídico de la Fase 2 trabajó en conjunto para revisar las preguntas propuestas por los miembros del Equipo responsable del EPDP para asegurarse de que:

1. las preguntas fueran realmente de naturaleza jurídica, en contraposición a las preguntas de políticas o de implementación de políticas;
2. las preguntas se formularan de manera neutral, evitando tanto los resultados supuestos como el posicionamiento de la unidad constitutiva;
3. las preguntas fueran adecuadas y oportunas para el trabajo del Equipo responsable del EPDP; y
4. el presupuesto limitado para la asesoría jurídica externa se utilizara de manera responsable.

El Comité jurídico presentó todas las preguntas acordadas al Equipo responsable del EPDP para su aprobación final antes de enviar las preguntas a Bird & Bird, con la excepción de las preguntas sobre la automatización de la toma de decisiones.

A la fecha, el Equipo responsable del EPDP acordó enviar ocho preguntas relacionadas con el SSAD a Bird & Bird. El texto completo de las preguntas y los resúmenes ejecutivos del asesoramiento jurídico recibido en respuesta a las preguntas se encuentran en el Anexo F.

2.5 Preguntas de la carta orgánica

Al abordar las preguntas de la carta orgánica,[2] el Equipo responsable del EPDP consideró lo siguiente: (1) los aportes de cada grupo como parte de las deliberaciones; (2) los aportes pertinentes de la fase 1; (3) los aportes de cada grupo en respuesta a la solicitud de aportes iniciales en relación con las preguntas específicas de la carta orgánica; (4) la lectura requerida identificada para cada tema en las hojas de trabajo; (5) los aportes realizados en respuesta a los foros de comentarios públicos; y (6) los aportes realizados por los asesores jurídicos del Equipo responsable del EPDP, Bird & Bird.

[2] En el anexo A, se examina con mayor profundidad la vinculación entre cada uno de los temas tratados en las recomendaciones y las preguntas pertinentes de la carta orgánica.

3 El Equipo responsable del EPDP responde a las preguntas de la carta orgánica y ofrece recomendaciones

Tras examinar los comentarios públicos sobre el Informe Inicial y el Anexo al Informe Inicial, el Equipo responsable del EPDP presenta sus recomendaciones para la consideración del Consejo de la GNSO. El Informe Final declara el nivel de consenso logrado dentro del Equipo responsable del EPDP para las diferentes recomendaciones. En resumen:

- Once (11) recomendaciones obtuvieron una designación de pleno consenso (1, 2, 3, 4, 11, 13, 15, 16, 17, 19 y 21)
- Tres (3) recomendaciones obtuvieron una designación de consenso (7, 20 y 21)
- Seis (6) recomendaciones obtuvieron un fuerte apoyo pero una designación de oposición significativa (5, 8, 9, 10, 12 y 18)
- Dos (2) recomendaciones obtuvieron una designación de divergencia (6 y 14)

Para obtener más detalles sobre estas designaciones, consulte el Anexo D y la sección 3.6 de las Pautas para los Grupos de Trabajo de la GNSO.

Únicamente en relación con las recomendaciones relacionadas con el SSAD, el Equipo responsable del EPDP considera que son interdependientes y, por lo tanto, deben ser consideradas como un solo paquete por el Consejo de la GNSO y, posteriormente, por la Junta Directiva de la ICANN.

Nota: durante la Fase 1 del trabajo del Equipo responsable del EPDP, se le encargó a dicho equipo la revisión de la Especificación Temporaria. La Especificación Temporaria se estableció como respuesta al GDPR.[3] Por consiguiente, el GDPR es la única ley a la que se hace referencia específica en este informe. El Equipo responsable del EPDP ha deliberado sobre la posibilidad de que este Informe Final se redacte de manera agnóstica a cualquier ley específica, pero el Equipo responsable del EPDP determinó que el informe se beneficiaría de referencias explícitas para facilitar la implementación de las recomendaciones del Equipo. El GDPR es una ley regional que abarca varias jurisdicciones y, habida cuenta de los estrictos criterios que contiene, es muy probable que el cumplimiento de esta ley se ajuste a otras leyes nacionales o regionales aplicables de protección de datos. El Equipo responsable del EPDP respalda plenamente la aspiración de la ICANN de ser globalmente inclusiva, y ningún contenido

[3] "La presente Especificación Temporaria para los Datos de Registración de los gTLD ("Especificación Temporaria") establece requisitos temporarios para permitir que la ICANN y los operadores de registro y registradores de gTLD continúen cumpliendo con los requisitos contractuales de la ICANN existentes y con las políticas desarrolladas por la comunidad habida cuenta del GDPR".

de este informe anulará el principio básico de que las partes contratadas pueden y deben cumplir con las leyes y reglamentos estatutarios aplicables a nivel local.

3.1 Sistema Estandarizado de Acceso/Divulgación a datos de registración sin carácter público (SSAD)

En el Anexo A, se proporcionan más detalles en relación con el enfoque y los materiales que el Equipo responsable del EPDP revisó para abordar las cuestiones relativas a la carta orgánica y elaborar las siguientes recomendaciones.

Como parte de sus deliberaciones, el Equipo responsable del EPDP consideró un modelo centralizado, en el que tanto las solicitudes como la autorización de divulgación serían realizadas por la ICANN, o su encargado del tratamiento de datos delegado, y un modelo descentralizado, en el que tanto las solicitudes como las decisiones de divulgación serían manejadas por partes contratadas. El Equipo no pudo llegar a un acuerdo sobre ninguna de las dos opciones y en su lugar presentó un modelo híbrido en el que las solicitudes se centralizarían y las decisiones sobre la divulgación de información serían tomadas normalmente (en la implementación inicial) por las partes contratadas. El modelo híbrido del SSAD se basa en los siguientes principios básicos:

- La recepción, autenticación y transmisión de las solicitudes del SSAD a la Parte contratada debe ser un proceso totalmente automatizado en la medida en que sea técnica y comercialmente factible y legalmente permitido. Las decisiones sobre la divulgación de información serán normalmente (en la implementación inicial) tomadas por la Parte contratada y debería ser un proceso automatizado únicamente cuando sea técnica y comercialmente factible y legalmente permitido. En las áreas en las cuales la automatización no cumpla estos criterios, el objetivo de base es la estandarización del proceso de decisión sobre la divulgación. La experiencia adquirida a lo largo del tiempo con las solicitudes de divulgación de información del SSAD y las correspondientes respuestas debe servir de base para seguir perfeccionando y estandarizando las respuestas.
- En reconocimiento de la necesidad de realizar ajustes en base a la experiencia en la función del SSAD, debería existir un Comité permanente de la GNSO que supervise la implementación del SSAD y recomiende mejoras que puedan realizarse. Las mejoras recomendadas a través de este proceso no deben infringir las políticas establecidas por el EPDP, las leyes de protección de datos, los Estatutos de la ICANN o los procedimientos y directrices de la GNSO.
- Es necesario establecer acuerdos de nivel de servicio (SLA) y se debe exigir su cumplimiento, pero es posible que tengan que cambiar con el transcurso del tiempo para reconocer que habrá una curva de aprendizaje.
- Las respuestas a las solicitudes de divulgación, independientemente de que la revisión se realice de forma manual o que se active una respuesta automatizada, son devueltas por la Parte contratada pertinente directamente al

Solicitante, pero deben existir mecanismos de registro adecuados que permitan al SSAD confirmar que se cumplen los acuerdos de nivel de servicio y que las respuestas se procesan de conformidad con la política (por ejemplo, la Puerta de enlace central DEBE ser notificada cuando se rechazan o conceden las solicitudes de divulgación).

Los beneficios de este modelo son los siguientes:

Lugar único para presentar solicitudes

- Reduce el tiempo y el esfuerzo que los solicitantes dedican a localizar puntos de contacto individuales o a seguir procedimientos individuales.
- Garantiza que las solicitudes se dirijan directamente a la parte responsable en cada entidad divulgadora, eliminando así la incertidumbre de que las solicitudes no se reciban o se envíen a alguien no cualificado para procesarlas.
- Permite oportunidades claras de divulgación para socializar la ubicación y el método de solicitud de datos de registración sin carácter público.
- Se puede hacer un seguimiento de las solicitudes y respuestas para ver si se cumplen los acuerdos de nivel de servicio.

Formularios de solicitud estandarizados

- Reduce el número de solicitudes de divulgación que se deniegan por falta de información.
- Aumenta la eficiencia con la cual las entidades divulgadoras pueden revisar las solicitudes.
- Reduce la incertidumbre de los solicitantes que ahora disponen de un conjunto de datos estándar/uniformes que deben proporcionar cuando presentan solicitudes de divulgación.
- Reduce la necesidad de que las partes divulgadoras exijan un conjunto individual de datos.

Proceso de autenticación incorporado

- Acelera el proceso de revisión de las entidades divulgadoras dado que no necesitarán volver a verificar al Solicitante.
- La garantía externa de que los Solicitantes han sido verificados puede aumentar la probabilidad y/o la rapidez de la divulgación.

Proceso estandarizado de revisión y respuesta

- Permite la creación de un formato de respuesta común.
- Permite la creación de reglas, directrices y mejores prácticas que las partes divulgadoras pueden seguir al examinar y responder a las solicitudes.
- Permite la adopción de un sistema común de revisión de respuestas
- Permite la automatización de ciertas solicitudes aún por definir por parte de los Solicitantes aún por definir.

- Facilita la toma de decisiones de divulgación automatizada en algunas situaciones.
- El registro de solicitudes y respuestas también permite a la Organización de la ICANN auditar las acciones de las entidades divulgadoras e identificar cualquier caso de incumplimiento sistémico y tomar las medidas apropiadas para exigir el cumplimiento.

Funciones y responsabilidades principales del SSAD:

- Administrador de la puerta de enlace central: función desempeñada o supervisada por la Organización de la ICANN. Responsable de la gestión de la recepción y el enrutamiento de las solicitudes de SSAD que requieren una revisión manual hacia las Partes contratadas responsables. Responsable de gestionar y dirigir las solicitudes que se confirme que están automatizadas hacia las Partes contratadas para la liberación de datos, de acuerdo con los criterios establecidos y acordados en estas recomendaciones de política o sobre la base de la recomendación del Comité Permanente de la GNSO para la revisión de la implementación de las recomendaciones de políticas relativas al SSAD. Responsable de recopilar datos sobre las solicitudes, respuestas y decisiones de divulgación adoptadas.
- Autoridad de acreditación: función desempeñada o supervisada por la Organización de la ICANN. Una entidad de gestión que ha sido designada para tener la autoridad formal de "acreditar" a los usuarios del SSAD, es decir, para confirmar y verificar la identidad del usuario (constatada mediante una Credencial de identificación) y las declaraciones (o afirmaciones) asociadas a la Credencial de identificación (constatadas mediante las Declaraciones firmadas).
- Proveedor de identidad: responsable de 1) verificar la identidad de un Solicitante y gestionar una Credencial de identificación asociada al Solicitante, 2) verificar y gestionar las Declaraciones firmadas asociadas a la Credencial de identificación. A los efectos del SSAD, el Proveedor de identidad puede ser la propia Autoridad de acreditación o la Autoridad de acreditación puede recurrir a ninguno o más terceros para prestar los servicios de Proveedor de identidad.
- Partes contratadas: responsables de responder a las solicitudes de divulgación que no cumplan los criterios para una respuesta automatizada.[4]
- Comité permanente de la GNSO para la revisión de la implementación de las recomendaciones de políticas relativas al SSAD: comité representativo de la comunidad de la ICANN responsable de evaluar las cuestiones operativas del SSAD que surgen como resultado de las Políticas de consenso de la ICANN adoptadas y/o su implementación. El Comité Permanente de la GNSO tiene por

[4] De forma predeterminada, el Administrador de la puerta de enlace central enviará solicitudes de divulgación a los Registradores, pero eso no impide que el Administrador de la puerta de enlace central envíe solicitudes de divulgación a los Registradores en determinadas circunstancias (véase la recomendación 5 para obtener más detalles).

objeto examinar los datos que se producen como consecuencia de las operaciones del SSAD y proporcionar al Consejo de la GNSO recomendaciones sobre la mejor manera de realizar cambios operativos en el SSAD, que sean estrictamente medidas de implementación, además de recomendaciones basadas en la revisión de las repercusiones que las Políticas de consenso existentes tengan en las operaciones del SSAD.

Se espera que las diferentes funciones y responsabilidades se describan en detalle y se confirmen en los acuerdos aplicables.

A continuación se presenta un desglose detallado de los supuestos subyacentes y las recomendaciones de políticas que el Equipo responsable del EPDP está planteando para recibir aportes de la comunidad.

3.2 Aportes de la Junta Directiva de la ICANN y de la Organización de la ICANN

A fin de ayudar a fundamentar sus deliberaciones, el Equipo responsable del EPDP se puso en contacto con la Junta Directiva y con la Organización de la ICANN "para comprender la posición de la Junta Directiva sobre el alcance de la responsabilidad operativa y el nivel de responsabilidad (relacionado con la toma de decisiones sobre la divulgación de datos de registración sin carácter público) que está dispuesta a aceptar en nombre de la organización de la ICANN junto con cualquier requisito previo que pueda ser necesario cumplir para hacerlo".

La Organización de la ICANN ofreció su respuesta el 19 de noviembre de 2019, que señaló en parte que "la Organización de la ICANN propuso que podría operar una puerta de enlace para la transmisión de datos autorizados. Como se ha señalado anteriormente, el operador de la puerta de enlace no toma la decisión de autorizar la divulgación. En el modelo propuesto, el proveedor de la autorización decidiría si se cumplen o no los criterios para la divulgación. Si se autoriza y autentica una solicitud, el operador de la puerta de enlace solicitaría los datos a la parte contratada y divulgaría el conjunto de datos pertinente al Solicitante".[5]

La Junta Directiva de la ICANN proporcionó su respuesta el 20 de noviembre de 2019, en la cual señaló en parte que "la Junta Directiva ha abogado sistemáticamente por el desarrollo de un modelo de acceso para los datos de registración de gTLD sin carácter público. Si el trabajo del Equipo responsable de la Fase 2 del EPDP da lugar a una recomendación consensuada de que la organización de la ICANN asuma la responsabilidad de una o más funciones operativas dentro de un SSAD, la Junta Directiva adoptaría esa recomendación a menos que la Junta Directiva determinara,

[5] Tenga en cuenta que el modelo aquí descrito no es el mismo que el modelo del SSAD presentado en este informe por el Equipo responsable del EPDP.

por el voto favorable de más de dos tercios de sus miembros, que esa política no sería la más conveniente para la comunidad de la ICANN o para la propia ICANN. Habida cuenta de la defensa de la Junta Directiva para el desarrollo de un modelo de acceso, y el apoyo al diálogo de la organización de la ICANN con el EDPB sobre una propuesta de UAM, es probable que la Junta Directiva adopte una recomendación del EPDP en este sentido".

El Equipo responsable del EPDP planteó una serie de preguntas aclaratorias adicionales a la organización de la ICANN, que pueden consultarse, junto con las respuestas, en el siguiente enlace: https://community.icann.org/x/5BdIBg. Este aporte también incluyó la estimación de costos de la organización de la ICANN para un Sistema Estandarizado de Acceso/Divulgación propuesto.

El equipo responsable del EPDP consideró este aporte, los comentarios recibidos de la DPA de Bélgica y los aportes recibidos durante el período de comentarios públicos, para tomar una decisión final sobre la división de funciones y responsabilidades en el SSAD.

3.3 Supuestos subyacentes del SSAD

El Equipo responsable del EPDP utilizó los supuestos subyacentes que se describen a continuación para elaborar sus recomendaciones de políticas. Estos supuestos subyacentes no crean necesariamente nuevos requisitos para las partes contratadas; en cambio, los supuestos están diseñados para ayudar a los lectores de este Informe Final y a los encargados de la implementación de políticas en última instancia a comprender la intención y los supuestos subyacentes del Equipo responsable del EPDP al presentar el modelo del SSAD y las recomendaciones relacionadas.

- El objetivo del SSAD es proporcionar un mecanismo previsible, transparente, eficiente y responsable para el acceso/divulgación de datos de registración sin carácter público.
- El SSAD debe cumplir con el GDPR.
- El SSAD debe tener la capacidad de cumplir estos principios y recomendaciones de políticas.
- Habida cuenta de las decisiones adoptadas por el Equipo responsable del EPDP en relación con el modelo del SSAD, la hipótesis de trabajo es que la ICANN y las partes contratadas serán responsables conjuntos del tratamiento de datos. Esta designación se basa en un análisis fáctico de la política propuesta.

3.4 Convenciones empleadas en este documento

Las palabras clave "DEBE", "NO DEBE", "REQUERIDO", "DEBERÁ", "NO DEBERÁ", "DEBERÍA", "NO DEBERÍA", "RECOMENDADO", "NO RECOMENDADO", "PUEDE" y "OPCIONAL" en el presente documento deben interpretarse como se describe en los documentos BCP 148, RFC2119 y RFC8174.

Nota: teniendo en cuenta la elección del modelo por parte del Equipo responsable del EPDP y en espera del asesoramiento jurídico específico sobre la responsabilidad de las partes y la identificación en cuanto a la responsabilidad del tratamiento de los datos, en lo que refiere al modelo propuesto, el Equipo responsable del EPDP señala que ciertas afirmaciones, en las recomendaciones, pueden requerir un perfeccionamiento de lo obligatorio a lo permitido y viceversa (por ejemplo, de "deberá" a "debería", de "DEBE" a "PUEDE", etc.).

Cuando se hace referencia a las Pautas para la implementación, el Equipo responsable del EPDP considera este contexto complementario y/o información aclaratoria para ayudar a fundamentar la implementación de las recomendaciones de políticas, pero el Equipo responsable del EPDP observa que las pautas para la implementación no tienen el mismo peso y categoría que el texto de la recomendación para crear una política.

3.5 Recomendaciones del SSAD del Equipo responsable del EPDP

3.5.1. Definiciones

- **Acreditación**: acción administrativa mediante la cual la autoridad de acreditación declara que un usuario tiene derecho a utilizar el SSAD en una configuración de seguridad determinada con un conjunto prescrito de medidas de protección.
- **Autoridad de acreditación**: entidad de gestión que ha sido designada para tener la autoridad formal de "acreditar" a los usuarios del SSAD, es decir, para confirmar y verificar la identidad del usuario (constatada mediante una Credencial de identificación) y las declaraciones (o afirmaciones) asociadas a la Credencial de identificación (constatadas mediante las Declaraciones firmadas).
- **Auditor de la Autoridad de acreditación**: entidad responsable de llevar a cabo los requisitos de auditoría de la Autoridad de acreditación, como se indica en la Recomendación 16 (Auditorías). La entidad podría ser un organismo independiente o, si la Organización de la ICANN en última instancia subcontrata la función de Autoridad de acreditación a un tercero, la Organización de la ICANN PUEDE ser el Auditor de la Autoridad de acreditación.
- **Autenticación**: proceso o acción de validar la Credencial de identificación y las Declaraciones firmadas de un Solicitante.
- **Autorización**: proceso para aprobar o denegar la divulgación de datos de registración sin carácter público.
- **Administrador de la puerta de enlace central (CGM)**: función desempeñada o supervisada por la Organización de la ICANN. Responsable de la gestión de la recepción y el enrutamiento de las solicitudes de SSAD que requieren una revisión manual hacia las Partes contratadas responsables. Responsable de gestionar y dirigir las solicitudes que se confirme que están automatizadas hacia

las Partes contratadas para la liberación de datos, de acuerdo con los criterios establecidos y acordados en estas recomendaciones de política o sobre la base de la recomendación del Comité Permanente de la GNSO para la revisión de la implementación de las recomendaciones de políticas relativas al SSAD. Responsable de recopilar datos sobre las solicitudes, respuestas y decisiones de divulgación adoptadas.

- **Desacreditación de la Autoridad de acreditación**: acción administrativa mediante la cual la organización de la ICANN revoca el acuerdo con la autoridad de acreditación, si esta función se subcontrata a un tercero, tras lo cual deja de estar aprobada para operar como la Autoridad de acreditación.
- **Entidad gubernamental elegible**: una entidad gubernamental (incluido el gobierno local y las Organizaciones Internacionales Gubernamentales) que tiene el propósito de acceder a datos de registración sin carácter público para el ejercicio de una tarea de política pública dentro de su mandato.
- **Credencial de identificación:** objeto de datos que es una representación portátil de la asociación entre un identificador y la información autenticada, y que puede presentarse para su utilización en la validación de una identidad reivindicada por una entidad que intenta acceder a un sistema. Ejemplo: Nombre de usuario/contraseña, credencial de OpenID, certificado de clave pública X.509.
- **Proveedor de identidad**: responsable de 1) verificar la identidad de un Solicitante y gestionar una Credencial de identificación asociada al Solicitante, 2) verificar y gestionar las Declaraciones firmadas asociadas a la Credencial de identificación. A los efectos del SSAD, el Proveedor de identidad puede ser la propia Autoridad de acreditación o la Autoridad de acreditación puede recurrir a ninguno o más terceros para prestar los servicios de Proveedor de identidad.
- **Solicitante**: usuario acreditado que procura la divulgación de datos de registración de un nombre de dominio a través del SSAD.
- **Revocación de credenciales de usuario**: acontecimiento que se produce cuando un Proveedor de identidad declara que una credencial anteriormente válida ha pasado a ser no válida.
- **Declaración firmada**: objeto de datos que es una representación portátil de la asociación entre una Credencial de identificación y una o más declaraciones de acceso, y que puede presentarse para su uso en la validación de esas declaraciones para una entidad que intente obtener dicho acceso. Ejemplo: [credencial OAuth], certificado de atributo X.509. Las Declaraciones firmadas pueden ser específicas para el usuario (por ejemplo, para indicar la afiliación profesional o la afirmación de tratamiento lícito de datos) o específicas para la solicitud (por ejemplo, que indiquen el fundamento jurídico de la solicitud de divulgación).
- **Sistema Estandarizado de Acceso/Divulgación de datos de registración de gTLD sin carácter público (SSAD)**: el SSAD es el conjunto general de partes y elementos que componen el sistema de solicitud, validación y divulgación.

- **Validar/validación**: probar, comprobar o establecer la validez o la exactitud de un constructo. (Ejemplo: el encargado de la divulgación validará la Credencial de identificación y las Declaraciones firmadas como parte de su proceso de autorización).
- **Verificar**: probar o comprobar la veracidad o exactitud de un hecho o valor. (Ejemplo: los Proveedores de identidad verifican la identidad del Solicitante antes de expedir una Credencial de identificación).
- **Verificación**: proceso de examinar información para establecer la veracidad de un hecho o valor alegado.

3.5.2. Recomendaciones

Recommendation #1. Acreditación[6]

1.1. El Equipo responsable del EPDP recomienda el establecimiento o la selección de una Autoridad de acreditación.

1.2. El Equipo responsable del EPDP recomienda que la Autoridad de acreditación establezca una política para la acreditación de usuarios del SSAD de conformidad con las recomendaciones que se exponen a continuación.

1.3. Las siguientes recomendaciones DEBEN incluirse en la política de acreditación:

1.3.1. El SSAD debe aceptar únicamente solicitudes de acceso/divulgación de organizaciones o personas acreditadas. Sin embargo, los requisitos de acreditación DEBEN dar cabida a cualquier usuario previsto del sistema, incluida una persona u organización que presente una única solicitud. Los requisitos de acreditación para los usuarios habituales del sistema y un usuario por única vez del sistema PUEDEN diferir.

1.3.2. Tanto las personas jurídicas como las personas físicas tienen derecho a acreditación. Una persona que acceda al SSAD utilizando las credenciales de una entidad acreditada (por ejemplo, personas jurídicas) garantiza que la persona está actuando bajo la autoridad de la entidad acreditada.

1.3.3. La política de acreditación define una única Autoridad de acreditación, gestionada por la Organización de la ICANN, que es responsable de la verificación, expedición y administración continua de las Credenciales de identificación y las Declaraciones firmadas. La Autoridad de acreditación DEBE desarrollar una política de privacidad. La Autoridad de acreditación PUEDE trabajar con Proveedores de identidad externos o de terceros que podrían prestar servicios como centros de intercambio de información para verificar la identidad y la información de autorización asociadas con los que soliciten la acreditación. La responsabilidad del procesamiento de datos

[6] Tenga en cuenta que la acreditación no se refiere a la acreditación/certificación que se indica en el Artículo 42/43 del GDPR.

personales, independientemente de la parte que lleve a cabo dicho procesamiento, seguirá correspondiendo a la Autoridad de acreditación. Si la organización de la ICANN opta por subcontratar la función de Autoridad de acreditación, o cualquier parte de la misma, la organización de la ICANN seguirá siendo responsable de supervisar la parte o partes a las cuales se tercerice la función o partes de la misma. La supervisión DEBE incluir el control y el abordaje de los posibles usos indebidos de la parte o partes a las que se ha tercerizado la función o partes de la misma.

1.3.4. La decisión de autorizar la divulgación de datos de registración, en base a la validación de la Credencial de identificación, las Declaraciones firmadas y los datos requeridos en la recomendación relativa a los criterios y el contenido de las solicitudes (Recomendación 3), corresponderá al Registrador, Registro o Administrador de la puerta de enlace central, según corresponda.

1.4. Requisitos de la Autoridad de acreditación

1.4.1. Verificar la identidad del Solicitante: la Autoridad de acreditación DEBE verificar la identidad del Solicitante, lo cual tiene como resultado una Credencial de identificación.

1.4.2. Gestión de las Declaraciones firmadas: la Autoridad de acreditación PUEDE verificar y gestionar un conjunto de declaraciones/afirmaciones dinámicas asociadas y vinculadas a la Credencial de identificación del Solicitante. Esta verificación, que puede ser realizada por un Proveedor de identidad, tiene como resultado una Declaración firmada. Las Declaraciones firmadas[7] transmiten información como:

- Declaración del propósito (o propósitos) de la solicitud
- Declaración del fundamento jurídico de la solicitud
- Declaración de que el usuario identificado por la Credencial de identificación está afiliado a la organización pertinente
- Declaración sobre el cumplimiento de las leyes (por ejemplo, almacenamiento, protección y retención/eliminación de datos)
- Declaración sobre el acuerdo de utilizar los datos divulgados para los fines legítimos y lícitos declarados

[7] Para mayor claridad, las Declaraciones firmadas son dinámicas y pueden cambiar en función de la solicitud (propósito, fundamento jurídico, tipo, urgencia, etc.) en comparación con una Credencial de identificación, que es estática y normalmente no cambia. Las Declaraciones firmadas solo se utilizan para asociar/enlazar atributos a una identidad. Estos atributos son dinámicos según la solicitud, pero pueden ser examinados y gestionados con anticipación como parte del proceso de acreditación, según sea necesario. La Autoridad de acreditación puede establecer de forma anticipada varias declaraciones para una Credencial de identificación específica o crearlas dinámicamente en función de cada solicitud. La forma de determinar esto es algo que se seguirá trabajando en la fase de implementación. La Autoridad de acreditación puede almacenar múltiples Declaraciones firmadas por cada Credencial de identificación, pero el Solicitante debe invocar las declaraciones pertinentes en cada solicitud.

- Declaración sobre el cumplimiento de medidas de protección y/o condiciones de servicio y sobre estar sujeto a revocación si se descubre que está en infracción
- Declaraciones sobre la prevención de usos indebidos, requisitos de auditoría, resolución de disputas y proceso de reclamos, etc.
- Declaraciones específicas del Solicitante, por ejemplo: propiedad/registro de marcas comerciales
- Declaraciones de poder notarial, cuando/según corresponda.

1.4.3. DEBE validar las Credenciales de identificación y las Declaraciones firmadas, además de la información contenida en la solicitud, para facilitar la decisión de aceptar o rechazar la autorización de una solicitud del SSAD. Para evitar dudas, la presencia de estas credenciales por sí solas NO DEBE dar lugar ni obligar a una autorización automática de acceso / divulgación. Sin embargo, la capacidad de automatizar la toma de decisiones de autorización de acceso/divulgación es posible en ciertas circunstancias, siempre que sean lícitas.

1.4.4. La Autoridad de acreditación DEBE definir un "código de conducta"[8] básico que establezca un conjunto de reglas que contribuyan a la correcta aplicación de las leyes de protección de datos, como el GDPR, entre las cuales se incluye:

- Una declaración explicativa clara y concisa.
- Un alcance definido que determine las operaciones de procesamiento cubiertas (el enfoque para el SSAD sería la operación de Divulgación).
- Mecanismo que permita supervisar el cumplimiento de las disposiciones.
- Identificación de un Auditor de la Autoridad de acreditación (también conocido como órgano de supervisión) y definición de los mecanismos que permitan a ese órgano desempeñar sus funciones.
- Descripción de la medida en que se ha llevado a cabo una "consulta" con las partes interesadas.

1.4.5. La Autoridad de acreditación DEBE elaborar una política de privacidad para el procesamiento de datos personales que realice, así como las condiciones de servicio para sus usuarios acreditados (como se indica en la recomendación 11).

1.4.6. Desarrollar un procedimiento básico de solicitud: la Autoridad de acreditación DEBE elaborar un procedimiento de solicitud básico y uniforme y los requisitos correspondientes para todos los Proveedores de identidad (según corresponda) y todos los solicitantes que requieran acreditación, entre ellos:

i. Cronología de la acreditación

[8] Para evitar dudas, el código de conducta al que aquí se hace referencia no tiene intención de referirse al Código de Conducta descrito en el GDPR. El código de conducta al que aquí se hace referencia se refiere a un conjunto de reglas y normas que debe seguir la Autoridad de acreditación.

ii. Definición de los requisitos de elegibilidad para los usuarios acreditados
iii. Validación de identidad, procedimientos
iv. Políticas de gestión de Credencial de identificación: vigencia/vencimiento, frecuencia de renovación, propiedades de seguridad (políticas/fuerza de contraseñas o claves), etc.
v. Procedimientos de revocación de Credenciales de identificación: circunstancias de la revocación, mecanismo o mecanismos de revocación, etc. (véase también la sección "Revocación del usuario acreditado y uso indebido", a continuación)
vi. Gestión de Declaraciones firmadas: vigencia/vencimiento, frecuencia de renovación, etc.
vii. NOTA: es posible que sean necesarios requisitos adicionales a los requisitos básicos, indicados anteriormente, para ciertas clases de Solicitantes.

1.4.7. Definir el proceso de resolución de disputas y reclamos: la Autoridad de acreditación DEBE definir un proceso de resolución de disputas y reclamos para impugnar las medidas adoptadas por la Autoridad de acreditación. El proceso definido DEBE incluir controles y mecanismos correctivos del debido proceso.

1.4.8. Auditorías: la Autoridad de acreditación DEBE ser auditada por un auditor de forma periódica. Si se descubre que la Autoridad de acreditación ha incumplido la política y los requisitos de acreditación, se le dará la oportunidad de subsanar el incumplimiento, pero en los casos de incumplimientos reiterados, se deberá identificar o crear una nueva Autoridad de acreditación. Asimismo, las entidades acreditadas DEBEN ser auditadas periódicamente para comprobar el cumplimiento de la política y los requisitos de acreditación; (Nota: la información detallada sobre los requisitos de auditoría para la Autoridad de acreditación y para los Proveedores de identidad que pueda utilizar se encuentra en la recomendación 16 de Auditoría).

1.4.9. Grupos de usuarios: la Autoridad de acreditación PODRÁ desarrollar grupos/categorías de usuarios para facilitar el proceso de acreditación, dado que todos los Solicitantes deberán estar acreditados y la acreditación incluirá la verificación de la identidad.

1.4.10. Presentación de Informes: la Autoridad de acreditación DEBE informar públicamente y de forma periódica sobre la cantidad de solicitudes de acreditación recibidas, solicitudes de acreditación aprobadas/renovadas, acreditaciones denegadas, acreditaciones revocadas, reclamos recibidos e información sobre los proveedores de identidad con los que trabaja. Véase también la recomendación 17 sobre la presentación de informes.

1.4.11. Renovación: La Autoridad de acreditación DEBE establecer un cronograma y requisitos para la renovación de la acreditación.

1.4.12. Confirmación de los datos del usuario: la Autoridad de acreditación DEBE enviar recordatorios periódicos (por ejemplo, anuales) a los

usuarios acreditados para confirmar los datos de los usuarios y recordarles que deben mantener actualizada la información necesaria para la acreditación. Los cambios en esta información requerida PODRÍAN dar lugar a la necesidad de volver a acreditarse.

1.5. Revocación de usuarios acreditados

1.5.1. Revocación, en el contexto del SSAD, significa que la Autoridad de acreditación puede revocar la condición de usuario acreditado como usuario acreditado del SSAD.[9] Una lista no exhaustiva de ejemplos en los que puede aplicarse la revocación incluye: 1) la infracción por parte del usuario acreditado de cualquier medida de protección o condición de servicio aplicable, 2) un cambio en la afiliación del usuario acreditado, 3) la infracción de los requisitos de retención / destrucción de datos o 4) cuando ya no existan requisitos previos para la acreditación.

1.5.2. La Autoridad de acreditación DEBE disponer de un mecanismo de apelación que permita a un usuario acreditado impugnar la decisión de revocar la condición de usuario acreditado dentro de un plazo definido que será decidido por la Autoridad de acreditación. Sin embargo, mientras dure la apelación, la condición de usuario acreditado permanecerá suspendida. Los resultados de una apelación DEBEN informarse de manera transparente.

1.5.3. El SSAD debe proporcionar un mecanismo para informar sobre la infracción de cualquier medida de protección o condición de servicio por parte de un usuario acreditado.[10] Los informes DEBEN transmitirse a la Autoridad de acreditación para su gestión. La Autoridad de acreditación PUEDE también obtener información de otras partes para determinar que se ha producido un uso indebido.

1.5.4. La política de revocación para personas/entidades DEBERÍA incluir penalizaciones graduales; las penalizaciones se describirán con mayor detalle durante la implementación, teniendo en cuenta cómo se aplican las penalizaciones graduales en otras áreas de la ICANN. En otras palabras, no todas las infracciones del sistema darán lugar a la revocación; sin embargo, la revocación PUEDE ocurrir si la Autoridad de acreditación determina que la persona o entidad acreditada ha incumplido sustancialmente las condiciones de su acreditación y no ha subsanado su incumplimiento en base a: i) un reclamo recibido que haya verificado un tercero; ii) los resultados de una auditoría o investigación por parte de la Autoridad de acreditación o del auditor; iii) cualquier uso indebido o abuso de los privilegios concedidos; iv) infracciones

[9] Para mayor claridad, una entidad jurídica no se desacreditará automáticamente por la acción única de un usuario individual cuya acreditación esté vinculada a la de la entidad jurídica, pero la entidad podrá ser considerada responsable de las acciones del usuario individual cuya acreditación esté vinculada a la de la entidad jurídica.
[10] Nota: el uso indebido del SSAD por parte de un usuario acreditado se aborda en la recomendación 13.

reiteradas de la política de acreditación; v) los resultados de una auditoría o investigación por parte de una DPA.

1.5.5. En el caso de que haya un patrón o práctica de comportamiento abusivo en un individuo/entidad, la credencial del individuo/entidad PODRÁ ser suspendida o revocada como parte de una sanción gradual.

1.5.6. La revocación DEBE impedir la reacreditación en el futuro, en ausencia de circunstancias especiales presentadas a satisfacción de la Autoridad de acreditación.

1.5.7. Para evitar dudas, la desacreditación no impide que las personas o entidades presenten futuras solicitudes en virtud del método de acceso previsto en la Recomendación 18 (Solicitudes razonables de divulgación lícita) del informe de la Fase 1 del EPDP.

1.6. Desautorización de Proveedores de identidad

1.6.1. Desautorización de Proveedores de identidad: los procedimientos de validación de Proveedores de identidad DEBERÍAN incluir sanciones graduales. En otras palabras, no todas las infracciones de la política darán lugar a la desautorización; sin embargo, la desautorización puede producirse si se ha determinado que el Proveedor de identidad ha incumplido sustancialmente las condiciones de su contrato y no ha subsanado la situación en base a: i) un reclamo recibido de un tercero; ii) los resultados de una auditoría o investigación por parte de la Autoridad de acreditación o del auditor; iii) cualquier uso indebido o abuso de los privilegios concedidos; iv) infracciones reiteradas de la política de acreditación. En función de la naturaleza y las circunstancias que conduzcan a la desautorización de un Proveedor de identidad, algunas o todas sus credenciales pendientes pueden ser revocadas o transferidas a un Proveedor de identidad diferente.

1.6.2. La Autoridad de acreditación DEBE disponer de un mecanismo de apelación que permita al Proveedor de identidad impugnar la decisión de desautorización. Sin embargo, mientras dure la apelación, la condición de Proveedor de identidad permanecerá suspendida. Los resultados de una apelación DEBEN informarse de manera transparente.

1.7. Consideraciones adicionales para entidades o personas acreditadas:

1.7.1. DEBEN estar de acuerdo y aceptar lo siguiente:

1.7.1.1. utilizar los datos divulgados únicamente para los fines legítimos y lícitos declarados;

1.7.1.2. las condiciones de servicio, en las cuales se describen los usos lícitos de los datos:

1.7.1.3. prevenir el uso indebido de los datos recibidos;

1.7.1.4. cooperar con cualquier auditoría o solicitud de información que forme parte de una auditoría;
1.7.1.5. estar sujetos a la desacreditación si se descubre que hacen un uso indebido de los datos o de la política / requisitos de acreditación;
1.7.1.6. almacenar, proteger y eliminar los datos de registración de gTLD de acuerdo con la ley aplicable;

1.7.2. retener únicamente los datos de registración de gTLD durante el tiempo necesario para lograr el propósito declarado en la solicitud de divulgación.

1.7.3. NO DEBE restringirse la cantidad de solicitudes de DSSA que pueden presentarse durante un período de tiempo determinado, salvo cuando la entidad acreditada represente una amenaza demostrable para el SSAD, o cuando pueda restringirse de otro modo en virtud de las presentes recomendaciones (como en el caso de la recomendación 1.5(d) y 13(b)). Se entiende que pueden aplicarse posibles limitaciones en la capacidad y velocidad de respuesta del SSAD.

1.7.4. DEBE mantener actualizada la información requerida para la acreditación y verificación e informar sin demora a la Autoridad de acreditación cuando haya cambios en esta información. Cualquier cambio PODRÁ dar lugar a la reacreditación o la reverificación de ciertas partes de la información proporcionada.

Pautas para la implementación

1.8. En relación con la acreditación, el Equipo responsable del EPDP proporciona las siguientes pautas para la implementación, con la salvedad de que se elaborarán más detalles en la fase de implementación:

1.8.1. Organizaciones reconocidas, aplicables y consolidadas podrían apoyar a la Autoridad de acreditación como Proveedor de identidad. Una investigación adecuada DEBE llevarse a cabo, como se describe en el apartado 1.3(f) anterior, si cualquiera de dichas organizaciones de buena reputación y consolidadas colaborará con la Autoridad de acreditación.

1.8.2. Entre los ejemplos de información adicional que la Autoridad de acreditación o el Proveedor de identidad PUEDE exigir al solicitante de la acreditación, se podrían incluir:

- un número de registro comercial y el nombre de la autoridad que lo haya expedido (si la entidad que solicita la acreditación es una persona jurídica);
- información que constate la propiedad de la marca comercial.[11]

[11] Para mayor claridad, los proveedores de servicios y/o los abogados que actúen en representación de los propietarios de las marcas comerciales también pueden ser elegibles para la acreditación. Sin embargo, esos proveedores de servicios y/o abogados actúan en representación (legalmente) del propietario de la marca comercial. Cuando dichos proveedores de servicios y/o abogados incumplan las reglas del SSAD, es necesario que las

1.9. Auditoría / registro por parte de la Autoridad de acreditación y los Proveedores de identidad

1.9.1. La actividad de acreditación/verificación (como la solicitud de acreditación, la información en base a la cual se tomó la decisión de acreditar o verificar la identidad) será registrada por la Autoridad de acreditación y los Proveedores de identidad.

1.9.2. Los datos registrados SERÁN únicamente divulgados, o puestos a disposición para su revisión, por la Autoridad de acreditación o el Proveedor de identidad, cuando la divulgación se considere necesaria para: a) cumplir o ejecutar una obligación legal aplicable de la Autoridad de acreditación o el Proveedor de identidad; b) llevar a cabo una auditoría en virtud de esta política o; c) apoyar el funcionamiento razonable del SSAD y la política de acreditación.

Véase también las recomendaciones sobre auditoría y registro para obtener más información.

1.10. Verificación. La organización de la ICANN debería utilizar su experiencia en otras áreas en las que la verificación está involucrada, como la acreditación de registradores, para presentar una propuesta de verificación de la identidad del Solicitante durante la fase de implementación.

1.11. Períodos de reacreditación. Como práctica recomendada, se puede considerar el período de reacreditación y los requisitos para los Registradores, que es de cinco años en la actualidad. Para evitar dudas, nada prohíbe a la Autoridad de acreditación exigir documentación adicional al renovar la acreditación.

1.12. Se prevé que la entidad acreditada elabore políticas y procedimientos adecuados para garantizar el uso apropiado de sus credenciales por parte de una persona. Cada usuario debe estar acreditado, pero un usuario que actúe en representación de una organización debe tener su acreditación vinculada a la de su organización.

Recommendation #2. Acreditación de entidades gubernamentales

2.1. Objetivo de la acreditación

entidades encargadas de la divulgación reciban dichos datos, y debe quedar claro que dicho incumplimiento puede considerarse en las futuras divulgaciones para el propietario de la marca comercial en cuya representación actúe el agente. El uso de diferentes agentes externos no puede utilizarse como medio para evitar sanciones pasadas por uso indebido del SSAD.

El SSAD DEBE proporcionar un acceso razonable a los datos de registración para las entidades que requieran acceso a estos datos para el ejercicio de sus tareas de políticas públicas. Habida cuenta de sus obligaciones en virtud de las normas de protección de datos aplicables, la responsabilidad final de la concesión de acceso a los datos de registración sin carácter público seguirá recayendo en la parte que se considere responsable del tratamiento de esos datos de registración que constituyen datos personales.

La elaboración e implementación de un procedimiento de acreditación que se aplique específicamente a las entidades gubernamentales facilitará las decisiones que las Partes contratadas tendrán que adoptar antes de conceder acceso a los datos de registración sin carácter público a una entidad determinada o el procesamiento automatizado de las decisiones de divulgación por parte del Administrador de la puerta de enlace central, según corresponda. Este procedimiento de acreditación puede proporcionar a los responsables del tratamiento de datos la información necesaria para que puedan evaluar y decidir sobre la divulgación de los datos.

2.2. Elegibilidad

La acreditación por parte del organismo gubernamental de un país/territorio o su organismo autorizado[12] estaría disponible para diversas entidades[13] gubernamentales elegibles que requieran acceso a datos de registración sin carácter público para el ejercicio de sus tareas en materia de políticas públicas, entre otras:

- Autoridades de aplicación del derecho civil y penal
- Autoridades reguladoras y de protección de datos
- Autoridades judiciales
- Organizaciones de derechos del consumidor a las que se les haya asignado una tarea de política pública por ley o por delegación de una entidad gubernamental
- Autoridades de ciberseguridad a las que se les haya asignado una tarea de política pública por ley o por delegación de una entidad gubernamental, incluidos los Equipo de Respuesta ante Emergencias Informáticas (CERT) a nivel nacional

2.3. Determinar la elegibilidad

Las entidades gubernamentales elegibles son las que exigen acceso a datos de registración sin carácter público para el ejercicio de sus tareas en materia de políticas públicas, en cumplimiento de las leyes de protección de datos aplicables. Una Autoridad de acreditación designada por el país/territorio es la encargada de

[12] Consideración de la implementación: dicho organismo podría ser una Organización Internacional Gubernamental.
[13] Las Organizaciones intergubernamentales (OIG) también pueden ser elegibles para la acreditación en virtud de la recomendación 2. Una OIG que desee ser acreditada DEBE procurar la acreditación a través de la Autoridad de acreditación de su país anfitrión.

determinar si una entidad debería ser elegible. Esta determinación de elegibilidad no afecta a la responsabilidad final de la Parte contratada de determinar si debe o no divulgar datos personales tras una solicitud de datos de registración sin carácter público o por el Administrador de la puerta de enlace central en el caso de solicitudes que cumplan los criterios para el procesamiento automatizado de las decisiones de divulgación, según corresponda.

2.4. Requisitos de la Autoridad de acreditación gubernamental

Los requisitos de acreditación gubernamental DEBEN seguir los requisitos establecidos en la Rec. 1.3.

Además, los requisitos DEBEN enumerarse y ponerse a disposición de las entidades gubernamentales elegibles. El incumplimiento de estos requisitos puede dar lugar a la desacreditación de la Autoridad de acreditación por parte de la Organización de la ICANN.

2.5. Procedimiento de acreditación

La acreditación DEBE ser proporcionada por una autoridad de acreditación aprobada. Esta autoridad
puede ser un organismo gubernamental de un país/territorio (por ejemplo, un Ministerio) o puede delegarse en una organización intergubernamental. Esta autoridad DEBERÍA publicar los requisitos para la acreditación y llevar a cabo el procedimiento de acreditación para las entidades gubernamentales elegibles.

2.5.1. La acreditación hace hincapié en las responsabilidades del Solicitante (receptor) de los datos, que es el responsable de cumplir con la ley.
2.5.2. La acreditación se centrará en los requisitos que exige la ley, como los relativos a la duración de la retención de datos, el almacenamiento seguro, los controles de datos de la organización y las notificaciones de incumplimiento.
2.5.3. La renovación, el registro, la auditoría, los reclamos y la desacreditación se tratarán de acuerdo con la Rec. 1.

Pautas para la implementación:

2.6. La acreditación es necesaria para que una entidad gubernamental participe en el SSAD. Las entidades gubernamentales no acreditadas pueden presentar solicitudes de datos al margen del SSAD y las Partes contratadas deberían disponer de procedimientos para proporcionar un acceso razonable.
2.7. Los usuarios acreditados deberán seguir las medidas de protección establecidas en la política (véase también la recomendación 11, Términos y

condiciones del SSAD). Ello se entiende sin perjuicio de que la entidad respete las medidas de protección previstas en virtud de la legislación nacional.

2.8. Las entidades acreditadas DEBERÍAN proporcionar detalles para ayudar a las Partes contratadas a tomar la decisión de divulgar la información, como por ejemplo cualquier ley local aplicable en relación con la solicitud.

Recommendation #3. Criterios y contenido de las solicitudes

3.1. El objetivo de esta recomendación es permitir la presentación estandarizada de los elementos de datos solicitados, incluida toda la documentación de respaldo.

3.2. El Equipo responsable del EPDP recomienda que cada solicitud del SSAD DEBE incluir toda la información necesaria para una decisión de divulgación, incluida la siguiente información:

3.2.1. Nombre de dominio correspondiente a la solicitud de acceso/divulgación.

3.2.2. Identificación e información sobre el Solicitante, incluida la información sobre la identidad y la Declaración firmada, como se define en la Recomendación 1, Sección 1.4a) y Sección 1.4b).[14]

3.2.3. Información sobre los derechos legales del Solicitante específicos para la solicitud y el interés legítimo u otra base legal y/o justificación para la solicitud (por ejemplo, ¿cuál es el interés legítimo u otra base legal?; ¿por qué es necesario que el Solicitante de pida estos datos?).

3.2.4. Afirmación de que la solicitud se realiza de buena fe y que los datos recibidos (si los hay) se procesarán lícitamente y únicamente de acuerdo con el propósito especificado en el apartado (c);

3.2.5. Una lista de los elementos de datos que requiere el Solicitante, y por qué los elementos de datos solicitados son necesarios para el propósito de la solicitud.

3.2.6. Tipo de solicitud (por ejemplo, Urgente – ver también la recomendación 6: Niveles de Prioridad, Confidencial – ver también la recomendación 12: Requisitos de Divulgación).

3.3. El Administrador de la puerta de enlace central[15] DEBE confirmar que se proporciona toda la información requerida. Si el Administrador de la puerta de enlace central detecta que la solicitud está incompleta, dicho Administrador DEBE notificar al Solicitante que la solicitud está incompleta, detallar qué datos requeridos faltan y dar la oportunidad al Solicitante de completar su solicitud. No debe ser posible que un Solicitante presente una solicitud incompleta.

[14] Todas las partes que participan en el SSAD deberán tener en cuenta los requisitos que pueden aplicarse a las transferencias transfronterizas de datos.

[15] Véase la definición en la sección 3.5.1 – Definiciones.

Pautas para la implementación

El Equipo responsable del EPDP prevé lo siguiente:

3.4. Cada solicitud debe incluir los datos asociados a la información detallada en la sección 3.2 anterior. Si bien en esta política no se especifica el mecanismo para recopilar y colocar estos datos en una solicitud (ya sea un formulario web, una API o similar), debería considerarse la posibilidad de ofrecer campos, casillas de verificación y opciones desplegables preestablecidas. Sin embargo, el uso de campos, casillas de verificación u opciones desplegables preestablecidas no debe excluir la posibilidad de que los Solicitantes presenten respuestas de forma libre.

3.5. Las solicitudes deben estar en inglés, a menos que la Parte contratada que reciba la solicitud indique que también está dispuesta a recibir la solicitud y/o los documentos de respaldo en otro idioma (o idiomas).

3.6. Una declaración firmada puede prever uno o más de los requisitos que se indican anteriormente.

Recommendation #4. Acuse de recibo y remisión de la solicitud de divulgación

4.1. Acuse de recibo

4.1.1. Tras la confirmación de que la solicitud es sintácticamente correcta y de que se han completado todos los campos obligatorios, el Administrador de la puerta de enlace central DEBE responder inmediatamente y de forma sincronizada con el acuse de recibo y remitir la solicitud[16] de divulgación a la Parte contratada responsable.
4.1.2. La respuesta proporcionada por el Administrador de la puerta de enlace central al Solicitante DEBERÍA incluir también información sobre los pasos subsiguientes, información sobre cómo se pueden obtener los datos de registración públicos, así como el plazo previsto en consonancia con los acuerdos de nivel de servicio descritos en la recomendación 10.

4.2. Remisión de la solicitud de divulgación

4.2.1. De forma predeterminada, el Administrador de la puerta de enlace central DEBE remitir la solicitud de divulgación al Registrador de registro. Sin embargo, si el Administrador de la puerta de enlace central toma conocimiento de cualquier circunstancia, evaluada de acuerdo con estas recomendaciones, que requiera la presentación de una solicitud de divulgación al Operador de Registro

pertinente, el Administrador de la puerta de enlace central PUEDE remitir la solicitud de divulgación al Operador de Registro correspondiente, siempre y cuando los motivos que hacen necesaria dicha transferencia de una solicitud sean proporcionados al operador de registro para su consideración El Solicitante DEBE ser capaz de señalar dicha circunstancia al Administrador de la puerta de enlace central, pero el Administrador de la puerta de enlace central DEBE realizar su propia evaluación de si la circunstancia identificada requiere la presentación de la solicitud de divulgación al Operador de Registro correspondiente. Para mayor claridad, nada en esta recomendación impide que un Solicitante se ponga en contacto directamente, fuera del SSAD, con el Operador de Registro correspondiente con una solicitud de divulgación.

Pautas para la implementación

El Equipo responsable del EPDP prevé lo siguiente:

4.3. En el acuse de recibo se incluirá un "número de ticket" o un mecanismo similar para facilitar las interacciones entre el Solicitante y el SSAD, los detalles se elaborarán en la etapa de implementación.
4.4. El Administrador de la puerta de enlace central remite a la a la Parte contratada la solicitud de divulgación así como la información necesaria y apropiada sobre el Solicitante. Si se trata de una solicitud de divulgación a la que se aplica el procesamiento automatizado de la decisión de divulgación (véase la recomendación sobre Automatización), la remisión de la solicitud de divulgación y de toda la información pertinente puede tener lugar al mismo tiempo que el Administrador de la puerta de enlace central indique a la Parte contratada que divulgue automáticamente los datos solicitados al Solicitante.

Recommendation #5. Requisitos de respuesta

5.1. Para el Administrador de la puerta de enlace central:[17]
5.1.1. Como parte de su remisión a la Parte contratada responsable, el Administrador de la puerta de enlace central PUEDE proporcionar una recomendación a la Parte contratada sobre si debe divulgar la información o no.

5.2. Para las Partes contratadas:
5.2.1. La Parte contratada PUEDE seguir la recomendación del Administrador de la puerta de enlace central, pero no está obligada a hacerlo. Si la Parte contratada decide no seguir la recomendación del Administrador de la puerta de enlace central, la Parte contratada DEBE comunicar sus motivos

[17] Tenga en cuenta que los requisitos de las solicitudes de divulgación que cumplen los criterios para las decisiones de divulgación automatizadas se abordan en la recomendación 9.

para no seguir la recomendación del Administrador de la puerta de enlace central para que dicho Administrador pueda obtener información y mejorar las futuras recomendaciones de respuesta.

5.2.2. DEBE proporcionar una respuesta de divulgación sin demoras indebidas, a menos que haya circunstancias excepcionales. Esas circunstancias excepcionales PUEDEN incluir la cantidad total de solicitudes recibidas si dicha cantidad supera con creces los acuerdos de nivel de servicio establecidos.[18] Las solicitudes del SSAD que cumplan los criterios de respuesta automática deben recibir una respuesta de divulgación automática. En el caso de las solicitudes que no cumplan los criterios de respuesta automática, DEBERÁ recibirse una respuesta conforme a los acuerdos de nivel de servicio descritos en la recomendación sobre Acuerdos de nivel de servicio.

5.2.3. Las respuestas en las cuales la divulgación de datos (en forma total o parcial) haya sido denegada, DEBEN incluir una justificación suficiente para que el Solicitante entienda objetivamente los motivos de la decisión, incluido, por ejemplo, un análisis y una explicación de cómo se aplicó la prueba de equilibrio[19] (si corresponde). Además, en su respuesta, la Parte contratada PODRÁ incluir información sobre la forma en que se pueden obtener los datos públicos de registración.

5.2.4. Si la Parte contratada determina que la divulgación de información infringiría las leyes aplicables o resultaría en una incongruencia con estas recomendaciones de políticas, la Parte contratada DEBE documentar la justificación y comunicar esta información al Solicitante y, si se solicita, a la Organización de la ICANN.

5.3. Si un Solicitante considera que su solicitud fue denegada en contravención de los requisitos de procedimiento de esta política, puede presentar un reclamo ante la Organización de la ICANN. La organización de la ICANN DEBE investigar los reclamos relativos a las solicitudes de divulgación en el marco de sus procesos de cumplimiento efectivo.

5.4. La organización de la ICANN DEBE poner a disposición un mecanismo de alerta mediante el cual tanto los Solicitantes como los titulares de los datos que hayan sido divulgados puedan alertar a la organización de la ICANN si consideran que la divulgación o no divulgación es el resultado de un uso indebido sistémico de una parte contratada. Este mecanismo de alerta no es un mecanismo de apelación (para impugnar la divulgación o la no divulgación se prevé que las partes afectadas utilicen los mecanismos de resolución de disputas disponibles, como los tribunales o las autoridades de protección de datos) pero debería ayudar a informar al departamento de Cumplimiento de la ICANN sobre las denuncias de incumplimiento sistémico de los

[18] Véase la recomendación 12 para obtener más detalles sobre lo que se considera uso indebido del SSAD.

[19] Según la recomendación 6, se debe tener cuidado de asegurar que no se revele ningún dato personal al Solicitante dentro de esta explicación.

requisitos de esta política, lo que debería desencadenar una acción adecuada de cumplimiento efectivo.

Pautas para la implementación

5.5. También se espera que la información obtenida del mecanismo de alerta se incluya en el Informe de estado de implementación del SSAD (véase la recomendación 18) para permitir un examen más a fondo de las posibles soluciones para hacer frente a los comportamientos abusivos.

5.6. No es la expectativa del Equipo responsable del EPDP que el Administrador de la puerta de enlace central proporcione una recomendación desde el primer día, dado que se entiende que será necesario adquirir experiencia antes de que el Administrador de la puerta de enlace central pueda estar en condiciones de proporcionar dicha recomendación a la Parte contratada. Se espera que la recomendación se elabore de manera automatizada teniendo en cuenta la información contenida en la solicitud, la información sobre el Solicitante y el historial de solicitudes del Solicitante.

Recommendation #6. Niveles de prioridad

6.1. El Equipo responsable del EPDP recomienda que el Administrador de la puerta de enlace central facilite al menos los siguientes tres (3) niveles de prioridad, entre los cuales un Solicitante pueda elegir al presentar solicitudes a través del SSAD. El nivel de prioridad define la urgencia con que la Parte contratada debería actuar en la Solicitud de divulgación:

6.1.1. **Prioridad 1** - Solicitudes urgentes - Los criterios para determinar las solicitudes urgentes se limitan a las circunstancias que plantean una amenaza inminente para la vida, lesiones físicas graves, infraestructura crítica (dentro y fuera de Internet) o explotación infantil. A los efectos de evitar dudas, la Prioridad 1 no se limita a las solicitudes de los organismos de cumplimiento de la ley.

6.1.2. **Prioridad 2** - Procedimientos administrativos de la ICANN: solicitudes de divulgación que sean el resultado de procedimientos administrativos en virtud de los requisitos contractuales de la ICANN o de las Políticas de consenso existentes, como las solicitudes de verificación de la UDRP y el URS.[20]

6.1.3. **Prioridad 3** - Todas las demás solicitudes.

6.2. En el caso de las solicitudes de Prioridad 3, los Solicitantes DEBEN tener la capacidad de indicar que la solicitud de divulgación refiere a una cuestión de

[20] Para mayor claridad, se prevé que esta asignación de prioridades se limite a los proveedores de servicios de resolución de disputas aprobados por la ICANN o a sus empleados en el contexto de los procedimientos administrativos de la ICANN.

protección del consumidor (phishing, malware o fraude), en cuyo caso la Parte contratada DEBERÍA dar prioridad a la solicitud sobre otras solicitudes de Prioridad 3. El uso indebido persistente de esta indicación puede dar lugar a la desacreditación del Solicitante.

6.3. La Parte Contratada:

- PUEDE reasignar el nivel de prioridad durante la revisión de la solicitud. Por ejemplo, como una solicitud se revisa manualmente, la Parte contratada PUEDE observar que aunque la prioridad se establece como Prioridad 2 (Procedimiento administrativo de la ICANN), la solicitud no muestra ninguna prueba que documente un Procedimiento administrativo de la ICANN como un caso de la UDRP presentado y, por consiguiente, la solicitud debería reclasificarse como Prioridad 3.
- DEBE comunicar cualquier reclasificación al Administrador de la puerta de enlace central y al Solicitante.

6.4. El Equipo responsable del EPDP recomienda que el SSAD DEBE respaldar las solicitudes de divulgación del SSAD "urgentes" a las que se aplican los siguientes requisitos:

6.4.1. Uso indebido de las solicitudes urgentes: las infracciones del uso de las Solicitudes Urgentes del SSAD darán lugar a una respuesta del Administrador de la puerta de enlace central para garantizar que los requisitos de las Solicitudes Urgentes del SSAD se conozcan y cumplan en primera instancia, pero las infracciones repetidas pueden dar lugar a que el Administrador de la puerta de enlace central suspenda la capacidad de presentar solicitudes urgentes a través del SSAD.

6.4.2. Las Partes contratadas DEBEN mantener un contacto dedicado a tratar las Solicitudes Urgentes de SSAD, que pueda ser almacenado y utilizado por el Administrador de la puerta de enlace central, en circunstancias en que una solicitud del SSAD haya sido marcada como Urgente.

6.5. El Equipo responsable del EPDP recomienda que las Partes contratadas DEBEN publicar sus horarios laborales estándar, días hábiles y la zona horaria correspondiente en el portal del SSAD.

Pautas para la implementación

6.6 Véase, como referencia, el Marco para que los Operadores de Registro Respondan ante Amenazas de Seguridad en el que se señala lo siguiente: "*El juicio inicial de que una solicitud es de "Prioridad alta" debería ser evidente y no requerir habilidades únicas para determinar un nexo con la seguridad pública. La "Prioridad*

alta" se debería considerar como una amenaza inminente para la vida humana, la infraestructura crítica o la explotación infantil".

6.7 Infraestructura crítica significa los sistemas físicos y cibernéticos que son vitales en la medida en que su incapacidad o destrucción tendría un impacto perjudicial importante en la seguridad física o económica o en la salud o la seguridad pública.

6.8 Véase también la recomendación 10, que contiene más detalles en relación con los requisitos para una solicitud Urgente del SSAD.

¿Cómo se define la prioridad?
La prioridad es un código asignado a las solicitudes de divulgación que supone que el procesamiento se realizará sobre la base de los tiempos de respuesta acordados y objetivos de mejor esfuerzo.

¿Quién establece la prioridad?
La prioridad inicial de una solicitud de divulgación la establece el Solicitante, mediante las opciones de prioridad definidas por esta política. Al seleccionar una prioridad, el Administrador de la puerta de enlace central indicará claramente los criterios aplicables a una Solicitud Urgente y las posibles consecuencias del uso indebido de esta configuración de prioridad.

¿Qué ocurre si es necesario cambiar la prioridad?
Es posible que sea necesario reasignar la prioridad fijada inicialmente durante la revisión de la solicitud. Por ejemplo, como una solicitud se revisa manualmente, la Parte contratada PUEDE observar que aunque la prioridad se establece como Prioridad 2 (UDRP/URS), la solicitud no muestra ninguna prueba que documente un caso de la UDRP presentado y, por consiguiente, la solicitud debería reclasificarse como Prioridad 3. Cualquier reclasificación DEBE ser comunicada al Administrador de la puerta de enlace central y al Solicitante. Una vez recibida una solicitud de divulgación no automatizada del Administrador de la puerta de enlace central, la Parte contratada es responsable de determinar si se divulgan los datos sin carácter público. Dentro de los tiempos de respuesta definidos anteriormente, la Parte contratada DEBE responder a la solicitud.

Recommendation #7. Propósitos del Solicitante

7.1. El Equipo responsable del EPDP recomienda que:

7.1.1. Los Solicitantes DEBEN presentar solicitudes de divulgación de datos para fines específicos como, por ejemplo, entre otros: (i) aplicación del derecho penal, seguridad nacional o pública, (ii) investigaciones no relacionadas con la aplicación de la ley y demandas civiles, incluidas las relativas a la infracción de la propiedad intelectual y los reclamos en

virtud de la UDRP y el URS, (iii) protección del consumidor, prevención del uso indebido y seguridad de las redes y (iv) obligaciones aplicables a las entidades reguladas.[21] Requestors MAY also submit data verification requests on the basis of Registered Name Holder (RNH) consent that has been obtained by the Requestor (and is at the sole responsibility of that Requestor), for example to validate the RNH's claim of ownership of a domain name registration, or contract with the Requestor.

7.1.2. La afirmación de uno de estos propósitos específicos no garantiza el acceso en todos los casos, sino que dependerá de la evaluación de los méritos de la solicitud específica, el cumplimiento de todos los requisitos de la política aplicables y el fundamento jurídico de la solicitud.

Recommendation #8. Autorización de Partes Contratadas

Para mayor claridad, esta recomendación se refiere a las solicitudes de divulgación que se envían a la Parte contratada para su revisión. Estos requisitos NO se aplican a las solicitudes de divulgación que cumplen los criterios para el procesamiento automatizado de las decisiones de divulgación descritos en la recomendación 9, independientemente de que el procesamiento automatizado de las decisiones de divulgación sea obligatorio o se realice a solicitud de la Parte contratada. Esta recomendación no anula la capacidad de las Partes contratadas de diferenciar entre los registratarios sobre una base geográfica, como se indica en la recomendación 16 (de la Fase 1 del EPDP), ni anula la capacidad de las Partes contratadas de diferenciar entre personas jurídicas y físicas, como se indica en la recomendación 17 (de la Fase 1 del EPDP) para esta recomendación específica.

Requisitos generales

La Parte contratada

8.1. DEBE revisar cada solicitud de forma individual y no de forma masiva, independientemente de que la revisión se realice automáticamente o mediante una revisión significativa y NO DEBE divulgar datos basándose únicamente en la categoría de usuario acreditado.

8.2. PUEDE tercerizar la responsabilidad de la autorización a un proveedor externo, pero la Parte contratada seguirá siendo responsable en última instancia de garantizar que se cumplan los requisitos aplicables.

[21] Por ejemplo, la Directiva de la Unión Europea sobre la seguridad de las redes y los sistemas de información (conocida como la Directiva NIS) impone obligaciones específicas a los proveedores de servicios digitales y a los operadores de servicios esenciales.

8.3. DEBE determinar su propio fundamento jurídico para el procesamiento relacionado con la decisión de divulgación.[22] El Solicitante tendrá la capacidad de identificar el fundamento jurídico en virtud del cual espera que la Parte contratada divulgue los datos solicitados; sin embargo, en todos los casos en que la Parte contratada sea responsable de tomar la decisión de divulgación, la Parte contratada DEBE tomar la determinación final del fundamento jurídico apropiado.

8.4. DEBE apoyar las solicitudes de reexamen recibidas a través del sistema SSAD y DEBE considerarlas sobre la base del fundamento proporcionado por el Solicitante. Para mayor claridad, si se vuelve a presentar una solicitud de divulgación que sea idéntica a la solicitud original, sin una justificación que respalde el motivo por el cual debe reconsiderarse la solicitud, no es necesario que la Parte contratada vuelva a considerarla.

8.5. Ante la ausencia de cualquier requisito legal en contrario, la divulgación NO DEBE ser rechazada únicamente por la falta de cualquiera de los siguientes elementos: (i) una orden judicial; (ii) una citación; (iii) una acción civil pendiente o (iv) un procedimiento UDRP o URS. Tampoco es posible rechazar una divulgación solo por el hecho de que la solicitud se basa en una presunta infracción de propiedad intelectual.

Requisitos para la determinación de la autorización

Tras la recepción de una solicitud del Administrador de la puerta de enlace central, la Parte contratada:

8.6. DEBE llevar a cabo una revisión *prima facie*[23] de la validez de la solicitud, es decir, si la solicitud es suficiente para que la Parte contratada fundamente una revisión sustancial y procese los datos subyacentes asociados. Si la Parte contratada determina que la solicitud no es válida, por ejemplo, que no aduce motivos suficientes para una revisión sustancial de los datos subyacentes, la Parte contratada DEBE pedirle al Solicitante que proporcione información adicional antes de denegar la solicitud.

8.7. Si la solicitud se considera válida sobre la base de la revisión prima facie, DEBERÁ realizar una revisión sustancial de la solicitud y los datos subyacentes:

8.7.1. Si, tras la evaluación de los datos subyacentes, la parte contratada determina razonablemente que la divulgación de los elementos de datos solicitados no daría lugar a la divulgación de datos personales, la Parte contratada DEBE divulgar los datos, a menos que la divulgación esté prohibida

[22] Véase también la pauta 17 para la implementación.

[23] Según el Diccionario de Cambridge, a primera vista (ligeramente y de paso en el reconocimiento de algo, para significar la facilidad de aprender o de reconocer algo).

en virtud de la ley aplicable.[24] Para mayor claridad, si la divulgación no da lugar a la divulgación de datos personales, la Parte contratada no tiene que seguir evaluando la solicitud.

8.7.2. Si, tras la evaluación de los datos subyacentes, la Parte contratada determina que la divulgación de los elementos de datos solicitados daría lugar a la divulgación de datos personales, la Parte contratada DEBE determinar, como mínimo, como parte de su revisión sustancial de la solicitud y la datos subyacentes:

8.7.2.1. si la parte contratada tiene un fundamento jurídico para la divulgación;[25]
8.7.2.2. si todos los elementos de datos solicitados son necesarios;[26]
8.7.2.3. si se requiere un balance o revisión según el fundamento jurídico identificado por la Parte contratada como en el caso de la sección 8.3.

8.8. Si la solicitud está sujeta a un balance o a una revisión según la sección 8.7.2.3:

8.8.1. DEBE divulgar los datos si, en base a su evaluación, la Parte contratada determina que el interés legítimo del Solicitante no es superado por los intereses o los derechos y libertades fundamentales del titular de los datos.

La Parte contratada DEBE documentar los fundamentos de su aprobación.

8.8.2. DEBE denegar la solicitud si, en base a su evaluación, la Parte contratada determina que el interés legítimo del Solicitante es superado por los intereses o los derechos y libertades fundamentales del titular de los datos. La Parte contratada DEBE documentar el fundamento de su denegación y DEBE comunicar la razón de la denegación al Administrador de la puerta de enlace central, con la precaución de asegurarse de que no se incluyan datos personales en la razón de la denegación.

8.9. Si la solicitud es objeto de un balance o a una revisión conforme a la sección 8.7.2.3:

8.9.1. DEBE divulgar si la Parte contratada determina que tiene un fundamento jurídico o que no está prohibido por la ley aplicable divulgar los datos. La Parte contratada DEBE documentar los fundamentos de su aprobación.

8.9.2. DEBE denegar la solicitud si la Parte contratada determina que no tiene un fundamento jurídico o que está prohibido por la ley aplicable divulgar los

[24] Al considerar la publicación de datos sin carácter público de personas jurídicas, en particular con respecto a las ONG y a las partes que realizan actividades relacionadas con derechos humanos que pueden estar protegidas por la legislación local (por ejemplo, la ley de Derechos Constitucionales y de la Carta), la Parte contratada debería considerar las repercusiones en las personas que podrían ser identificadas al divulgar los datos de la persona jurídica.

[25] Véase también la pauta 17 para la implementación

[26] Para obtener más información sobre la definición de "necesario", consulte la página 7 del asesoramiento jurídico al que el Equipo responsable del EPDP se refirió al formular esta definición.

datos. La Parte contratada DEBE documentar el fundamento de su denegación y DEBE comunicar la razón de la denegación al Administrador de la puerta de enlace central, con la precaución de asegurarse de que no se incluyan datos personales en la razón de la denegación.

El Solicitante:

8.10. PUEDE presentar una solicitud de reexamen si cree que su solicitud fue indebidamente denegada.

8.11. DEBE, dentro de su solicitud de reexamen, proporcionar un fundamento que justifique por qué su solicitud debe ser reexaminada. La justificación debería proporcionar suficientes detalles sobre por qué el solicitante cree que su solicitud fue denegada indebidamente.

8.12. Si un Solicitante cree que una Parte contratada no está cumpliendo con alguno de los requisitos de esta política, el Solicitante DEBERÍA notificar a la organización de la ICANN además del mecanismo de alerta descrito en la Recomendación 5 - Requisitos de respuesta.

Pautas para la implementación

8.13. El Equipo responsable del EPDP prevé que la Parte contratada tenga la capacidad de comunicarse con el Solicitante a través de un ticket dedicado en el SSAD. El Equipo responsable del EPDP también prevé que el SSAD esté plenamente protegido por la tecnología de protección de datos estándar de la industria, incluido el cifrado para proteger la transmisión de datos personales, de conformidad con las leyes de protección de datos y las leyes de ciberseguridad aplicables.

8.14. El Equipo responsable del EPDP toma nota de los detalles de cómo se evaluará la comunicación del párrafo 8.6 en la fase de implementación de la política; sin embargo, el Equipo responsable del EPDP proporciona esta orientación adicional para ayudar. El Equipo responsable del EPDP prevé que la Parte contratada envíe una notificación al Solicitante, a través del correspondiente ticket del SSAD, en la cual notifique su decisión de denegar la solicitud. El Solicitante dispondría entonces de un plazo de (x) días para proporcionar información actualizada a la Parte contratada. Una vez que el Solicitante proporcione información actualizada, se restablecerá el tiempo de respuesta del SLA. Por ejemplo, la Parte contratada tendría un día hábil para responder a la solicitud urgente actualizada. Si el Solicitante opta por no proporcionar la información, el SLA se contaría cuando la Parte contratada envíe la notificación de "intención de denegar" al Solicitante. Si el Solicitante decide no responder, la solicitud será denegada en cuanto el plazo haya vencido.

8.15. En situaciones en las que la Parte contratada está evaluando el interés legítimo del Solicitante, la Parte contratada DEBERÍA considerar lo siguiente:

8.15.1. El interés debe ser específico, real y presente en lugar de ser vago y especulativo.

8.15.2. Por lo general, un interés se considera legítimo siempre y cuando se pueda reivindicar conforme a la ley de protección de datos y otras leyes.

8.15.3. Entre los ejemplos de intereses legítimos se incluyen los siguientes: (i) cumplimiento, ejercicio o defensa de los derechos legales, incluida la infracción de la propiedad intelectual; (ii) prevención del fraude y uso indebido de los servicios; (iii) seguridad física, informática y de redes.

8.16. La Parte contratada DEBERÍA, como parte de su revisión sustancial, evaluar al menos lo siguiente:

8.16.1. Según corresponda, los siguientes factores deberían utilizarse para determinar si el interés legítimo del Solicitante no es superado por los intereses o los derechos y libertades fundamentales del titular de los datos. Ningún factor es determinante, sino que la Parte contratada DEBERÍA considerar la totalidad de las circunstancias que se exponen a continuación:

8.16.1.1. *Evaluación del impacto*. Considerar el impacto directo en los titulares de los datos así como las posibles consecuencias más amplias del procesamiento de datos. Considerar el interés público y los intereses legítimos que persigue el Solicitante para, por ejemplo, mantener la seguridad y la estabilidad del DNS. Siempre que las circunstancias de la solicitud de divulgación o la naturaleza de los datos a divulgar sugieran un mayor riesgo para el titular de los datos afectado, esto se tendrá en cuenta durante la toma de decisiones.

8.16.1.2. *Naturaleza de los datos.* Considerar el nivel de sensibilidad de los datos así como si los datos ya están disponibles de forma pública.

8.16.1.3. *Estatus del titular de los datos.* Considerar si el estatus del titular de los datos aumenta su vulnerabilidad (por ejemplo, niños, solicitantes de asilo, otras clases protegidas)

8.16.1.4. *Alcance del procesamiento.* Considerar la información de la solicitud de divulgación u otras circunstancias pertinentes que indique si los datos se conservarán en condiciones de seguridad (riesgo menor) o si se divulgarán públicamente, si se pondrán a disposición de una gran cantidad de personas, o si se combinarán con otros datos (riesgo mayor),[27] siempre y cuando no tenga por objeto prohibir divulgaciones públicas para acciones legales o procedimientos administrativos de resolución de disputas como la UDRP o el URS.

[27] Para obtener más información sobre el contexto relacionado con el riesgo mayor cuando se combinan los datos, consulte la página 5 del asesoramiento jurídico al que el Equipo responsable del EPDP se refirió al considerar estos factores.

8.16.1.5. *Expectativas razonables del titular de los datos.* Considerar si el titular de los datos esperaría razonablemente que su datos se procesen/divulguen de esta manera.
8.16.1.6. *Estatus del responsable del tratamiento y del titular de los datos.* Considerar el poder de negociación y cualquier desequilibrio de autoridad entre el responsable del tratamiento y el titular de los datos.[28]
8.16.1.7. *Marcos jurídicos involucrados.* Considerar los marcos legales jurisdiccionales del Solicitante, las Partes contratadas y el titular de los datos, y cómo esto puede afectan a las posibles divulgaciones.
8.16.1.8. *Transferencias transfronterizas de datos.* Considerar los requisitos que pueden aplicarse a las transferencias transfronterizas de datos.

8.17. Un fundamento jurídico puede basarse en la presencia de un fundamento jurídico según la política de la ICANN (o la ley aplicable).

La aplicación de la prueba de equilibrio y los factores considerados en esta sección DEBERÍAN revisarse, según corresponda, para tener en cuenta la jurisprudencia aplicable que interprete el GDPR, las directrices publicadas por el EDPB o las revisiones al GDPR u otras leyes de privacidad aplicables que puedan producirse en el futuro.

Recommendation #9. Automatización del procesamiento del SSAD

9.1. El Equipo responsable del EPDP recomienda que el Administrador de la puerta de enlace central DEBE automatizar la recepción, autenticación y transmisión de las solicitudes del SSAD a la Parte contratada pertinente en la medida en que sea técnica y comercialmente factible y legalmente permitido.

9.2. El SSAD DEBE permitir la automatización del procesamiento de solicitudes bien formadas, válidas, completas y debidamente identificadas de usuarios acreditados, como se describe a continuación.

Procesamiento automatizado de las decisiones de divulgación

9.3. Las Partes contratadas DEBEN procesar de manera automatizada las decisiones de divulgación para cualquier categoría de solicitudes para las que se determine que la automatización (véase la sección 9.4 y los procesos detallados en la recomendación 18)

[28] En el contexto de la autorización de la Parte contratada, las partes relevantes son la Parte contratada (responsable del tratamiento) y el registratario (titular de los datos); sin embargo, las funciones y responsabilidades de las partes se examinarán más a fondo en la implementación.

es un proceso técnica y comercialmente[29] factible[30] y legalmente permitido. Para evitar dudas, el Equipo responsable del EPDP recomienda que las categorías de decisiones de divulgación que no cumplan actualmente esos criterios no se excluyan de la consideración de la divulgación automatizada en el futuro, con sujeción a los procesos detallados en la Recomendación 18. En las áreas en las cuales las decisiones de divulgación no cumplan estos criterios, el objetivo de base es la estandarización del proceso de decisión sobre la divulgación.

9.4. De acuerdo con el asesoramiento jurídico obtenido (véase Asesoramiento sobre reautomatización de casos de uso en el contexto de la divulgación de datos de registratario sin carácter público - abril de 2020), el Equipo responsable del EPDP recomienda que los siguientes tipos de solicitudes de divulgación, para los cuales se haya indicado que está permitido legalmente en el marco del GDPR para la automatización completa (tanto la recepción como el procesamiento de la decisión de divulgación) DEBEN automatizarse desde el momento del lanzamiento de la SSAD:

- 9.4.1. Las solicitudes de los organismos encargados de la aplicación de la ley de las jurisdicciones locales o de otra índole con 1) un fundamento jurídico confirmado por la sección 6(1)e del GDPR, o 2) el procesamiento que se llevará a cabo conforme a una exención del Artículo 2 del GDPR.
- 9.4.2. La investigación de una infracción de la legislación de protección de datos presuntamente cometida por la ICANN/Partes contratadas que afecte al registratario.
- 9.4.3. Solicitud únicamente del campo que especifica la ciudad, para evaluar si se interpondrá un reclamo o con fines estadísticos.
- 9.4.4. Ningún dato personal en el acta de la registración que haya sido divulgado previamente por la Parte contratada.

9.5. Para mayor claridad, si una Parte contratada determina que el procesamiento automatizado de las decisiones de divulgación para los casos de uso especificados en esta recomendación o mediante los procesos detallados en la Recomendación 18 no está legalmente permitido o conlleva un riesgo importante que no se reconoció en la orientación jurídica obtenida por el Equipo responsable del EPDP pero que posteriormente se ha identificado y documentado mediante, por ejemplo, una Evaluación del Impacto en la Protección de Datos (DPIA), la Parte contratada DEBE

[29] Durante la implementación, habrá que seguir considerando la factibilidad comercial de los registradores que puedan recibir un número muy limitado de solicitudes que cumplan los criterios para el procesamiento automatizado de las decisiones de divulgación y si la carga financiera de permitir este procesamiento automatizado es de tal magnitud que pueda ser necesario prever una exención. Como parte de esta consideración, el Administrador de la puerta de enlace central también debería considerar cómo puede facilitar la integración del sistema de una Parte contratada con el SSAD para reducir cualquier posible carga de procesamiento automatizado de las decisiones de divulgación.

[30] La consideración inicial de la factibilidad financiera de la automatización será abordada por la organización de la ICANN con el Equipo para la Revisión de la Implementación y, posteriormente, mediante el mecanismo de evolución del SSAD, según corresponda.

notificar a la organización de la ICANN que requiere una exención del procesamiento automatizado de las decisiones de divulgación para el caso o los casos de uso identificados y DEBE incluir documentación de respaldo con su notificación. Las notificaciones de exención no razonables PUEDEN estar sujetas a revisión por parte de la Organización de la ICANN. La organización de la ICANN DEBE revertir el reconocimiento de la exención si considera que la notificación de la Parte contratada es incorrecta o abusiva.

9.6. Tan pronto como se notifique a la organización de la ICANN, el Administrador de la puerta de enlace central DEBE detener la transmisión de los casos de uso identificados como que requieren procesamiento automatizado y DEBE transmitir la solicitud conforme a los requisitos de la Recomendación 8 – Autorización de la Parte contratada.

9.7. La organización de la ICANN DEBE proporcionar un proceso de notificación y comentarios para permitir a las partes interesadas afectadas realizar sus aportes sobre las exenciones previstas en el apartado 9.5. La organización de la ICANN PODRÍA facilitar un debate posterior entre las partes interesadas afectadas y la Parte contratada en cuestión para facilitar el entendimiento mutuo de la exención y la información de apoyo En la implementación se determinarán más detalles, incluida la posible confidencialidad del proceso.

9.8. Tan pronto como la Parte contratada tome conocimiento de que la exención ya no es aplicable, DEBE informar a la organización de la ICANN en consecuencia.

9.9. Tras la notificación de una Parte contratada en virtud del apartado 9.8, el Administrador de la puerta de enlace central DEBE transmitir a la Parte contratada las solicitudes que cumplan los criterios de procesamiento automatizado de conformidad con esta recomendación y la Parte contratada DEBE reanudar el procesamiento automatizado de las decisiones de divulgación para los casos de uso pertinentes.

9.10. Con respecto a las solicitudes de divulgación que se enviarían a una Parte contratada para su revisión, una Parte contratada PUEDE solicitar a la Puerta de enlace central que automatice el procesamiento de la decisión de divulgación de todas o ciertos tipos de solicitudes de divulgación y/o solicitudes provenientes de un determinado Solicitante,[31] después de que la Parte contratada haya sopesado el riesgo y evaluado si es legalmente permitido, según corresponda.

9.11. Una Parte Contratada PUEDE retractarse o revisar en cualquier momento una solicitud para automatizar la decisión de divulgación que no sea requerida por estas recomendaciones de políticas.

[31] Por ejemplo, una Parte contratada podría considerar la posibilidad de implementar un plan de Notificadores de confianza que permitiera calificar a los Solicitantes que cumplieran determinados criterios establecidos por la Parte contratada pertinente para obtener respuestas automatizadas a sus solicitudes de divulgación.

9.12. Para mayor claridad, el Administrador de la puerta de enlace central supervisa si una solicitud de divulgación ha cumplido los criterios para el procesamiento automatizado de las decisiones de divulgación que PUEDEN implicar una revisión no automatizada en la Puerta de enlace central. Asimismo, la Puerta de enlace central PUEDE solicitar a la Parte contratada más información que pueda ayudar al Administrador de la puerta de enlace central a determinar si se han cumplido o no los criterios para un procesamiento automatizado de las decisiones de divulgación. Una Parte contratada PUEDE proporcionar dicha información adicional, si se le solicita. No se espera que se transfieran datos personales en respuesta a una solicitud de información de ese tipo.

Pautas para la implementación

Además de los requisitos detallados en la Recomendación 4 (Acuse de recibo) y la Recomendación 10 (SLA), que también se aplicarán al procesamiento automatizado de las decisiones de divulgación, se aplicarán las siguientes pautas para la implementación al procesamiento automatizado de las decisiones de divulgación, es decir, a las solicitudes para las cuales el Administrador de la puerta de enlace central determine que se requiere una decisión automatizada para la solicitud de divulgación de la Parte contratada, conforme a esta recomendación.

9.13. El Equipo responsable del EPDP espera que se puedan automatizar aspectos del SSAD como la recepción de solicitudes, la verificación de credenciales y la validación de la presentación de solicitudes (el formato y si están completas, no el contenido), aunque es probable que no sea posible automatizar completamente todos los aspectos de la revisión y la divulgación de las solicitudes de divulgación en todos los casos.

9.14. En el contexto de una mayor consideración sobre los posibles casos de uso que se consideran legalmente permitidos en el contexto de la recomendación 18, se prevé que la parte o partes que asuman la responsabilidad del procesamiento automatizado de las decisiones de divulgación se encarguen de determinar si están legalmente permitidas, ante la ausencia de directrices autoritativas (por ejemplo, el EDPB, Tribunal de Justicia de la Unión Europea, ley nueva).

9.15. Además del asesoramiento jurídico mencionado anteriormente, el Equipo responsable del EPDP recomienda al Comité Permanente de la GNSO (véase la recomendación 18) que, en su revisión, siga considerando las medidas de protección descritas en el apéndice 2 del Asesoramiento sobre casos de uso para la reautomatización en el contexto de la divulgación de datos de registratarios sin carácter público - abril de 2020 y los casos de uso descritos en la Sección 3.4 de dicho Asesoramiento, para considerar si la divulgación constituiría un efecto jurídico o un efecto significativo similar que pudiera impedir la automatización de la divulgación.

9.16. Se espera que el procesamiento automatizado de las decisiones de divulgación funcione en la práctica, dado que el Administrador de la puerta de enlace central confirmará que la solicitud cumple los requisitos para el procesamiento automatizado y dará instrucciones a la Parte contratada para que divulgue automáticamente los datos solicitados al Solicitante. Se prevé que el mecanismo se determine durante la implementación.

9.17. Todas las partes que participan en el SSAD deberán tener en cuenta los requisitos que pueden aplicarse a las transferencias transfronterizas de datos.

Recommendation #10. Determinación de los SLA variables para los tiempos de respuesta para el SSAD

10.1. El Equipo responsable del EPDP recomienda que las Partes contratadas DEBEN cumplir los Acuerdos de Nivel de Servicio (SLA) que se desarrollen, apliquen y hagan cumplir, y que se actualicen oportunamente según la Recomendación 18, conforme a las pautas para la implementación que se proporciona a continuación.

10.2. A los efectos de calcular el tiempo de respuesta del SLA, el Equipo responsable del EPDP recomienda que el SLA comience cuando el Administrador de la puerta de enlace central proporcione a la Parte contratada una solicitud validada con toda la información de apoyo y que se detenga cuando la Parte contratada responda (a través de la puerta de enlace central) ya sea con la información solicitada, una respuesta de rechazo o una solicitud de información adicional. Una solicitud de reexamen o una respuesta del Solicitante con más información se considerarían el inicio de una nueva solicitud a efectos del cálculo del SLA.

Matriz de prioridades para las solicitudes de divulgación no automatizadas

Tipo de solicitud	Prioridad	SLA propuesto[32] (Cumplimiento a los 6 meses / 12 meses / 18 meses)
Solicitudes urgentes	1	1 día hábil, no más de 3 días calendario (85 % / 90 % / 95 %)
Procedimientos administrativos de la ICANN	2	Máx. 2 días hábiles (85 % / 90 % / 95 %)
Todas las demás solicitudes*	3	Ver las pautas para la implementación a continuación.

[32] Nota: los días hábiles a los que se hace referencia en la tabla son desde el momento en que la Parte contratada recibe la solicitud de divulgación del Administrador de la puerta de enlace central.

* Nota: Nada en estas recomendaciones de política prohíbe explícitamente el desarrollo de nuevas categorías y SLA definidos.

Pautas para la implementación

10.3. Se pretende que los requisitos de prioridad 1 y 2 se hagan vinculantes mediante el documento de política de consenso. Los requisitos de nivel de servicio de prioridad 3 también se pueden hacer vinculantes como parte del documento de la política de consenso, en consulta con el IRT.

Definiciones propuestas

Días hábiles:[33] definidos en la jurisdicción de la Parte contratada.
Tiempo de respuesta promedio: promedio móvil de todos los tiempos de respuesta, calculado de forma automática con frecuencia (por ejemplo, diario o semanal) como utilidad para que una Parte contratada pueda evaluar su propio desempeño en cualquier momento.
Intervalo de evaluación del objetivo de la respuesta: período de 3 meses que permite revisar el rendimiento del tiempo de respuesta 4 veces al año.
Valor objetivo de respuesta: valor de la medición del Tiempo de respuesta promedio en el día de cierre del Intervalo de evaluación del objetivo de respuesta.
Valor objetivo de cumplimiento: la misma definición que el Valor objetivo de respuesta, pero con una revisión de cumplimiento de este objetivo de SLA.

Los requisitos de tiempo de respuesta de las Partes contratadas para las solicitudes de SSAD se acelerarán en dos fases:

- La Fase 1 comienza **seis (6) meses** después de la fecha de entrada en vigencia de la política del SSAD.
- La Fase 2 comienza **un (1) año** después de la fecha de entrada en vigencia de la política del SSAD.

FASE 1 (solo se aplica a las solicitudes de prioridad 3)

10.4. Durante la Fase 1, y continuando a partir de entonces, los objetivos de respuesta de las Partes contratadas para las solicitudes de Prioridad 3 del SSAD serán cinco (5) días hábiles.

10.5. El Administrador de la puerta de enlace central DEBE medir los objetivos de respuesta mediante el uso de un Tiempo de respuesta promedio, no en base a cada respuesta.

[33] Véase también la recomendación 6.5.

10.6. El SSAD DEBE calcular el Tiempo promedio de respuesta en curso de la Parte contratada como un promedio móvil, como una utilidad para que la Parte contratada evalúe su propio desempeño en cualquier momento.

10.7. El SSAD también DEBE medir el Valor objetivo de respuesta del promedio móvil en curso al final del Intervalo de evaluación del objetivo de respuesta. Solo el Valor objetivo de respuesta de 3 meses DEBE utilizarse para determinar el éxito o el fracaso en el cumplimiento de los objetivos de respuesta como se describe a continuación. A los efectos de evitar dudas, la intención del SSAD que proporciona a la Parte contratada el tiempo de respuesta promedio es advertirle sobre que puede haber un problema con sus tiempos de respuesta y permitirle a la Parte contratada remediarlo de manera cooperativa. Por lo tanto, las Partes contratadas deben tener acceso en todo momento a la visualización de su propio Valor objetivo de respuesta actual. Si el Valor objetivo de respuesta de la Parte contratada supera los cinco (5) días hábiles, esto NO DEBE dar lugar a un incumplimiento de la política.

En cambio, el incumplimiento de un objetivo de respuesta hará que la ICANN alerte a la Parte contratada de un incumplimiento del objetivo de respuesta.

10.8. La Parte contratada DEBE responder a la notificación de incumplimiento de objetivo de respuesta de la ICANN en un plazo de cinco (5) días hábiles.

10.9. La respuesta de la Parte contratada debe incluir una justificación de por qué no pudo cumplir su objetivo de respuesta.

10.10. La falta de respuesta de la Parte contratada a la notificación de la ICANN DEBE considerarse un incumplimiento de la política; por consiguiente, la falta de respuesta a la notificación de cumplimiento dará lugar a una consulta de Cumplimiento de la ICANN.

FASE 2 (solo se aplica a las solicitudes de prioridad 3)

10.11. En la fase 2, los objetivos de cumplimiento de las Partes contratadas para las solicitudes de Prioridad 3 del SSAD serán diez (10) días hábiles.

10.12. El Administrador de la puerta de enlace central DEBE medir los objetivos de cumplimiento mediante el uso de un Tiempo de respuesta promedio, no en base a cada respuesta. El SSAD calculará el promedio del objetivo de cumplimiento de la Parte contratada en el último día del Intervalo de evaluación del objetivo de respuesta.

10.13. Si el Valor objetivo de respuesta de la Parte contratada supera los diez días hábiles, esto dará lugar a un incumplimiento de la política y, en consecuencia, la Parte contratada estará sujeta a la imposición del cumplimiento.

10.14. Los objetivos de respuesta y los objetivos de cumplimiento DEBEN revisarse, como mínimo, después de cada seis meses en el primer año y, posteriormente, una vez al año (dependiendo del resultado de la primera revisión).

10.15. Se prevé que los objetivos de respuesta a las solicitudes de divulgación que cumplan los criterios de las respuestas totalmente automatizadas se desarrollen más durante la fase de implementación, pero se prevé que sean inferiores a 60 segundos.

10.16. El Equipo para la Revisión de la Implementación debería seguir examinando el efecto de los acuerdos de nivel de servicio en los casos en que se solicite información adicional a la Parte contratada y esta sea proporcionada por el Solicitante. (Para obtener más información, véase la Recomendación 8, Autorización de las Partes contratadas).

Recommendation #11. Términos y condiciones del SSAD

11.1. El Equipo responsable del EPDP recomienda que, durante la fase de implementación, se definan con mayor detalle las expectativas mínimas de acuerdos y políticas adecuadas, como las condiciones de uso del SSAD, una política de privacidad del SSAD, un acuerdo de divulgación y una política de uso aceptable, para que, posteriormente, la entidad responsable del SSAD los desarrolle y exija su cumplimiento (mediante la organización de la ICANN o un tercero al cual la organización de la ICANN haya encomendado esta función para exigir el cumplimiento). Estos acuerdos y políticas DEBEN tener en cuenta todas las recomendaciones de esta política. Se prevé que estos acuerdos y políticas sean elaborados y negociados, según corresponda, por las partes que participan en el SSAD, teniendo en cuenta las pautas para la implementación que figuran a continuación.

11.2. Todos los acuerdos necesarios relativos al procesamiento de las solicitudes de datos a través del SSAD, DEBEN incluir cláusulas relativas a las transferencias transfronterizas y asegurar el compromiso de las partes, según corresponda, de garantizar y prever un nivel adecuado de protección de los datos.

11.3. Los Términos y Condiciones del SSAD PUEDEN ser actualizados, según corresponda, por la organización de la ICANN para abordar las leyes y prácticas aplicables.

Pautas para la implementación:

11.4. Política de privacidad para el procesamiento de datos personales de los Usuarios del SSAD (Solicitantes y Partes contratadas del SSAD) mediante el SSAD

El EPDP recomienda, como mínimo, que la política de privacidad DEBE incluir los principios de protección de datos pertinentes, entre ellos los siguientes:

- El tipo (o tipos) de datos personales procesados.
- Cómo y por qué se procesan los datos personales, por ejemplo:
  - verificación de identidad
  - comunicación de notificaciones de servicio
- Tiempo durante el cual se conservarán los datos personales.
- Los tipos de terceros con los que se comparten los datos personales.
- Cuando proceda, detalles de cualquier transferencia internacional de datos o requisito de la misma.
- Información sobre los derechos de los titulares de los datos y el método mediante el cual pueden ejercerlos.
- Notificación sobre cómo se comunicarán los cambios en la política de privacidad.
- Requisitos de transparencia.
- Requisitos de seguridad de los datos.
- Medidas de responsabilidad (privacidad por diseño, de forma predeterminada, Delegado de Protección de Datos (DPO) por encima de cierto tamaño, etc.)

11.5. Condiciones de uso para los usuarios del SSAD (Solicitantes y Partes contratadas del SSAD)

El EPDP recomienda, como mínimo, que las condiciones de uso DEBEN abordar lo siguiente:

- Indemnización del Solicitante a los responsables del tratamiento de datos (entidad responsable de la decisión de divulgación) en base a los siguientes principios:
  - Los solicitantes son responsables de los daños y perjuicios o los costos relacionados con los reclamos de terceros que se deriven de: (i) sus declaraciones falsas en el proceso de acreditación o solicitud; o (ii) el uso indebido de los datos solicitados en contravención de las condiciones de uso o las leyes aplicables.
  - Nada de lo dispuesto en los presentes términos limita la responsabilidad o los derechos de recuperación de las partes en virtud de las leyes aplicables (es decir, no se impide que los Solicitantes procuren la recuperación de los responsables del tratamiento de datos cuando esos derechos estén previstos en la ley).
  - Nada de lo dispuesto en los presentes términos se interpretará en el sentido de crear obligaciones de indemnización para los Solicitantes de autoridades públicas que carezcan de la autoridad legal necesaria para suscribir dichas cláusulas de indemnización. Asimismo, nada de lo dispuesto en esta cláusula alterará la responsabilidad

gubernamental potencialmente existente como recurso para los operadores del SSAD.

- Requisitos de solicitud de datos.
- Requisitos de registro y auditoría.
- Capacidad para demostrar el cumplimiento.
- Prohibiciones aplicables.
- Requisitos de prevención del uso indebido.

11.6. Acuerdos de divulgación para Solicitantes del SSAD

El EPDP recomienda que, como mínimo, los acuerdos de divulgación DEBEN abordar los requisitos para los Solicitantes después de que los datos hayan sido divulgados al Solicitante:

- Utilización de los datos para el fin indicado en la solicitud.
- Requisitos para la utilización de los datos con un nuevo fin distinto del indicado en la solicitud.
- Retención y destrucción de datos: los Solicitantes DEBEN confirmar que almacenarán, protegerán y eliminarán los datos de registración de gTLD de acuerdo con la ley aplicable. Los Solicitantes DEBEN retener únicamente los datos de registración de gTLD durante el tiempo que sea necesario para lograr el propósito declarado en la solicitud de divulgación, a menos que la ley aplicable exija que se retengan esos datos durante un período más prolongado.
- Utilización lícita de los datos.

11.7. Política de uso aceptable para Solicitantes del SSAD. El Solicitante DEBE aceptar la Política de uso aceptable antes de que las solicitudes de divulgación puedan ser presentadas a través del SSAD.

Como mínimo, la Política de uso aceptable DEBE incluir los siguientes requisitos:

El Solicitante:

11.7.1. DEBE solicitar únicamente datos del conjunto de datos del RDS actual (no datos históricos);

11.7.2. DEBE, para cada solicitud de datos de RDS, proporcionar declaraciones del propósito correspondiente y el fundamento jurídico del procesamiento, que estarán sujetos a auditorías (véase la recomendación 16 sobre auditorías para obtener más detalles);

11.7.3. PUEDE solicitar datos del SSAD para múltiples propósitos por cada solicitud, para el mismo conjunto de datos solicitados;

11.7.4. para cada uno de los propósitos declarados debe proporcionar: (i) una declaración sobre el uso previsto de los datos solicitados y (ii)

una declaración que indique que el Solicitante únicamente procesará los datos para los fines declarados. Estas declaraciones estarán sujetas a auditorías (véase la recomendación 16 sobre auditorías para más obtener detalles).

Recommendation #12. Requisito de divulgación

12.1. El Equipo responsable del EPDP recomienda lo siguiente:

las Partes contratadas:

12.1.1. DEBEN divulgar únicamente los datos solicitados por el Solicitante;
12.1.2. DEBE devolver los datos actuales o un subconjunto de ellos (no datos históricos);

12.2. Las Partes contratadas y el Administrador de la puerta de enlace central:

12.2.1. DEBEN procesar los datos de acuerdo con la ley aplicable.
12.2.2. Cuando lo exija la legislación aplicable, DEBEN revelar al Titular del nombre registrado (titular de los datos), previa solicitud razonable, la confirmación del procesamiento de los datos personales que le conciernen, señalando, no obstante, que la naturaleza de las investigaciones o procedimientos legales PUEDE exigir al SSAD y/o a la entidad encargada de la divulgación que mantengan la confidencialidad sobre la naturaleza o la existencia de determinadas solicitudes ante el titular de los datos. Las solicitudes confidenciales PUEDEN ser divulgadas a los titulares de los datos en cooperación con la entidad solicitante y de conformidad con los derechos del titular de los datos en virtud de la legislación aplicable.
12.2.3. Cuando así lo exija la legislación aplicable, DEBEN prever mecanismos que permitan al titular de los datos ejercer su derecho a la eliminación, a oponerse al procesamiento automatizado de sus datos personales cuando dicho procesamiento tenga un efecto jurídico o de importancia similar, así como cualquier otro derecho aplicable.
12.2.4. DEBEN, de forma coherente, transparente, inteligible y de fácil acceso, mediante el uso de un lenguaje claro y sencillo, notificar a los titulares de los datos los tipos de entidades/terceros que pueden procesar sus datos. A los efectos de evitar dudas, las Partes contratadas DEBEN proporcionar la notificación descrita anteriormente a sus clientes registratarios, y el SSAD DEBE proporcionar la notificación descrita anteriormente a los usuarios del SSAD. En el caso de las Partes contratadas, esta notificación DEBE contener información sobre los posibles destinatarios de los datos de registración sin carácter público, incluidos, entre otros, los destinatarios enumerados en la Recomendación 7, Propósitos del Solicitante, en el marco de lo permitido por la ley. Los deberes de información de acuerdo con las leyes aplicables pueden aplicarse

adicionalmente, pero la información mencionada anteriormente DEBE estar contenida como mínimo.

Pautas para la implementación

12.3. El término "datos actuales" refiere a los datos revisados por la Parte contratada al determinar si se deben divulgar los datos. A fin de reducir la posibilidad de que se produzcan cambios en los datos durante la tramitación de una solicitud de divulgación pendiente, por ejemplo, si el registratario actualiza sus datos de contacto, se sugiere a las Partes contratadas que divulguen los datos lo antes posible tras su decisión sobre la divulgación. A los efectos de evitar dudas, el término "datos históricos" refiere a los datos de registración vigentes antes de que se realizara la solicitud de divulgación, no a los datos de registración que puedan haber cambiado como resultado de cualquier actualización realizada por el registratario entre el momento en que se examine la solicitud de divulgación y la decisión de divulgar los datos de registración.

12.4. La naturaleza de las investigaciones o procedimientos jurídicos no se limita a las investigaciones penales u otras investigaciones (por ejemplo, muchas investigaciones civiles requieren confidencialidad).

Recommendation #13. Política de consultas

13.1. El Equipo responsable del EPDP recomienda que el Administrador de la puerta de enlace central:

13.1.1. DEBE monitorear el sistema y tomar las medidas apropiadas,[34] como revocar o limitar el acceso, para protegerse contra el abuso o el uso indebido del sistema.

13.1.2. PUEDE tomar medidas para limitar la cantidad de solicitudes que presente el mismo Solicitante si se demuestra que las solicitudes son de carácter abusivo.

El uso "abusivo" del SSAD PUEDE incluir (entre otros) la detección de uno o más de los siguientes comportamientos/prácticas:

13.1.2.1. Cantidad elevada de presentaciones automatizadas de solicitudes incompletas.

13.1.2.2. Cantidad elevada[35] de solicitudes duplicadas automatizadas que sean de carácter frívolo, malicioso o vejatorio.

[34] El Equipo responsable del EPDP espera que el término "medidas apropiadas" se defina con mayor detalle en la fase de implementación.

[35] El Equipo responsable del EPDP prevé que el término "cantidad elevada" se defina con mayor detalle en la fase de implementación.

13.1.2.3. Uso de credenciales falsas, robadas o falsificadas para acceder a la sistema.

13.1.2.4. Almacenamiento/retraso y envío de una cantidad elevada de solicitudes que impidan el cumplimiento del SLA por parte del SSAD u otras partes. Cuando se investigue el uso indebido en base a este comportamiento específico, debe tenerse en cuenta el concepto de la proporcionalidad.

13.1.3. Al igual que con otras infracciones de la política de acceso, el comportamiento abusivo puede dar lugar en última instancia a la suspensión o cancelación del acceso al SSAD. En el caso de que el Administrador de la puerta de enlace central tome una determinación basada en el uso indebido para limitar la cantidad de solicitudes de un Solicitante, el Solicitante PUEDE procurar una remediación[36] a través de la organización de la ICANN si cree que la determinación es injustificada. A los efectos de evitar dudas, si el SSAD recibe una gran cantidad de solicitudes del mismo Solicitante, el volumen por sí solo no debe dar lugar a una determinación *de facto* de uso indebido del sistema.

13.1.4. DEBE responder únicamente a las solicitudes de un nombre de dominio específico para el que se solicita que se divulguen datos de respuesta sin carácter público y DEBE examinar[37] cada solicitud de forma individual y no de forma masiva, independientemente de que la consideración se realice automáticamente o mediante una revisión significativa.

13.2. El Equipo responsable del EPDP recomienda que las Partes contratadas:

13.2.1. NO DEBEN rechazar las solicitudes de divulgación del SSAD sobre la base de un comportamiento abusivo que no haya sido determinado como abusivo por el Administrador de la puerta de enlace central conforme a los puntos a) y b) anteriores. Sin embargo, las Partes contratadas también deben tener algún medio para informar este comportamiento al CGM/SSAD. El Administrador de la puerta de enlace central DEBE proporcionar un mecanismo para que las Partes contratadas informen sobre solicitudes/solicitantes que se consideren abusivos y proporcionen una determinación sobre la solicitud/solicitante dentro del plazo previsto para que la Parte contratada presente una respuesta. De forma alternativa, se permitirá a la Parte contratada aplazar la respuesta hasta que el Administrador de la

[36] Para mayor claridad, la remediación consistiría en una reconsideración por parte del Administrador de la puerta de enlace central, para lo cual el Solicitante puede proporcionar nueva información pero no está obligado a hacerlo.
[37] Se prevé que este examen no se realice de forma automática.

puerta de enlace central haya examinado el informe de uso indebido y haya tomado una determinación.

13.3. El Equipo responsable del EPDP recomienda lo siguiente:

13.3.1. El Administrador de la puerta de enlace central DEBE apoyar las solicitudes introducidas con el nombre de dominio completo (sin comodines).

13.3.2. El Administrador de la puerta de enlace central DEBE apoyar la capacidad de un Solicitante para presentar varios nombres de dominio en una única solicitud.[38]

13.3.3. En el caso de solicitudes de divulgación que no estén sujetas al procesamiento automatizado de la decisión de divulgación, el Administrador de la puerta de enlace central DEBE dirigir cada dominio individualmente a la Parte contratada responsable de la decisión de divulgación (esto puede requerir que el SSAD divida una solicitud en múltiples transacciones).

13.3.4. Sin perjuicio de las recomendaciones relativas al manejo del comportamiento abusivo, el Administrador de la puerta de enlace central y las Partes contratadas DEBEN tener la capacidad de manejar un número razonable de solicitudes en consonancia con los acuerdos de nivel de servicio establecidos.

13.3.5. El Administrador de la puerta de enlace central DEBE apoyar únicamente las solicitudes de datos actuales (no los datos sobre el historial de la registración del nombre de dominio).

13.3.6. El SSAD DEBE ser capaz de guardar el historial de las diferentes solicitudes de divulgación, a fin de mantener la trazabilidad de los intercambios entre los Solicitantes del SSAD y las Partes contratadas a través del SSAD. Es necesario establecer las medidas de protección adecuadas para proteger esta información. Se debe proporcionar a las Partes contratadas un acceso adecuado a dichas estadísticas de actividades pertinentes, según se considere necesario, para garantizar que toda la información pertinente relativa a las solicitudes de divulgación esté disponible para su consideración en dichas decisiones de divulgación.

Véase también los requisitos de la Política de uso aceptable en la Recomendación 11 - Términos y condiciones.

Pautas para la implementación

13.4. El comportamiento abusivo puede dar lugar en última instancia a la suspensión o cancelación del acceso al SSAD; sin embargo, en la implementación debería

[38] El Equipo responsable del EPDP prevé que en la implementación se determine razonablemente cuántos pueden presentarse a la vez, de acuerdo con la Política de consultas.

considerarse un plan de sanciones graduales. Sin embargo, puede haber ciertos casos de uso indebido flagrante, como la falsificación o el robo de credenciales, en los que la cancelación sería inmediata.

13.5. Se debe recibir una solicitud del SSAD por cada registración de nombres de dominio para la cual se solicite la divulgación de datos sin carácter público, pero los Solicitantes deben poder presentar varias solicitudes al mismo tiempo, por ejemplo, mediante la presentación varios registros de nombres de dominio en el mismo formulario de solicitud, siempre que se aplique la misma información de la solicitud.

13.6. En relación con la expresión "Se debe proporcionar a las Partes contratadas un acceso adecuado a dichas estadísticas de actividades pertinentes, según se considere necesario" en la sección 13.3, se prevé que esto se limite a la propia actividad de las Partes contratadas.

Recommendation #14. Sostenibilidad financiera

14.1. El Equipo responsable del EPDP recomienda que, al considerar los costos y la sostenibilidad financiera del SSAD, es necesario distinguir entre el desarrollo y la puesta en marcha del sistema y el posterior funcionamiento del mismo.

14.2. El objetivo es que el SSAD sea financieramente autosuficiente sin causar ningún cargo adicional a los registratarios. Los titulares de los datos NO DEBEN sufragar los costos de divulgación de sus datos a terceros; los Solicitantes de los datos del SSAD deberían sufragar principalmente los costos de mantenimiento de este sistema. Asimismo, los titulares de los datos NO DEBEN sufragar los costos del procesamiento de las solicitudes de divulgación de datos, que han sido denegadas por las Partes contratadas tras la evaluación de las solicitudes presentadas por los usuarios del SSAD. La ICANN PUEDE contribuir a la cobertura (parcial) de los costos de mantenimiento de la Puerta de enlace central. Para mayor claridad, el Equipo responsable del EPDP entiende que los registratarios son, en última instancia, la fuente de gran parte de los ingresos de la ICANN. Estos ingresos no infringen *per se* la restricción que indica que "los titulares de los datos NO DEBEN sufragar los costos de divulgación de sus datos a terceros". La Puerta de enlace central NO DEBE cobrar una tarifa aparte a los titulares de los datos por el hecho de que sus datos sean solicitados por o divulgados a terceros. Sin embargo, el Equipo responsable del EPDP señala que los titulares de los nombres registrados siempre asumirán indirectamente los costos en los que incurran los registradores y registros. El Equipo responsable del EPDP también entiende que el RAA prohíbe a la ICANN limitar lo que los Registradores pueden cobrar. La Sección 3.7.12 del RAA estipula lo siguiente: "No existe ninguna disposición en el presente Acuerdo que prescriba o limite la cantidad que el Registrador pueda facturar a los Titulares de Nombres Registrados en concepto de la registración de Nombres Registrados.

14.3. Se debería consultar a los posibles usuarios del SSAD, según se determine en base a la implementación del proceso de acreditación y los Proveedores de identidad que se utilicen, para establecer las tarifas de uso del SSAD. En particular, los potenciales solicitantes del SSAD que no forman parte de la comunidad de la ICANN deben tener la oportunidad de presentar sus comentarios e interactuar con el IRT. Estos aportes deberían ayudar a informar las deliberaciones del IRT sobre este tema.

14.4. El SSAD NO DEBERÍA ser considerado como una plataforma para generar ganancias para la ICANN o las partes contratadas. La financiación del SSAD debería ser suficiente para cubrir los costos, incluidos los subcontratistas, a un valor de mercado justo y para establecer un fondo de riesgo jurídico.[39] Es fundamental asegurar que todo pago en el SSAD esté relacionado con los costos operativos y no sea simplemente un intercambio de dinero por datos de registración sin carácter público.

14.5. En relación con el marco de acreditación:

- 14.5.1. Se DEBE cobrar a los solicitantes de acreditación una tarifa no reembolsable a determinar que sea proporcional al costo de la validación de una solicitud, excepto en determinadas circunstancias en que se podrá eximir de esas tarifas, o se podrán fijar en cero, para determinados tipos o categorías de solicitantes que DEBERÍAN definirse con mayor detalle durante la fase de implementación.
- 14.5.2. Los solicitantes rechazados PUEDEN volver a presentar una solicitud, pero las nuevas solicitudes PUEDEN ser objeto de la aplicación de la tarifa de solicitud.
- 14.5.3. Las tarifas serán establecidas por la autoridad de acreditación. Si la Autoridad de acreditación terceriza la función de Proveedor de identidad, el Proveedor de identidad PUEDE establecer sus propias tarifas después de consultar a la Autoridad de acreditación.
- 14.5.4. Los usuarios y organizaciones acreditados DEBEN renovar su acreditación de forma periódica.

Pautas para la implementación

14.6. El Equipo responsable del EPDP prevé que los costos de desarrollo, despliegue y puesta en funcionamiento del sistema, al igual que para la implementación de otras recomendaciones de políticas adoptadas, sean sufragados inicialmente por la organización de la ICANN,[40] las Partes contratadas y otras partes que puedan estar

[39] Habida cuenta de la posibilidad de incertidumbre jurídica y del mayor riesgo jurídico y operativo que corren todas las partes incluidas en el suministro del SSAD, la creación de un fondo para riesgos jurídicos se refiere a la creación de un plan de contingencia jurídico adecuado, que incluya, entre otras cosas, una cobertura de seguro apropiada y cualquier otra medida apropiada que se considere suficiente para cubrir las posibles multas reglamentarias o costos jurídicos relacionados.

[40] Consulte también los aportes que la Organización de la ICANN proporcionó a solicitud del Equipo responsable del EPDP en relación con el costo estimado para la propuesta de un Sistema Estandarizado de Acceso/Divulgación (véase https://community.icann.org/x/GIIEC)

involucradas.[41] Como parte de la puesta en marcha del SSAD, se prevé que la organización de la ICANN considere la posibilidad de aprovechar los mecanismos existentes o utilizar un proceso de RFP para reducir los costos, en lugar de crear el SSAD y sus componentes desde cero. El Equipo responsable del EPDP prevé que el SSAD genere, en última instancia, costos iguales o inferiores para las Partes contratadas en comparación con la recepción y revisión manual de las solicitudes como medida de factibilidad comercial y técnica.

14.7. Se prevé que el funcionamiento posterior del sistema se realice sobre la base de la recuperación de costos, de modo que se puedan considerar los costos históricos[42]. Por ejemplo, los costos relacionados con la acreditación serían sufragados por quienes la soliciten. De manera similar, algunos de los costos de funcionamiento del SSAD DEBERÍAN compensarse mediante el cobro de tarifas a los usuarios del SSAD.

14.8. Al implementar y poner en funcionamiento el SSAD, se debería evitar una carga desproporcionadamente alta para los operadores de menor tamaño.

14.9. El Equipo responsable del EPDP reconoce que las tarifas asociadas con el uso del SSAD pueden diferir para los usuarios en función del volumen de solicitudes o el tipo de usuario, entre otros posibles factores. El Equipo responsable del EPDP también reconoce que los gobiernos pueden estar sujetos a ciertas restricciones de pago, que deberían tenerse en cuenta como parte de la implementación.

14.10. La estructura tarifaria y el período de renovación se determinarán en la fase de implementación, siguiendo los principios mencionados anteriormente. El Equipo responsable del EPDP reconoce que puede que no sea posible establecer las tarifas exactas hasta que se conozcan los costos reales. El Equipo responsable del EPDP también reconoce que la estructura tarifaria del SSAD puede necesitar una revisión con el transcurso del tiempo.

Recommendation #15. Registro

15.1. El Equipo responsable del EPDP recomienda que DEBEN establecerse los procedimientos de registro apropiados para facilitar los procedimientos de auditoría descritos en estas recomendaciones. Estos requisitos de registro cubrirán lo siguiente:

- Autoridad de acreditación
- Administrador de la puerta de enlace central
- Proveedor de identidad

[41] Para mayor claridad, la organización de la ICANN afrontará sus propios costos para el desarrollo del sistema. Las Partes contratadas serán responsables de sus propios costos.
[42] El término "costos históricos" se refiere a los costos de desarrollo, despliegue y puesta en funcionamiento del sistema.

- Partes Contratadas
- Actividad de usuarios acreditados, como intentos de acceso, consultas
- Qué consultas y decisiones de divulgación se realizan

15.2. El Equipo responsable del EPDP recomienda lo siguiente:

15.2.1. El Administrador de la puerta de enlace central DEBE elaborar registros de todas las actividades de todas las entidades que interactúen con el Administrador de la puerta de enlace central (para obtener más detalles, ver a continuación).

15.2.2. Los registros DEBEN incluir todas las consultas y todos los elementos necesarios para auditar cualquier decisión tomada en el contexto del SSAD.

15.2.3. Los registros DEBEN conservarse durante un período suficiente para los fines de auditoría y resolución de reclamos, y se debe tener en cuenta los límites legales relacionados con los reclamos contra el responsable del tratamiento de datos.

15.2.4. Los registros NO DEBERÍAN contener ninguna información personal. Si se registra cualquier información que contenga información personal, es necesario establecer las medidas de protección adecuadas. Los registros PUEDEN utilizarse para los informes de transparencia, que pueden ponerse a disposición del público. (Véase también la recomendación 17 sobre requisitos de informes). Los datos registrados que contengan información personal DEBEN ser confidenciales.

15.2.5. Los registros DEBEN conservarse en un formato comúnmente utilizado,[43] legible por computadoras, acompañado de una descripción inteligible de todas las variables.

15.2.6. Los datos registrados pertinentes DEBEN divulgarse, cuando esté permitido legalmente, en las siguientes circunstancias:

- En caso de reclamo por uso indebido, se podrán solicitar registros para su examen por una autoridad de acreditación o un proveedor de servicios de resolución de disputas.
- Los registros deberían estar también disponibles para la ICANN y el organismo de auditoría.
- Cuando así lo exija el debido proceso legal, incluidas las autoridades reguladoras y de aplicación de la ley pertinentes, según corresponda.

15.2.7. Los datos registrados pertinentes pueden ser divulgados para:

- la operativa técnica general para asegurar el buen funcionamiento del sistema.

15.2.8. Los registros pertinentes deberían utilizarse como fuente para poner a disposición cualquier dato pertinente. Estos datos deberían

[43] Para mayor claridad, "comúnmente" se refiere a un formato que es utilizado por muchos, en contraposición a un formato uniforme para todos.

permitir a los Solicitantes y a las Partes contratadas revisar sus propias estadísticas.

15.3. Como mínimo, los siguientes eventos DEBEN ser registrados:

- Registro relacionado con el Proveedor de identidad[44]
- Registro relacionado con la Autoridad de acreditación
    - Detalles de las solicitudes de acreditación recibidas
    - Resultados del procesamiento de las solicitudes de acreditación, por ejemplo, expedición de la Credencial de identificación o motivos de denegación
    - Detalles de las solicitudes de revocación
    - Indicación de cuándo se han validado las Credenciales de identificación y las Declaraciones firmadas.
    - Número de referencia único
- Registro relacionado con el Administrador de la puerta de enlace central
    - Información relacionada con el contenido de la propia consulta.
    - Resultados del procesamiento de la consulta, incluidos los cambios de estado (por ejemplo, recibida, pendiente, en trámite, denegada, aprobada, aprobada con cambios)
    - Tarifas de:
        - divulgación y no divulgación;
        - uso de cada motivo de denegación para la no divulgación;
        - divergencia entre las decisiones de divulgación y no divulgación de una Parte contratada y las recomendaciones de la puerta de enlace central.

Registro relacionado con las Partes contratadas

- Detalles de la respuesta a las solicitudes, por ejemplo, el motivo de la denegación, la notificación de la aprobación y los campos de datos divulgados. Las decisiones de divulgación, incluido el motivo de negación, se deben almacenar.

Recommendation #16. Auditorías

16.1. El Equipo responsable del EPDP recomienda que se DEBEN establecer los procesos y procedimientos de auditorías apropiados para garantizar el monitoreo y el cumplimiento adecuados de los requisitos descritos en estas recomendaciones.

16.2. Como parte de cualquier auditoría, el auditor DEBE estar sujeto a obligaciones razonables de confidencialidad con respecto a los procesos de propiedad y la información personal divulgada durante la auditoría.

Más específicamente:

44 Se incluirán más detalles en la fase de implementación.

Auditorías de la Autoridad de acreditación

16.3. Si la ICANN terceriza la función de autoridad de acreditación a un tercero cualificado, la autoridad de acreditación DEBE ser auditada periódicamente para garantizar el cumplimiento de los requisitos de la política que se definen en la recomendación de acreditación. Si se descubre que la Autoridad de acreditación ha incumplido la política y los requisitos de acreditación, se le dará la oportunidad de subsanar el incumplimiento, pero en los casos de faltas de auditoría o incumplimientos reiterados, se deberá identificar o crear una nueva Autoridad de acreditación. La organización de la ICANN como Autoridad de acreditación no está obligada a auditar a las entidades gubernamentales, cuyos requisitos de acreditación y auditoría están definidos en la Recomendación 2.

16.4. Toda auditoría de la autoridad de acreditación DEBE adaptarse a los fines de evaluar el cumplimiento, y el auditor DEBE notificar con antelación razonable cualquier auditoría de ese tipo, en cuya notificación se especificarán con razonable detalle las categorías de documentos, datos y demás información solicitada.

16.5. Como parte de dichas auditorías, la autoridad de acreditación DEBE proporcionar al auditor, de manera oportuna, todos los documentos pertinentes, datos y cualquier otra información necesaria para demostrar el cumplimiento de la política de acreditación.

16.6. Si la ICANN actúa como autoridad de acreditación, se prevé que los mecanismos de responsabilidad existentes aborden cualquier incumplimiento de la política de acreditación, teniendo en cuenta que, en un caso tan extremo, se revisarán las credenciales expedidas durante el tiempo del incumplimiento. Las modalidades de esta revisión DEBERÍAN establecerse en la fase de implementación.

Auditorías del Proveedor de identidad

16.7. Los Proveedores de identidad DEBEN ser auditados periódicamente para asegurar el cumplimiento de los requisitos de la política, tal como se define en la recomendación de acreditación. Si se descubre que el Proveedor de identidad ha incumplido la política y los requisitos de acreditación, se le dará la oportunidad de subsanar el incumplimiento, pero en los casos de faltas de auditoría o incumplimientos reiterados, se deberá identificar un nuevo Proveedor de identidad.

16.8. Toda auditoría de un Proveedor de identidad DEBE adaptarse a los fines de evaluar el cumplimiento, y el auditor DEBE notificar con antelación razonable cualquier

auditoría de ese tipo, en cuya notificación se especificarán con razonable detalle las categorías de documentos, datos y demás información solicitada.

16.9. Como parte de dichas auditorías, el Proveedor de identidad DEBE proporcionar al auditor, de manera oportuna, todos los documentos pertinentes, datos y cualquier otra información necesaria para demostrar el cumplimiento de la política de acreditación.

Auditorías de personas/entidades acreditadas

16.10. En la fase de implementación, DEBEN desarrollarse mecanismos apropiados para garantizar el cumplimiento por parte de las personas y entidades acreditadas de los requisitos de la política definidos en las recomendaciones de acreditación 1 y 2. Entre ellas, podrían figurar, por ejemplo, las auditorías que tengan su origen en denuncias verificadas, las auditorías aleatorias o las auditorías en respuesta a una autocertificación o autoevaluación. Si se descubre que la persona o entidad acreditada ha incumplido la política y los requisitos de acreditación, se le dará la oportunidad de subsanar el incumplimiento, pero en los casos de faltas de auditoría o incumplimientos reiterados, la cuestión debería remitirse a la Autoridad de acreditación y/o al Proveedor de identidad, según corresponda, para que adopten medidas.

16.11. Toda auditoría de personas/entidades acreditadas DEBE adaptarse a los fines de evaluar el cumplimiento, y el auditor DEBE notificar con antelación razonable cualquier auditoría de ese tipo, en cuya notificación se DEBE especificar con razonable detalle las categorías de documentos, datos y demás información solicitada.

16.12. Como parte de dichas auditorías, las personas/entidades acreditadas DEBEN proporcionar al auditor, de manera oportuna, todos los documentos pertinentes, datos y cualquier otra información necesaria para demostrar el cumplimiento de la política de acreditación.

Recommendation #17. Requisitos de informes

17.1. El Equipo responsable del EPDP recomienda que la organización de la ICANN DEBE establecer informes públicos periódicos sobre el uso y funcionamiento del SSAD. A los efectos de evitar dudas, esta recomendación no pretende impedir que la organización de la ICANN realice informes adicionales sin carácter público para los usuarios del SSAD.

17.2. Dentro un plazo no anterior a 3 meses y no posterior a 9 meses después de la puesta en marcha del SSAD, la organización de la ICANN DEBE publicar un Informe de

estado o tablero de control del SSAD, y continuar haciéndolo de forma trimestral, en el que se incluirá, como mínimo, lo siguiente:

- Cantidad de solicitudes de divulgación recibidas
- Promedios de tiempo de respuesta a las solicitudes de divulgación, clasificados por nivel de prioridad
- Cantidad de solicitudes clasificadas según los fines/justificaciones de terceros (como se indica en la recomendación 4)
- Cantidad de solicitudes de divulgación aprobadas y denegadas
- Cantidad de solicitudes de divulgación automatizadas
- Cantidad de solicitudes procesadas manualmente
- Información sobre la sostenibilidad financiera del SSAD
- Nuevas directrices del EDPB o nueva jurisprudencia temática (si procede)
- Dificultades técnicas o del sistema
- Mejoras operativas y del sistema

Pautas para la implementación:

17.3. El Equipo responsable del EPDP recomienda que, durante la implementación, se sigan considerando los siguientes aspectos:

- La frecuencia de presentación de informes públicos. Una presentación trimestral de informes públicos se consideraría razonable.
- Los datos que se deben notificar, que se prevé que incluyan información como: a) cantidad de solicitudes de divulgación; b) solicitudes de divulgación por categoría de Solicitantes; c) solicitudes de divulgación por Solicitante (para entidades jurídicas); solicitudes de divulgación concedidas / denegadas, y; tiempos de respuesta. Tenga en cuenta que esta no es una lista exhaustiva.
- Mecanismo para la presentación de informes públicos - considerar la posibilidad de un tablero de control a disposición del público en lugar de o además de los informes que se publican.
- Necesidad de una posible confidencialidad en ciertos casos, como la información sobre personas físicas y las solicitudes de LEA. Se podría considerar la posibilidad de utilizar datos agregados o seudónimos para abordar posibles problemas de confidencialidad.

Recommendation #18. Revisión de la implementación de las recomendaciones de políticas relativas al SSAD mediante un Comité Permanente de la GNSO

18.1. El Equipo responsable del EPDP recomienda que el Consejo de la GNSO DEBE establecer un Comité Permanente de la GNSO para evaluar los problemas operativos del SSAD que surjan como resultado de las Políticas de Consenso de

la ICANN adoptadas y/o su implementación. El Comité Permanente de la GNSO tiene por objeto examinar los datos que se producen como consecuencia de las operaciones del SSAD y proporcionar al Consejo de la GNSO recomendaciones sobre la mejor manera de realizar cambios operativos en el SSAD, que sean estrictamente medidas de implementación, además de recomendaciones basadas en la revisión de las repercusiones que las Políticas de consenso existentes tengan en las operaciones del SSAD.

18.2. El Equipo responsable del EPDP también recomienda que el Consejo de la GNSO utilice los siguientes principios como base para que el Comité Permanente de la GNSO lleve a cabo su misión, que debe reflejarse en su carta orgánica:

18.2.1 Composición: la composición del Comité Permanente de la GNSO será representativa de los Comités Asesores de la ICANN y de las Unidades constitutivas y Grupos de Partes Interesadas de la GNSO representados en el actual Equipo responsable del EPDP sobre la Especificación Temporaria para los Datos de Registración de los gTLD. Esta composición incluirá al menos un miembro del GAC, ALAC, SSAC, RySG, RrSG, NCSG, IPC, BC e ISPCP, así como al menos un miembro suplente de cada grupo. Nota: la cantidad de miembros por grupo no debería afectar al proceso de designación por consenso, dado que se prevé que las posiciones se consideren por grupo y no a nivel de miembro individual. El Consejo de la GNSO también puede considerar la posibilidad de invitar a coordinadores de enlace de la organización de la ICANN como miembros del Comité Permanente de la GNSO.

18.2.2. Alcance: el Consejo de la GNSO debe elaborar una carta orgánica junto con los Comités Asesores, por ejemplo, el GAC, el SSAC y el ALAC para el Comité Permanente de la GNSO. La Carta orgánica debe permitir que el Comité se ocupe de cualquier cuestión operacional relacionada con el SSAD. Esto puede incluir, entre otros, temas como los Acuerdos de Nivel de Servicio (SLA), centralización/descentralización, automatización, propósitos de terceros, sostenibilidad financiera y mejoras operativas / del sistema. El umbral para aceptar que un tema figure en la agenda del Comité Permanente de la GNSO será lo suficientemente bajo como para permitir que cualquiera de los grupos que participen pueda hacer que sus intereses en las operaciones del SSAD sean considerados seriamente por el Comité. La identificación de las cuestiones que el Comité pueda abordar se determinará mediante los dos métodos siguientes:

i. Cualquier tema de política o implementación relativo a las operaciones del SSAD podrá ser planteado por un miembro del Comité Permanente de la GNSO y se incluirá en la agenda de trabajo

del Comité si es secundado por al menos otro miembro del Comité del "grupo".

ii. Además, el Consejo de la GNSO puede identificar problemas operacionales del SSAD. El Consejo de la GNSO puede optar por encargar al Comité Permanente de la GNSO la evaluación de los problemas que identifique, a fin de que el Comité proporcione al Consejo recomendaciones consensuadas de las partes interesadas afectadas sobre la mejor manera de abordarlos.

Las recomendaciones relativas a las pautas para la implementación se enviarán al Consejo de la GNSO para su consideración y adopción, después de lo cual se enviarán a la Organización de la ICANN para continuar con el trabajo de implementación. Las recomendaciones que requieran la introducción de cambios en las Políticas de consenso existentes de la ICANN se registrarán y mantendrán, para ser utilizadas en la fase de determinación del alcance de los problemas en el desarrollo y/o revisión de políticas futuras.

18.2.3. Consenso requerido: nivel de consenso para las recomendaciones del Comité Permanente de la GNSO: las recomendaciones sobre las operaciones del SSAD y políticas elaboradas por el Comité Permanente deben lograr el consenso de los miembros del Comité para ser enviadas como recomendaciones formales al Consejo de la GNSO. Para que las recomendaciones logren una designación consensuada, se requerirá el apoyo de las Partes contratadas. A los efectos de evaluar el nivel de consenso, los Miembros deben representar la posición formal de su grupo de partes interesadas/unidad constitutiva u organización de apoyo/comité asesor, no las opiniones o posiciones individuales. A los efectos de determinar el nivel de consenso, cada uno de los nueve grupos que lo componen debe tener igual peso, con sujeción al requisito de que las Partes contratadas deben apoyar las recomendaciones específicas.

18.2.4. Disolución del Comité Permanente de la GNSO: El Comité Permanente puede recomendar al Consejo de la GNSO que el propio Comité se disuelva, si fuera necesario. Para que el Comité Permanente recomiende al Consejo de la GNSO su disolución, se requiere el voto afirmativo de una mayoría simple de los grupos involucrados. Esta recomendación tendría que ser adoptada posteriormente por el Consejo de la GNSO.

3.6 Recomendaciones de prioridad 2 del Equipo responsable del EPDP

Recommendation #19. Visualización de información de proveedores de servicios de privacidad/representación afiliados y/o acreditados

19.1. En el caso de una registración de nombre de dominio en la que se utiliza un servicio de privacidad/representación afiliado y/o acreditado, por ejemplo, en el que se enmascaran los datos asociados a una persona física, el Registrador (y el Registro, según corresponda) DEBE incluir los datos completos del RDDS del servicio de privacidad/representación correspondiente en respuesta a una consulta del RDDS. Los datos completos del RDDS de privacidad/representación también pueden incluir un correo electrónico en el que se haya utilizado un seudónimo.

Notas de implementación:
19.2. Una vez que la organización de la ICANN haya implementado un programa de acreditación de servicios de privacidad/proxy, esta recomendación 19, una vez que entre en vigencia, reemplazará o sustituirá de otra manera la recomendación 14 de la Fase 1 del EPDP.
19.3. La intención de esta recomendación es proporcionar instrucciones claras a los registradores (y a los registros, según corresponda) para que cuando una registración de dominio se realice a través de un proveedor de servicios de privacidad/proxy afiliado y/o acreditado, esos datos NO DEBEN censurarse tampoco. El grupo de trabajo tiene la intención de establecer que los datos de registración de los dominios NO DEBEN censurarse ni ocultarse mediante servicios de privacidad/proxy.

Recommendation #20. Campo que especifica la ciudad

El Equipo responsable del EPDP recomienda que se actualice la recomendación 11 de la Fase 1 del EPDP para establecer que la censura PUEDE aplicarse al campo que especifica la ciudad en referencia a la información de contacto del registratario, en lugar de DEBE.

Recommendation #21. Retención de datos

El Equipo responsable del EPDP confirma su recomendación de la Fase 1 que señala que los registradores DEBEN retener únicamente los elementos de datos que se consideren necesarios a los efectos de la TDRP, durante un período de quince meses posteriores a la vigencia del registro más tres meses para implementar la eliminación, es decir, 18 meses. Esta retención se basa en la estipulación de la política establecida en la TDRP que establece que los reclamos en virtud de la política pueden plantearse únicamente durante un período de 12 meses después del presunto incumplimiento (nota al pie: véase la sección 2.2 de la TDRP) de la Política de Transferencia (nota al pie: véase la sección 1.15 de la TDRP). Para mayor claridad, esto no impide que los Solicitantes, incluido el departamento de Cumplimiento de la ICANN, soliciten la divulgación de estos elementos de datos retenidos para otros fines que no estén relacionados con la TDRP, pero la divulgación de los mismos estará sujeta a las leyes de

protección de datos pertinentes, por ejemplo, si existe un fundamento legal para la divulgación. A los efectos de evitar dudas, este período de retención no restringe la capacidad de los registros y registradores de retener elementos de datos durante períodos más prolongados.

Pautas para la implementación:
A los efectos de evitar dudas, los registradores deben mantener los datos durante 15 meses después de la vigencia del registro y PUEDEN eliminarlos después de ese período de 15 meses.

Para mayor claridad, esto no impide la identificación de períodos de retención adicionales para los fines declarados por los responsables del tratamiento de datos, que identifiquen y establezcan los responsables del tratamiento de datos, para fines distintos de la TDRP; esto no excluye la posible divulgación de dichos datos retenidos a cualquier parte, con sujeción a las leyes pertinentes de protección de datos.

Recommendation #22. Propósito 2
El Equipo responsable del EPDP recomienda que se agregue el siguiente propósito a los propósitos de la Fase 1 de dicho equipo, que constituyen la base de la nueva política de la ICANN:

- Contribuir al mantenimiento de la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio de acuerdo con la misión de la ICANN.

3.7 Conclusiones de prioridad 2 del Equipo responsable del EPDP

Conclusión – Propósito de la OCTO
Tras haber considerado este aporte, la mayoría de los miembros del Equipo responsable del EPDP estuvieron de acuerdo en que en esta etapa no hay necesidad de proponer un propósito o propósitos adicionales para facilitar a la Oficina del Director de Tecnologías (OCTO) de la ICANN el cumplimiento de su misión. El motivo de este acuerdo se debe a que el recientemente actualizado Propósito 2 de la ICANN cubre suficientemente el trabajo de la OCTO, junto con el trabajo de otros equipos de la organización de la ICANN, como el de Cumplimiento Contractual, entre otros. La mayoría también estuvo de acuerdo en que la decisión del Equipo responsable del EPDP de abstenerse de proponer uno propósito o propósitos adicionales no impediría que la organización y/o la comunidad de la ICANN identificara propósitos adicionales para apoyar actividades futuras no identificadas que pudieran requerir el acceso a datos de registración sin carácter público.

Conclusión – Exactitud y Sistema de Informes sobre la Exactitud de WHOIS
De acuerdo con las instrucciones del Consejo de la GNSO, el Equipo responsable del EPDP no seguirá examinando este tema; en cambio, se prevé que el Consejo de la GNSO forme un equipo de estudio para explorar más a fondo las cuestiones

relacionadas con la exactitud y el ARS para ayudar a fundamentar una decisión sobre los próximos pasos apropiados para abordar las posibles cuestiones identificadas.

4 Próximos pasos

4.1 Próximos pasos

Este Informe Final será presentado al Consejo de la GNSO para su consideración y aprobación. Si el Consejo de la GNSO lo adopta, el Informe Final se remitirá a la Junta Directiva de la ICANN para su consideración y, potencialmente, su aprobación como Política de Consenso de la ICANN.

Glosario

1. Comité Asesor
Un Comité Asesor es un órgano formal de carácter consultivo integrado por representantes de la comunidad de Internet para asesorar a la ICANN sobre una cuestión o área de política en particular. Varios se rigen por los Estatutos de la ICANN y es posible crear otros según sea necesario. Los Comités Asesores no tienen la facultad legal de actuar en representación de la ICANN, sino que deben comunicar sus conclusiones y presentar recomendaciones a la Junta Directiva de la ICANN.

2. ALAC - Comité Asesor At-Large
El Comité Asesor At-Large (ALAC) de la ICANN tiene a su cargo la tarea de considerar y de brindar asesoramiento sobre las actividades de la ICANN, en la medida en que se relacionen con los intereses de los usuarios individuales de Internet en general (la comunidad "At-Large"). La ICANN es una corporación privada y sin fines de lucro, cuya responsabilidad comprende la gestión técnica del sistema de direcciones y nombres de dominio de Internet. En tal sentido, la ICANN cuenta con el ALAC y su infraestructura de apoyo para que los intereses de los usuarios individuales de Internet sean incluidos y estén ampliamente representados.

3. Unidad Constitutiva de Negocios
La Unidad Constitutiva de Negocios representa a los usuarios comerciales de Internet. La Unidad Constitutiva de Negocios es una de las unidades constitutivas dentro del Grupo de Partes Interesadas Comerciales (CSG) al cual se hace referencia en el Artículo 11.5 de los Estatutos de la ICANN. La Unidad Constitutiva de Negocios es uno de los grupos de partes interesadas y unidades constitutivas de la Organización de Apoyo para Nombres Genéricos (GNSO) a cargo de la responsabilidad de asesorar a la Junta Directiva de la ICANN sobre cuestiones de política relativas a la gestión del Sistema de Nombres de Dominio.

4. ccNSO - Organización de Apoyo para Nombres de Dominio con Código de País
La ccNSO es la organización de apoyo que se encarga de desarrollar y recomendar a la Junta Directiva de la ICANN políticas globales en relación con los nombres de dominio de alto nivel con código de país (ccTLD). Es un foro en el cual los administradores de dominios de alto nivel con código de país se reúnen y debaten inquietudes desde una perspectiva global. La ccNSO designa a una persona para desempeñarse en la Junta Directiva.

5. ccTLD - Dominio de Alto Nivel con Código de País
Los ccTLD son dominios de dos letras, por ejemplo, .UK para Reino Unido, .DE para Alemania y .JP para Japón; se denominan dominios de alto nivel con código de país (ccTLD) y corresponden a un país, territorio u otra denominación geográfica. Las reglas y políticas para el registro de nombres de dominio en los ccTLD varían

considerablemente, y los Registros de ccTLD circunscriben el uso del ccTLD a los ciudadanos del país correspondiente.

Para más información sobre los ccTLD, consulte: http://www.iana.org/cctld/cctld.htm. El sitio incluye una base de datos completa de los ccTLD y administradores designados.

6. Datos de registración de nombres de dominio
Los datos de registración de nombres de dominio, también denominados datos de registración, se refiere a la información que los registratarios suministran al registrar un nombre de dominio y que los Registradores o Registros recaban. Parte de esta información se encuentra disposición del público. En lo que respecta a la interacción entre los Registradores de Dominios Genéricos de Alto Nivel (gTLD) acreditados por la ICANN y los registratarios, los datos se indican en el RAA actualmente vigente. Para los Dominios de Alto Nivel con Código de País (ccTLD), los operadores de estos TLD determinan sus propios datos, o bien acatan la política de sus respectivos gobiernos sobre la solicitud de divulgación y la visualización de la información de los registratarios.

7. Nombre de dominio
Dentro del Sistema de Nombres de Dominio, los nombres de dominio identifican recursos del Protocolo de Internet, como un sitio web en Internet.

8. DNS - Sistema de Nombres de Dominio
DNS se refiere al Sistema de Nombres de Dominio de Internet. El Sistema de Nombres de Dominio (DNS) ayuda a los usuarios a ubicarse en Internet. Cada computadora en Internet tiene una dirección única, comparable a un número telefónico, que consiste en una secuencia numérica bastante complicada. Recibe el nombre de "dirección IP" (IP significa "Protocolo de Internet"). Las direcciones IP son difíciles de recordar. El DNS facilita el uso de Internet ya que permite visualizar una cadena de letras (el "nombre de dominio") que resulta más familiar que la dirección arcana de IP. De este modo, en lugar de ingresar 207.151.159.3, usted puede ingresar www.internic.net. Esto es un recurso nemotécnico que hace que las direcciones sean más fáciles de recordar.

9. EPDP - Proceso Expeditivo de Desarrollo de Políticas
Conjunto de pasos formales, definidos en los estatutos de la ICANN, para guiar el inicio, la revisión interna y externa, los plazos y la aprobación de las políticas necesarias para coordinar el sistema de identificadores únicos de Internet. Un EPDP puede ser iniciado por el Consejo de la GNSO sólo en las siguientes circunstancias específicas: (1) para hacer frente a un asunto de política en el sentido estricto, que haya sido identificado y cuyo alcance haya sido establecido ya sea después de la adopción de una recomendación de política de la GNSO por parte de la Junta Directiva de la ICANN, o de la implementación de una recomendación adoptada; o (2) para brindar recomendaciones de política nuevas o adicionales sobre un asunto de política específico cuyo alcance haya sido previamente establecido en forma tal que ya exista

mucha información de referencia relevante; por ejemplo: (a) un Informe de cuestiones para un posible PDP que no se inició; (b) como parte de un PDP anterior que no se completó; o (c) a través de otros proyectos tales como un Proceso de Orientación de la GNSO (GGP).

10. GAC: Comité Asesor Gubernamental
El GAC es un comité asesor integrado por representantes de gobiernos nacionales, organizaciones intergubernamentales, organizaciones que se rigen por tratados y economías diferenciadas. Su función es la de asesorar a la Junta Directiva de la ICANN sobre temas que preocupan a los gobiernos. El GAC es un foro de debate de los temas que interesan y preocupan a los gobiernos, entre ellos, los intereses de los consumidores. Como comité asesor, el GAC no tiene autoridad legal para actuar en representación de la ICANN, pero presenta sus conclusiones y recomendaciones a la Junta Directiva de la ICANN.

11. Reglamento General de Protección de Datos (GDPR)
El Reglamento General sobre la Protección de Datos (UE) 2016/679 (GDPR) es un reglamento de la legislación de la Unión Europea sobre protección de datos y privacidad para todas las personas dentro de la Unión Europea (UE) y el Espacio Económico Europeo (EEE). También aborda la exportación de datos personales fuera de las áreas de la UE y EEE.

12. GNSO - Organización de Apoyo para Nombres Genéricos
La GNSO es la organización de apoyo responsable de desarrollar y recomendar políticas sustanciales en relación con los dominios genéricos de alto nivel a la Junta Directiva de la ICANN. Sus miembros incluyen representantes de los Registros de gTLD, los Registradores de gTLD, intereses de propiedad intelectual, proveedores de servicio de Internet, empresas e intereses no comerciales.

13. Dominios genéricos de alto nivel (gTLD)
“gTLD” se refiere los dominios de alto nivel del DNS delegados por la ICANN en virtud de un acuerdo de registro que se encuentra en plena vigencia, a excepción de cualquier TLD con código de país (ccTLD) o TLD con código de país de nombres de dominio internacionalizados (IDN).

14. Grupo de Partes Interesadas de Registros (RySG)
El Grupo de Partes Interesadas de Registros de gTLD (RySG) es una entidad reconocida dentro de la Organización de Apoyo para Nombres Genéricos (GNSO), conformada en virtud del Artículo X, Sección 5 (septiembre de 2009) de los Estatutos de la Corporación para la Asignación de Nombres y Números en Internet (ICANN).

El rol principal del RySG es representar los intereses de los Operadores de Registro de gTLD (o patrocinadores en el caso de los gTLD patrocinados) ("Registros") (i) que se encuentran bajo contrato vigente con la ICANN para suministrar servicios de registro

de gTLD, como apoyo para uno o más dominios de alto nivel (gTLD); (ii) que acuerdan, en dicho contrato, su vinculación obligatoria a las políticas de consenso; y (iii) que eligen, en forma voluntaria, ser miembros del RySG. El RySG puede incluir Grupos de Interés, en conformidad con lo establecido en el Artículo IV. El RySG representa las opiniones del RySG ante el Consejo de la GNSO y a la Junta Directiva de la ICANN, con especial énfasis en las políticas de consenso de la ICANN relacionadas con la interoperabilidad, la fiabilidad técnica y el funcionamiento estable de Internet o del Sistema de Nombres de Dominio.

15. ICANN - Corporación para la Asignación de Nombres y Números en Internet
La Corporación para la Asignación de Nombres y Números en Internet (ICANN) es una corporación internacional sin fines de lucro responsable de la asignación del espacio de direcciones de Protocolo de Internet (IP), la asignación de identificadores de protocolo, la administración del sistema de nombres de dominio genéricos de alto nivel (gTLD) y de dominios de alto nivel con código de país (ccTLD), y las funciones de administración del sistema del servidor raíz. Originariamente, la Autoridad para Números Asignados en Internet (IANA) y otras entidades prestaban estos servicios en virtud de un contrato con el gobierno de los Estados Unidos. Actualmente, la ICANN desempeña las funciones de la IANA. Como asociación privada-pública, la ICANN está dedicada a preservar la estabilidad operativa de Internet; promover la competencia; lograr una amplia representación de las comunidades mundiales de Internet; y elaborar políticas adecuadas a su misión a través de un proceso participativo y basado en el consenso.

16. Unidad Constitutiva de Propiedad Intelectual (IPC)
La Unidad Constitutiva de Propiedad Intelectual (IPC) representa las opiniones y los intereses de la comunidad de propiedad intelectual en todo el mundo, con especial énfasis en las marcas comerciales, los derechos de autor y derechos de propiedad intelectual relacionados, y sus efectos e interacción con el Sistema de Nombres de Dominio (DNS). La IPC es una de las unidades constitutivas de la Organización de Apoyo para Nombres Genéricos (GNSO) a cargo de la responsabilidad de asesorar a la Junta Directiva de la ICANN sobre cuestiones de política relativas a la gestión del Sistema de Nombres de Dominio.

17. Unidad Constitutiva de Proveedores de Servicios de Internet y Conectividad (ISPCP)
La Unidad Constitutiva de Proveedores de Servicios de Internet (ISP) y Conectividad es una unidad constitutiva de la GNSO. El objetivo de la Unidad Constitutiva es cumplir con los roles y responsabilidades que se crean mediante los estatutos, reglas o políticas relevantes de la ICANN y la GNSO, a medida que la ICANN procede a concluir sus actividades organizacionales. El ISPCP garantiza que las opiniones de los Proveedores de Servicios de Internet y Servicios de Conectividad contribuyan a cumplir los objetivos y metas de la ICANN.

18. Servidor de nombre

Un servidor de nombre es un componente del DNS que almacena información sobre una o más zonas del espacio de nombres del DNS.

19. Grupo de Partes Interesadas No Comerciales (NCSG)
El Grupo de Partes Interesadas No Comerciales (NCSG) es un grupo de partes interesadas dentro de la GNSO. El propósito del Grupo de Partes Interesadas No Comerciales (NCSG) es representar, a través de sus representantes electos y sus unidades constitutivas, los intereses y preocupaciones de los registratarios no comerciales y los usuarios de Internet no comerciales de dominios genéricos de alto nivel (gTLD). Proporciona una voz y representación en los procesos de la ICANN para: las organizaciones sin fines de lucro que sirven a intereses no comerciales; los servicios sin fines de lucro tales como educación, filantropías, protección al consumidor, organización comunitaria, promoción de las artes, defensa de políticas de interés público, bienestar de los niños, religión, investigación científica y derechos humanos; las preocupaciones de software de interés público; familias o individuos que registran nombres de dominio para uso personal no comercial; y los usuarios de Internet cuya inquietud principal es el aspecto no comercial y de interés público de las políticas de nombres de dominio.

20. Procedimiento para la Resolución de Disputas con Posterioridad a la Delegación (PDDRP)
Los Procedimientos para la Resolución de Disputas con Posterioridad a la Delegación fueron desarrollados para que aquellos perjudicados por la conducta de un Operador de Registro de nuevo gTLD cuenten con una vía para presentar su reclamo a causa de dicha conducta. Todos estos procedimientos de resolución de disputas son administrados por proveedores externos a la ICANN y requieren que las partes reclamantes sigan pasos específicos para abordar sus cuestiones antes de presentar un reclamo formal. Un panel de expertos determinará si un Operador de Registro está en falta y, de ser así, recomendará soluciones a la ICANN.
21. Nombres registrados
"Nombre registrado" se refiere a un nombre de dominio dentro del dominio de un gTLD que consiste en dos (2) o más niveles (p. ej., javier.cedillo.nombre) sobre los cuales un Operador de Registro de gTLD (o una filial o subcontratista del mismo comprometido en la prestación de servicios de Registro) mantiene datos en la Base de Datos del Registro, se encarga de su mantenimiento o deriva ingresos a partir de dicho mantenimiento. Un nombre en una Base de Datos del Registro puede ser un Nombre registrado, incluso si no figura en un archivo de zona (por ejemplo, un nombre registrado pero inactivo).

22. Registrador
La palabra "registrador", incluso cuando aparece sin la letra inicial mayúscula, se refiere a una persona física o jurídica que posee un contrato con Titulares de Nombres Registrados y con un Operador de Registro y que recopila los datos de registración a

partir de los Titulares de Nombres Registrados y remite la información de registración para ser ingresada en la Base de Datos del Registro.

23. Grupo de Partes Interesadas de Registradores (RrSG)
El Grupo de Partes Interesadas de Registradores es uno de los varios grupos de partes interesadas dentro de la comunidad de la ICANN y es el órgano representativo de los Registradores. Es un grupo diverso y activo que trabaja para garantizar que los intereses de los Registradores y sus clientes se alcancen de manera efectiva. Le invitamos a conocer más sobre los registradores de nombres de dominio acreditados y los roles importantes que desempeñan en el sistema de nombres de dominio.

24. Operador de Registro
Un "Operador de Registro" es la persona física o jurídica responsable al efecto, en virtud de un acuerdo entre la ICANN (o la persona que ésta designe) y esa persona física o jurídica (aquellas personas físicas o jurídicas) o, en caso de que ese acuerdo se haya rescindido o haya vencido, en virtud de un acuerdo entre el Gobierno de EE. UU. y esa persona física o jurídica (aquellas personas físicas o jurídicas) para prestar Servicios de Registro a un gTLD específico.

25. Servicio de Directorio de Datos de Registración de Nombres de Dominio (RDDS)
El Servicio de Directorio de Datos de Registración de Nombres de Dominio o RDDS se refiere a los servicios ofrecidos por los Registros y los Registradores para brindar acceso a los datos de registración de nombres de dominio.

26. Procedimiento para la resolución de disputas por restricciones de registro (RRDRP)
El Procedimiento de Resolución de Disputas por Restricción del Registro (RRDRP) tiene el objetivo de abordar circunstancias en las cuales un Operador de Registro de un nuevo gTLD basado en la comunidad no cumple con las restricciones en materia de registraciones según lo establecido en su Acuerdo de Registro.

27. SO - Organizaciones de Apoyo
Las SO son los tres órganos consultivos especializados que asesoran a la Junta Directiva de la ICANN sobre cuestiones relacionadas con nombres de dominio (GNSO y CCNSO) y direcciones de IP (ASO).

28. SSAC - Comité Asesor de Seguridad y Estabilidad
Comité asesor de la Junta Directiva de la ICANN compuesto por expertos técnicos de la industria y del mundo académico, así como por operadores de servidores raíz de Internet, registradores y registros de dominios de primer nivel.

29. TLD - Dominio de Alto Nivel
Los Dominios de Alto Nivel (TLD) son los nombres que encabezan la jerarquía de nombres del DNS. En los nombres de dominio, son la cadena de letras que aparece a la

derecha del último punto ".", por ejemplo, "net" en http://www.example.net. El administrador de un TLD controla qué nombres de segundo nivel son reconocidos en ese TLD. Los administradores del dominio raíz o de la zona raíz controlan los TLD reconocidos en el DNS. Los TLD más comunes son .com, .net, .edu, .jp, .de, etc.

30. Procedimiento Uniforme de Resolución de Disputas por Nombres de Dominio (UDRP)

La Política Uniforme de Resolución de Disputas por Nombres de Dominio (UDRP) especifica los procedimientos y las reglas que aplican los Registradores en relación con disputas planteadas en materia de registración y uso de nombres de dominio de gTLD. La UDRP proporciona un procedimiento administrativo obligatorio, principalmente para solucionar los reclamos por registraciones de nombres de dominio consideradas abusivas y de mala fe. Se aplica únicamente a disputas entre registratarios y terceros, no a disputas entre un Registrador y su cliente.

31. Sistema Uniforme de Suspensión Rápida (URS)

El Sistema Uniforme de Suspensión Rápida es un mecanismo de protección de derechos que complementa la Política Uniforme de Resolución de Disputas por Nombres de Dominio

(UDRP) existente, mediante la oferta de una vía menos costosa y más rápida para asistir a los titulares de derechos que estén experimentando los casos de incumplimiento más evidentes.

32. WHOIS

El protocolo de WHOIS es un protocolo de Internet utilizado para consultar bases de datos y obtener información sobre la registración de un nombre de dominio (o dirección IP). El protocolo de WHOIS fue inicialmente especificado en el documento RFC 954, publicado en 1985. Su especificación actual se encuentra en el documento RFC 3912. Los acuerdos de gTLD de la ICANN exigen que los Registros y los Registradores ofrezcan una página web interactiva y un servicio de WHOIS de puerto 43, con acceso público a los datos de los nombres registrados. Esos datos son comúnmente conocidos como “datos de WHOIS” e incluyen elementos como las fechas de creación y vencimiento de las registraciones de nombres de dominio, servidores de nombre, información de contacto del registratario y contactos administrativos y técnicos designados.

Por lo general, los servicios de WHOIS se utilizan para identificar a los titulares de nombres de dominio con fines comerciales, y a quienes puedan solucionar problemas técnicos relacionados con el dominio registrado.

Anexo A – Sistema Estandarizado de Acceso/Divulgación a datos de registración sin carácter público – Información de referencia

DESCRIPCIÓN DE CUESTIONES Y/O PREGUNTAS SOBRE LA CARTA ORGÁNICA

Por el Equipo responsable del EPDP:
(a) Propósitos para acceder a los datos: ¿Cuáles son las preguntas de política sin contestar que guiarán la implementación?

a1) En virtud del derecho aplicable, ¿cuáles son los fines legítimos de terceros para acceder a los datos de registración?
a2) ¿Qué fundamentos jurídicos existen para respaldar este acceso?
a3) ¿Cuáles son los criterios de elegibilidad para acceso a datos de registración no públicos?
a4) ¿Esas partes/grupos consisten en diferentes tipos de terceros Solicitantes?
a5) ¿Cuáles son los elementos de datos a los que cada usuario/parte debería tener acceso en base a sus propósitos?
a6) ¿En qué medida podemos determinar un conjunto de elementos de datos y el posible alcance (volumen) para terceros y/o propósitos específicos?
a7) ¿Cómo puede el RDAP, que es técnicamente capaz, permitir a los Registros/Registradores aceptar los identificadores de acreditación y el propósito de la consulta? Una vez que los acreditadores desarrollen los modelos de acreditación y que las autoridades legales pertinentes los aprueben, ¿cómo podemos asegurarnos de que el RDAP sea técnicamente capaz y esté listo para aceptar, registrar y responder al identificador del Solicitante acreditado?

(b) Credenciales: ¿Cuáles son las preguntas de política sin contestar que guiarán la implementación?

b1) ¿Cómo se concederán y gestionarán las credenciales?
b2) ¿Quién es responsable de proporcionar las credenciales?
b3) ¿Cómo se integrarán estas credenciales en los sistemas técnicos de los registradores/registros?

(c) Condiciones de acceso y cumplimiento de las condiciones de uso: ¿Cuáles son las preguntas de política sin contestar que guiarán la implementación?

c1) ¿Qué normas/políticas regirán el acceso de los usuarios a los datos?
c2) ¿Qué normas/políticas regirán el uso de los datos de los usuarios una vez que tengan acceso?
c3) ¿Quién será responsable de establecer y hacer cumplir estas normas/políticas?

c4) ¿A qué sanciones o penalizaciones, si procede, se enfrentará un usuario por un uso indebido de los datos, incluidas futuras restricciones de acceso o compensación a los titulares de los datos cuyos datos hayan sido objeto de uso indebido, además de las sanciones ya previstas en la ley aplicable?
c5) ¿Qué tipo de conocimientos tendrán las Partes contratadas sobre los datos a los que se accede y cómo se utilizan?
c6) ¿Qué derechos tienen los titulares de los datos para determinar cuándo y cómo se accede y se utilizan sus datos?
c7) ¿Cómo puede un modelo de acceso de terceros dar cabida a los diferentes requisitos de notificación de titulares de los datos de la divulgación de datos?

Del Anexo de la Especificación Temporaria:

- Desarrollar métodos para brindar a las potenciales partes reclamantes de URS y UDRP suficiente acceso a los datos de registración para respaldar las presentaciones de reclamos en buena fe.
- Limitaciones en términos de volumen de consultas previstas en un programa de acreditación equilibradas con las necesidades realistas de investigación de referencias cruzadas.
- Confidencialidad de las consultas de datos de registración por parte de las autoridades encargadas del cumplimiento de la ley.
- En virtud de la sección 4.4, seguir con el trabajo de la comunidad para desarrollar un modelo de acreditación y acceso que cumpla con el GDPR, al mismo tiempo que se reconoce la necesidad de obtener pautas adicionales del Grupo de Trabajo del Artículo 29/Comité Europeo de Protección de Datos.
- Proceso uniforme para el acceso continuo a los datos de registración, incluidos los datos no públicos, para usuarios con un fin legítimo, hasta el momento en el que un mecanismo final de acreditación y acceso esté en pleno funcionamiento, de forma obligatoria para todas las partes contratadas.

Informe Final de la Fase 1 del Equipo responsable del EPDP:

Recomendación 3 del Equipo responsable del EPDP.
De acuerdo con la carta orgánica del equipo responsable del EPDP y en concordancia con el Propósito 2, ahora que las preguntas críticas en dicha carta orgánica han sido respondidas, el equipo responsable del EPDP se compromete a hacer una recomendación relativa a un modelo estandarizado para la divulgación lícita de datos de registración no públicos (el cual se encuentra mencionado en la carta orgánica como 'acceso estandarizado'). Esto incluirá abordar preguntas tales como:

- Si dicho sistema debería ser adoptado.
- ¿Cuáles son los propósitos legítimos para que terceros accedan a datos de registración?

- ¿Cuáles son los criterios de elegibilidad para acceso a datos de registración no públicos?
- ¿Esas partes/grupos consisten en diferentes tipos de terceros Solicitantes?
- ¿Cuáles son los elementos de datos a los que cada usuario/parte debería tener acceso?

En este contexto, el Equipo responsable del EPDP considerará, entre otras cuestiones, la divulgación de información durante el curso de una investigación por infracción a la propiedad intelectual y casos de uso indebido del DNS. Es necesario confirmar que la divulgación de información con fines legítimos no sea incompatible con los fines para los cuales dichos datos han sido recopilados.

Preguntas sobre políticas del TSG

1. Resultado del EPDP, u otras iniciativas de política, en relación con el acceso a los datos de registración de nombres de dominio de gTLD sin carácter público.
2. Identificar y seleccionar los Proveedores de identidad (si se elige esa opción) que puedan otorgar credenciales para su uso en el sistema.[45]
3. Describir las cualificaciones generales de un Solicitante que está autorizado a acceder a los datos de registración de nombres de dominio de gTLD sin carácter público, por ejemplo, qué tipos de Solicitantes obtienen acceso a qué campos de los datos de registración de nombres de dominio de gTLD sin carácter público ("la política de autorización").
4. Detallar si una categoría particular de Solicitantes o los Solicitantes en general, pueden descargar registros de su actividad.
5. Describir los requisitos de retención de datos impuestos a cada componente del sistema.
6. Describir los Requisitos de Nivel de Servicio (SLR) para cada componente del sistema, incluso si se hacen públicos esos SLR y las evaluaciones de los operadores de los componentes en su contra, y para la tramitación de los reclamos sobre el acceso.
7. Especificar las causas legítimas para denegar una solicitud.
8. Esbozar el respaldo a la correlación mediante una consulta seudonimizada como se describe en la Sección 7.2.
9. Esbozar la selección de un modelo de actor como se describe en la Sección 8 y los componentes de apoyo apropiados y el descubrimiento de servicios como se describe en las Secciones 10.1 a 10.5.
10. Describir las condiciones, si las hubiera, en virtud de las cuales las solicitudes serían divulgadas a las Partes contratadas.
11. Proporcionar un análisis jurídico sobre la responsabilidad de los operadores de los diversos componentes del sistema.

[45] Varios señalaron que esta pregunta podría no estar dentro del alcance del Equipo responsable del EPDP para abordarla.

12. Esbozar un procedimiento para presentar reclamos sobre divulgaciones inapropiadas y, en consecuencia, una Política de uso aceptable.

ENTREGABLE PREVISTO

Recomendaciones de políticas para un modelo estandarizado de divulgación/acceso legítimo a datos de registración sin carácter público

LECTURA GENERAL REQUERIDA

Descripción	Enlace	Motivo del requisito
Elementos del marco del Modelo de Acceso Unificado para el acceso continuo a los datos completos de WHOIS (18 de junio de 2018)	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-18jun18-en.pdf	
Modelo preliminar de acreditación y acceso para datos sin carácter público de WHOIS (BC/IPC)	Modelo Versión 1.7 con fecha del 23 de julio de 2018	
Modelo de acceso a datos de registratarios diferenciados de Palage (también conocido como Philly Special)	Modelo de acceso a datos de registratarios diferenciados de Palage (también conocido como Philly Special) - Versión 2.0 con fecha del 30 de mayo de 2018	
Modelo de Acceso Unificado para el acceso continuo a los datos completos de WHOIS - Comparación de los modelos presentados por la comunidad (18 de junio de 2018)	https://www.icann.org/en/system/files/files/draft-unified-access-model-summary-elements-18jun18-en.pdf	

Opinión 2/2003 del Grupo de Trabajo del Artículo 29 sobre la aplicación de los principios de protección de datos a los directorios de Whois (2003)	https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp76_en.pdf	
Informe del EWG, Sección 4c, Principios de acreditación de usuarios del RDS (Junio de 2014)	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf	
Investigación del EWG - RFI sobre Acreditación de usuarios del RDS	https://community.icann.org/download/attachments/45744698/EWG%20USER%20ACCREDITATION%20RFI%20SUMMARY%2013%20March%202014.pdf	
Parte 1: Cómo funciona: RDAP – 10 de marzo de 2019	https://64.schedule.icann.org/meetings/963337	
Parte 2: Comprensión del RDAP y la función que puede desempeñar en la política del RDDS - 13 de marzo de 2019	https://64.schedule.icann.org/meetings/961941	
Modelo Técnico para el Acceso a los Datos de Registración sin Carácter Público propuesto por el Grupo de Análisis Técnico del Acceso a los Datos de Registración sin Carácter Público (30 de abril de 2019)	TSG01, Modelo Técnico para el Acceso a los Datos de Registración sin Carácter Público	
Informe Final sobre las cuestiones de acreditación de los servicios de privacidad y representación (proxy) (7 de diciembre de 2015)	https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf	

• Definiciones - páginas 6-8 • Anexo B – Marco de Divulgación ilustrativo aplicable a las solicitudes de divulgación del titular de Derechos de Propiedad Intelectual – páginas 85 – 93 • Acuerdo preliminar de acreditación de proveedores de servicios de privacidad y representación (proxy)		

SESIONES INFORMATIVAS A PROPORCIONAR

Tema	Posibles presentadores	Motivo de la importancia
RDAP - Preguntas y respuestas tras la revisión de las sesiones de la reunión ICANN65	Francisco Arias, Organización de la ICANN	Asegurar un entendimiento común del funcionamiento y las capacidades del RDAP

DEPENDENCIAS

Descripción de la dependencia	Depende de	Cronograma previsto o recomendado
La negociación y finalización de los acuerdos de protección de datos requeridos según el informe de la fase 1 son un requisito previo para gran parte del trabajo de la fase 2 (sugerido por la ISPCP)	Partes contratadas/Organización de la ICANN	

CRONOGRAMA Y ENFOQUE PROPUESTOS

Introducción
El objetivo del Equipo responsable del EPDP es desarrollar y acordar recomendaciones de políticas para compartir datos de registración sin carácter público[46] con las partes solicitantes (Sistema Estandarizado de Acceso/Divulgación de datos de registración sin carácter público).

Hasta que se proporcionen garantías jurídicas satisfactorias a las partes relevantes, el desarrollo de las recomendaciones de políticas para un Sistema Estandarizado de Acceso/Divulgación será agnóstica a las modalidades del Sistema.

Paralelamente, el Equipo responsable del EPDP en su conjunto debería participar con la Organización de la ICANN en el desarrollo de preguntas de políticas que ayuden a informar los debates con las DPA que tienen por objeto determinar qué modelo de Sistema de Divulgación Estandarizada se ajustaría plenamente al GDPR, sería viable y abordaría/mitigaría la responsabilidad jurídica de las partes contratadas.

Lista no exhaustiva de los temas que se prevé abordar:

- Terminología y definiciones de trabajo
- Se necesita asesoramiento jurídico
- Requisitos, incluida la definición de grupos de usuarios, criterios y criterios/contenido de la solicitud
- Se requiere la publicación del proceso, los criterios y la solicitud de contenido

[46] Del Informe Final de la Fase 1 del EPDP: El término "datos de registración" significará los elementos de datos identificados en el Anexo D [del Informe Final de la Fase 1 del EPDP], recopilados de una persona física y jurídica en relación con la registración de un nombre de dominio.

- Cronograma del proceso
- Recepción de la confirmación
- Acreditación
- Autenticación y autorización
- Propósitos de la divulgación a terceros
- Fundamento jurídico para la divulgación
- Política de uso aceptable
- Condiciones de uso / acuerdos de divulgación, incluido el cumplimiento de los requisitos legales
- Políticas de privacidad
- Política de consultas
- Retención y destrucción de datos
- Acuerdos de Nivel de Servicio
- Sostenibilidad financiera

Enfoque

Determinar desde el inicio:

a) Terminología y definiciones de trabajo
b) Identificar el asesoramiento jurídico necesario (nota: esta es también una actividad permanente en todos los temas).

Posible orden lógico para abordar los temas restantes:

c) Definir grupos de usuarios, criterios y propósitos / fundamento jurídico por grupo de usuarios
↓
d) Autenticación / autorización / acreditación de grupos de usuarios
↓
e) Criterios/contenido de las solicitudes por grupo de usuarios
↓
f) Política de consultas
↓
g) Recepción de la confirmación, incluido el cronograma
↓
h) Requisitos de respuesta / expectativas, incluido el cronograma/SLA
↓
i) Política de uso aceptable
↓
j) Condiciones de uso / acuerdos de divulgación / políticas de privacidad
↓
k) Retención y destrucción de datos

l) Tema general de consideración: sostenibilidad financiera

A continuación, se proporcionan más detalles sobre cada uno de estos temas. Para saltar a cada sección, utilice los siguientes enlaces:

Una vez completadas ésta y otras hojas de trabajo, cada tema (incluidos los temas de la Fase 1) y su alcance de trabajo constituirá la base de un plan de trabajo general programado. Algunos temas pueden abordarse en paralelo, mientras que otros pueden depender de otros trabajos antes de que se puedan tener deliberaciones más informadas. Se asignará a cada tema un tiempo determinado para llevar a cabo las deliberaciones de la cuestión, formular posibles conclusiones y/o posibles recomendaciones a las preguntas de políticas. Las conclusiones o recomendaciones que obtengan un nivel general de apoyo avanzarán para su posterior consideración y perfeccionamiento con miras a la elaboración de un Informe Inicial. El objetivo es lograr los niveles de consenso sobre las propuestas cuando sea posible antes de su publicación.

a) Tema: Terminología y definiciones de trabajo

Objetivo: Para garantizar que se asocie el mismo significado a los términos utilizados en el contexto de este análisis y evitar confusiones, el Equipo responsable del EPDP debe acordar un conjunto de definiciones de trabajo. Se entiende que estas definiciones de trabajo sirven simplemente para aclarar la terminología utilizada, no pretenden en modo alguno restringir el alcance del trabajo ni predeterminar el resultado. Se entiende que estas definiciones de trabajo deberán ser examinadas y revisadas, según sea necesario, al final del proceso.

Materiales a revisar:

- Terminología utilizada en el GDPR y otras leyes de protección de datos
- Informe Final sobre cuestiones de acreditación de servicios de privacidad y representación (proxy) (7 de diciembre de 2015) - Definiciones - páginas 6-8

Pregunta relacionada con los mapas conceptuales: None

Implementación de la Fase 1 del EPDP relacionada: A confirmar - la implementación de la recomendación 18 puede incluir definiciones que tal vez sea necesario incluir en las deliberaciones de la fase 2 del Equipo responsable del EPDP.

Tareas:

- Confirmar si se prevé la elaboración o aplicación de alguna definición en la implementación de la recomendación 18 (Personal)
- Desarrollar una primera versión preliminar de definiciones de trabajo. (Personal)
- El Equipo responsable del EPDP realizará una revisión y proporcionará aportes (EPDP)
- Obtener un acuerdo sobre el conjunto básico de definiciones (EPDP)
- Mantener el documento de trabajo de definiciones mediante deliberaciones (Todos)

Fecha prevista de finalización: 30 de mayo de 2019

b) Tema: Preguntas legales

Objetivo: identificar las preguntas legales que sean esenciales para ayudar a informar las deliberaciones del Equipo responsable del EPDP sobre este tema.

Preguntas presentadas hasta la fecha:

Pregunta	Estado	Encargado
1. Es necesario confirmar que la divulgación de información con fines legítimos no sea incompatible con los fines para los cuales dichos datos han sido recopilados.	**EN ESPERA** El Comité jurídico de la Fase 2 ha señalado esta pregunta como prematura en este momento y la marcará como "en espera". La pregunta se volverá a examinar una vez que el Equipo responsable del EPDP haya identificado los propósitos de la divulgación.	
2. Responder a la pregunta sobre la responsabilidad del tratamiento de los datos y el fundamento jurídico para un sistema de Acceso estandarizado a los datos de registración sin carácter público, suponiendo un marco técnico coherente con el TSG, y de forma que se aborden suficientemente las cuestiones relacionadas con la responsabilidad y la mitigación de riesgos con el objetivo de reducir los riesgos de responsabilidad para las Partes contratadas mediante la adopción de un sistema de Acceso estandarizado (IPC).	**RETRABAJO** El Comité jurídico de la Fase 2 está en el proceso de reformular esta pregunta, y, tras la revisión del texto actualizado, determinará si la pregunta debe remitirse a un asesor externo.	
3. Se debería procurar asesoramiento jurídico sobre la posibilidad de un sistema de	**EN ESPERA**	

divulgación basado en la acreditación como tal. (ISPCP)	El Comité jurídico de la Fase 2 ha señalado esta pregunta como prematura en este momento y la marcará como "en espera". La pregunta se volverá a examinar una vez que el Equipo responsable del EPDP haya identificado los propósitos de la divulgación.	
4. La pregunta de la divulgación a los organismos encargados de la aplicación de la ley de países no pertenecientes a la UE, en base al Art. 6 I f del GDPR, debería ser presentada a un asesor jurídico. (ISPCP)	**RETRABAJO** El Comité jurídico de la Fase 2 está en el proceso de procurar más información del autor de esta pregunta, y, tras la revisión de la aclaración y/o texto actualizado, determinará si la pregunta debería remitirse a un asesor externo.	
5. ¿Puede diseñarse un modelo centralizado de acceso/divulgación (en el que una única entidad se encargue de recibir las solicitudes de divulgación, realizar la prueba de equilibrio, comprobar la acreditación, responder a las solicitudes, etc.) de manera que se limite la responsabilidad de las partes contratadas en la mayor medida posible? IE - ¿se puede opinar que la entidad centralizada puede hacerse cargo en gran medida (si no totalmente) de la responsabilidad asociada a la divulgación (incluidas la acreditación y la	**RETRABAJO** El Comité jurídico de la Fase 2 está en el proceso de reformular esta pregunta, y, tras la revisión del texto actualizado, determinará si la pregunta debe	

autorización) y podría limitarse la responsabilidad de las partes contratadas a las actividades estrictamente asociadas con otros procesos no relacionados con la divulgación, como la recopilación y la transferencia segura de datos? En caso afirmativo, ¿qué debe considerarse/articularse en la política para dar cabida a esto? (ISPCP)	remitirse a un asesor externo.	
6. En el contexto de un SSAD, además de determinar su propio fundamento jurídico para la divulgación de datos, ¿necesita el solicitante (entidad que alberga los datos solicitados) evaluar el fundamento jurídico del tercero Solicitante? (Pregunta de la reunión ICANN65 del GAC/IPC)	**RETRABAJO** El Comité jurídico de la Fase 2 está en el proceso de reformular esta pregunta, y, tras la revisión del texto actualizado, determinará si la pregunta debe remitirse a un asesor externo.	
7. ¿En qué medida, si procede, son responsables las partes contratadas cuando un tercero tergiversa su procesamiento previsto, y cómo se puede reducir esta responsabilidad? (BC)	**RETRABAJO** El Comité jurídico de la Fase 2 está en el proceso de reformular esta pregunta, y, tras la revisión del texto actualizado, determinará si la pregunta debe remitirse a un asesor externo.	
8. La Unidad Constitutiva de Negocios (BC) propone que el EPDP divida el Propósito 2 en dos propósitos separados: • Permitir a la ICANN mantener la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio de acuerdo con la misión y los estatutos de	**EN ESPERA** El Comité jurídico de la Fase 2 ha señalado esta pregunta como prematura en este momento y la	

la ICANN a través del control y el procesamiento de los datos de registración de gTLD. • Permitir a terceros abordar la protección del consumidor, la ciberseguridad, la propiedad intelectual, el ciberdelito y el uso indebido del DNS en relación con la utilización o el registro de nombres de dominio. Se consultará a los asesores legales para determinar si es posible el propósito reformulado 2 (como se ha indicado anteriormente). ¿Se puede consultar a un asesor legal para determinar si el propósito reformulado 2 (como se ha indicado anteriormente) es posible en el marco del GDPR? Si el texto anterior no es posible, ¿hay alguna sugerencia que el asesor pueda aportar para mejorarlo? (BC)	marcará como "en espera". La pregunta se volverá a examinar una vez que se hayan completado las consultas de la Junta Directiva y el Consejo de la GNSO sobre la Recomendación 1, Propósito 2	
9. ¿Se puede proporcionar un análisis jurídico sobre cómo se debe realizar la prueba de equilibrio en virtud del apartado 6(1)(f) y en qué circunstancias dicho apartado podría requerir una revisión manual de una solicitud? (BC)	**RETRABAJO** El Comité jurídico de la Fase 2 está en el proceso de reformular esta pregunta, y, tras la revisión del texto actualizado, determinará si la pregunta debe remitirse a un asesor externo.	
10. Si no todas las solicitudes se benefician de la revisión manual, ¿existe una metodología legal para definir las categorías de solicitudes (por ejemplo, respuesta rápida a un ataque de malware o contactar a un infractor de la propiedad intelectual que no responda) que pueda estructurarse para reducir la necesidad de la revisión manual? (BC)	**RETRABAJO** El Comité jurídico de la Fase 2 está en el proceso de reformular esta pregunta, y, tras la revisión del texto actualizado, determinará si la	

	pregunta debe remitirse a un asesor externo.	
11. ¿Puede consultarse a un asesor legal para determinar si el GDPR impide un mayor volumen de acceso a los profesionales de ciberseguridad debidamente acreditados, que hayan acordado las medidas de protección adecuadas? Si dicho acceso no está prohibido, ¿puede el asesor legal proporcionar ejemplos de medidas de protección (como la seudonimización) que deberían considerarse? (BC)	**RETRABAJO** El Comité jurídico de la Fase 2 está en el proceso de reformular esta pregunta, y, tras la revisión del texto actualizado, determinará si la pregunta debe remitirse a un asesor externo.	
12. Para identificar el apartado 6(1)(b) como propósito para el procesamiento de los datos de registración, deberíamos seguir el asesoramiento de B&B que indica que "será necesario exigir que el titular de los datos ya tenga conocimiento, al menos de forma abstracta, sobre el tercero específico o, al menos, el procesamiento por parte del tercero en el momento de la conclusión del contrato y que el responsable del tratamiento, como socio contractual, informe de ello al titular de los datos antes de la transferencia al tercero". B&B debería aclarar por qué cree que el único fundamento para proporcionar WHOIS es para la prevención del uso indebido del DNS. Su conclusión en el párrafo 10 no considera los otros propósitos identificados por el EPDP en la Rec. 1, y, en cualquier caso, debería considerar el reciente reconocimiento por parte de la CE que indica que la ICANN tiene un propósito amplio para: "contribuir al mantenimiento de la seguridad, estabilidad y flexibilidad del Sistema de	**RETRABAJO** El Comité jurídico de la Fase 2 está en el proceso de reformular esta pregunta, y, tras la revisión del texto actualizado, determinará si la pregunta debe remitirse a un asesor externo.	

Nombres de Dominio de acuerdo con la misión de la ICANN" que está en el centro del rol de la ICANN como "custodia" del Sistema de Nombres de Dominio.		
13. B&B debería asesorar sobre la medida en que la base de interés público 6(1)e del GDPR es aplicable, habida cuenta del reconocimiento de la CE que señala lo siguiente: "Con respecto a la formulación del segundo propósito, la Comisión Europea reconoce el papel central y la responsabilidad de la ICANN de garantizar la seguridad, la estabilidad y la flexibilidad del Sistema de Nombres de Dominio de Internet y que al hacerlo actúa en beneficio del interés público".	**RETRABAJO** El Comité jurídico de la Fase 2 está en el proceso de reformular esta pregunta, y, tras la revisión del texto actualizado, determinará si la pregunta debe remitirse a un asesor externo.	

Tareas:

- Determinar las preguntas prioritarias de los temas relacionados con la Fase 2
- Acordar el enfoque y el proceso de aprobación de las cuestiones que surjan a lo largo de las deliberaciones

Fecha prevista de finalización: Etapa continua

c) Tema: Definir grupos de usuarios, criterios y propósitos / fundamento jurídico por grupo de usuarios

Objetivo:

- Definir las categorías de grupos de usuarios que pueden solicitar la divulgación de / acceso a los datos de registración sin carácter público, así como los criterios que deben aplicarse para determinar si una persona o entidad pertenece a esta categoría.
- Determinar los propósitos y el fundamento jurídico por grupo de usuarios para el procesamiento de datos.
- Determinar si el marco estandarizado de la Fase 2 puede dar cabida a las solicitudes exclusivas de los grupos de huellas de gran tamaño. Considerar si los que no encajan en ninguno de los grupos de usuarios identificados pueden todavía solicitar la divulgación/acceso mediante la implementación de la recomendación 18 o por otros medios.

Preguntas relacionadas con los mapas conceptuales:

P1-Carta orgánica-a
(a) Propósitos para acceder a los datos: ¿Cuáles son las preguntas de política sin contestar que guiarán la implementación?

a1) En virtud del derecho aplicable, ¿cuáles son los fines legítimos de terceros para acceder a los datos de registración?
a2) ¿Qué fundamentos jurídicos existen para respaldar este acceso?
a3) ¿Cuáles son los criterios de elegibilidad para acceso a datos de registración no públicos?
a4) ¿Esas partes/grupos consisten en diferentes tipos de terceros Solicitantes?

Anexo de la Especificación Temporaria:
3. Desarrollar métodos para proporcionar a los posibles reclamantes del URS y la UDRP suficiente
acceso a los datos de registración para apoyar la presentación de reclamos de buena fe.

Recomendaciones de la Fase 1
Rec. 3 del Equipo responsable del EPDP

- ¿Cuáles son los propósitos legítimos para que terceros accedan a datos de registración?
- ¿Cuáles son los criterios de elegibilidad para acceso a datos de registración no públicos?
- ¿Esas partes/grupos consisten en diferentes tipos de terceros Solicitantes?

El Equipo responsable del EPDP solicita que, al comenzar sus deliberaciones sobre un marco de acceso estandarizado, un representante del PDP WG de RPM proporcione una actualización del estado actual de las deliberaciones de manera que el Equipo responsable del EPDP pueda determinar si o cómo las recomendaciones del Grupo de Trabajo pueden afectar la consideración del URS y del UDRP en el contexto de dichas deliberaciones.

Cabe señalar que el Propósito 2 propuesto en este informe es un indicador, pendiente del trabajo adicional sobre el asunto del acceso que se llevará a cabo en la Etapa 2 de este EPDP, y se prevé volver a él una vez concluida dicha labor. [nota del personal - vinculada a los propósitos pero el momento de revisar el propósito 2 es una vez que se ha completado el trabajo de la Fase 2]

TSG-Final-Q#3
3. Describir las cualificaciones generales de un Solicitante que está autorizado a acceder a los datos de registración de nombres de dominio de gTLD sin carácter público, por ejemplo, qué tipos de Solicitantes obtienen acceso a qué campos de los datos de registración de nombres de dominio de gTLD sin carácter público ("la política de autorización").

Materiales a revisar:

Descripción	Enlace	Motivo del requisito
A fines de junio de 2017, la ICANN solicitó a las partes contratadas y a las partes interesadas que identificaran los tipos de usuarios y los propósitos de los elementos de datos requeridos por las políticas y contratos de la ICANN. A continuación, se presentan las respuestas individuales recibidas y una recopilación de las mismas.	Matriz de flujo de datos, compilación de respuestas recibidas - Versión actual	Iniciativa más reciente para identificar los tipos de usuarios
En el Informe Final del EWG se presenta un resumen no exhaustivo de los usuarios del sistema WHOIS existente, incluidos 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.	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf - páginas 20-25	
Revisar los propósitos establecidos y base legal identificada en la Fase 1 del Equipo responsable del EPDP.	https://gnso.icann.org/en/drafts/epdp-gtld-registration-data-specs-final-20feb19-en.pdf (páginas 34-36 / 67-71)	
Disposiciones pertinentes del GDPR	Disposiciones pertinentes en el GDPR - Véase el Artículo 6(1), el Artículo 6(2) y el Considerando 40	

Página de información sobre el fundamento jurídico de la Oficina del Comisionado de Información (ICO) para el procesamiento	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/	

Implementación de la Fase 1 del EPDP relacionada:
Ninguna prevista

Tareas:

- Elaborar una primera lista de categorías de Solicitantes en base a los materiales originales. (Personal)
- Revisar la lista de categorías de Solicitantes y determinar los criterios de elegibilidad. (Todos)
- Elaborar tipos y escenarios de uso indebido para formular casos de uso que determinen las necesidades de cada Solicitante.
- Determinar los propósitos y el fundamento jurídico por grupo de usuarios para el procesamiento de datos. (Todos)
- Determinar si el marco estandarizado de la Fase 2 puede dar cabida a las solicitudes exclusivas de los grupos de huellas de gran tamaño. Considerar si los que no encajan en ninguno de los grupos de usuarios identificados pueden todavía solicitar la divulgación/acceso mediante la implementación de la recomendación 18 o por otros medios. (Todos)
- Confirmar que todas las preguntas de la carta orgánica han sido abordadas y documentadas.

Fecha prevista de finalización: 13 de junio de 2019
(Revisar el propósito 2 - una vez que se haya completado el trabajo de la fase 2)

d) Autenticación / autorización / acreditación de grupos de usuarios

Objetivo:

- Establecer si se debe exigir la autenticación, autorización y/o acreditación de los grupos de usuarios.
    - ¿Puede un modelo de acreditación complementar o ser usado con lo que se implemente de la Recomendación 18 de la Fase 1 del EPDP?
- En caso afirmativo, establecer principios de políticas para la autenticación, autorización y/o acreditación, incluido el tratamiento de cuestiones como:
    - si un usuario autenticado que solicita acceso a datos sin carácter público de WHOIS debe o no especificar su interés legítimo para cada consulta/solicitud individual.
- En caso contrario, explicar por qué no y qué implicaciones puede tener esto en las consultas de ciertos grupos de usuarios, si las hubiere.

Preguntas relacionadas con los mapas conceptuales:

P1-Carta orgánica-a/b

(a) Propósitos para acceder a los datos: ¿Cuáles son las preguntas de política sin contestar que guiarán la implementación?
a7) ¿Cómo puede el RDAP, que es técnicamente capaz, permitir a los Registros/Registradores aceptar los identificadores de acreditación y el propósito de la consulta? Una vez que los acreditadores desarrollen los modelos de acreditación y que las autoridades legales pertinentes los aprueben, ¿cómo podemos asegurarnos de que el RDAP sea técnicamente capaz y esté listo para aceptar, registrar y responder al identificador del Solicitante acreditado?

(b) Credenciales: ¿Cuáles son las preguntas de política sin contestar que guiarán la implementación?
b1) ¿Cómo se concederán y gestionarán las credenciales?
b2) ¿Quién es responsable de proporcionar las credenciales?
b3) ¿Cómo se integrarán estas credenciales en los sistemas técnicos de los registradores/registros?

Anexo de la Especificación Temporaria

1. En virtud de la sección 4.4, seguir con el trabajo de la comunidad para desarrollar un modelo de acreditación y acceso que cumpla con el GDPR, al mismo tiempo que se reconoce la necesidad de obtener pautas adicionales del Grupo de Trabajo del Artículo 29/Comité Europeo de Protección de Datos.

TSG-Final-Q#2

Identificar y seleccionar los Proveedores de identidad (si se elige esa opción) que puedan otorgar credenciales para su uso en el sistema.

Materiales a revisar:

Descripción	Enlace	Motivo del requisito
Identificación y autenticación en el modelo del TSG	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf páginas 23-24	
Informe final del EWG - Principios de autorización de uso de contactos y acreditación de usuarios del RDS	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf páginas 39-40 y páginas 62-67	
Marco preliminar para un posible modelo de acceso unificado para el acceso continuo a la totalidad de los Datos de WHOIS - ¿Cómo se desarrollarían los requisitos de autenticación para los usuarios legítimos?	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf páginas 9-10, 10-11, 18, 23	

Implementación de la Fase 1 del EPDP relacionada:
Ninguna prevista.

Tareas:

- Revisar los materiales enumerados anteriormente y analizar las perspectivas sobre autenticación / autorización. (EPDP)
- Confirmar las definiciones de los términos clave Autorización, Acreditación y Autenticación.
- Determinar la lista completa de preguntas de políticas y deliberar sobre cada una de ellas.
- Determinar las posibles soluciones o la recomendación propuesta, si las hubiera.
- Confirmar que todas las preguntas de la carta orgánica han sido abordadas y documentadas.

Fecha prevista de finalización: ICANN 65

e) Criterios / contenido de las solicitudes por grupo de usuarios

Objetivo: establecer los requisitos de la política, los criterios y los contenidos mínimos de las solicitudes por grupo de usuarios identificados en el apartado c.

Preguntas relacionadas con los mapas conceptuales:

P1-Carta orgánica-c
c1) ¿Qué normas/políticas regirán el acceso de los usuarios a los datos?

Materiales a revisar:

Descripción	Enlace	Motivo del requisito
• Anexo B – Marco de Divulgación ilustrativo aplicable a las solicitudes de divulgación del titular de Derechos de Propiedad Intelectual – páginas 85 - 93 • Acuerdo de acreditación de proveedores de servicios de privacidad y representación (proxy)	Informe Final sobre cuestiones de acreditación de servicios de privacidad y representación (proxy) (7 de diciembre de 2015)	
Ejemplo: Formulario de información y solicitud de .DE	https://www.denic.de/en/service/whois-service/third-party-requests-for-holder-data/ https://www.denic.de/fileadmin/public/downloads/Domaindatenanfrage/Antrag_Domaindaten_Rechteinhaber_EN.pdf	

Ejemplo: Formulario de solicitud de Nominet	https://s3-eu-west-1.amazonaws.com/nominet-prod/wp-content/uploads/2018/05/22101442/Data-request-form.pdf	

Implementación de la Fase 1 del EPDP relacionada:

Recomendación 18 (pero NO requiere la divulgación automática de información)

Información mínima requerida para las solicitudes razonables de divulgación lícita:

- Identificación e información sobre el Solicitante (que incluya la naturaleza / tipo de entidad comercial o persona, declaraciones de poder notarial, según corresponda y sea relevante);
- Información sobre los derechos legales del Solicitante y el fundamento y / o justificación específica de la solicitud (por ejemplo, ¿cuál es la base o la razón de la solicitud?; ¿por qué es necesario que el Solicitante pida estos datos?);
- Afirmación de que la solicitud de divulgación se está presentando de buena fe;
- Una lista de elementos de datos solicitados por el Solicitante y la razón por la cual dichos datos se limitan a la necesidad;
- Acuerdo para procesar lícitamente cualquier dato recibido en respuesta a la solicitud de divulgación.

Tareas:

- Confirmar el enfoque de implementación de la recomendación 18.
- Confirmar las definiciones de los términos clave.
- Determinar la lista completa de preguntas de políticas y deliberar sobre cada una de ellas.
- Determinar las posibles soluciones o la recomendación propuesta, si las hubiera.
- Confirmar que todas las preguntas de la carta orgánica han sido abordadas y documentadas.

Fecha prevista de finalización: ICANN 65

f) Política de consultas

Objetivo: Establecer requisitos mínimos de la política para el registro de las consultas, definiendo los controles apropiados para el momento en que los registros de las consultas deban estar disponibles, y si debe haber limitaciones de las consultas para los usuarios autenticados y no autenticados del SSAD.

- ¿Cómo se limitará el acceso a los datos de registración sin carácter público a fin de reducir al mínimo los riesgos de acceso y utilización no autorizados (por ejemplo, permitiendo el acceso únicamente en base a consultas específicas, en contraposición a las transferencias masivas y/u otras restricciones a las búsquedas o a los servicios de directorio invertidos, incluidos los mecanismos para restringir el acceso a los campos a lo que sea necesario para lograr el propósito legítimo en cuestión)?
- ¿Debería considerarse la confidencialidad de las consultas, por ejemplo, por parte de los organismos de aplicación de la ley?
- ¿Cómo se deberían equilibrar las limitaciones de las consultas con las necesidades realistas de investigación de cruce de referencias?

Preguntas relacionadas con los mapas conceptuales:

P1-Carta orgánica-a
a7) ¿Cómo puede el RDAP, que es técnicamente capaz, permitir a los Registros/Registradores aceptar los identificadores de acreditación y el propósito de la consulta? Una vez que los acreditadores desarrollen los modelos de acreditación y que las autoridades legales pertinentes los aprueben, ¿cómo podemos asegurarnos de que el RDAP sea técnicamente capaz y esté listo para aceptar, registrar y responder al identificador del Solicitante acreditado?

Anexo de la Especificación Temporaria:
6 Limitaciones en cuanto al volumen de consultas previsto en un programa de acreditación equilibrado
contra las necesidades realistas de investigación de cruce de referencias.
7 Confidencialidad de las consultas de datos de registración por parte de las autoridades encargadas del cumplimiento de la ley.

Materiales a revisar:

Descripción	**Enlace**	**Motivo del requisito**
SSAC 101 - Documento de asesoramiento del SSAC sobre el acceso a los datos de registración de nombres de dominio	https://www.icann.org/en/system/files/files/sac-101-en.pdf	Describe los efectos de de limitar tarifas.

Implementación de la Fase 1 del EPDP relacionada: Ninguna.

Tareas:

- Confirmar las definiciones de los términos clave.
- Determinar la lista completa de preguntas de políticas y deliberar sobre cada una de ellas.
- Determinar las posibles soluciones o la recomendación propuesta, si las hubiera.
- Confirmar que todas las preguntas de la carta orgánica han sido abordadas y documentadas.

Fecha prevista de finalización: ICANN 65

g) Recepción de la confirmación, incluido el cronograma

Objetivo: Definir los requisitos de la política en torno al plazo del acuse de recibo y los requisitos adicionales (si los hubiera) que debería contener el acuse de recibo.

¿Cuáles son, en su caso, los requisitos mínimos de referencia para el acuse de recibo estandarizado de los registradores/registros? ¿Qué hay de las solicitudes "urgentes" y cómo se definen?

Preguntas relacionadas con los mapas conceptuales:

P1-Carta orgánica-c
c1) ¿Qué normas/políticas regirán el acceso de los usuarios a los datos?

Materiales a revisar:

Descripción	Enlace	Motivo del requisito
Informe final de la Fase 1 Rec. 18 Plazo estipulado y criterios para las respuestas del Registrador y del Operador de Registro	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf p. 19	

Implementación de la Fase 1 del EPDP relacionada: - Recomendación 18:
Plazo estipulado y criterios para las respuestas del Registrador y del Operador de Registro -

Los Registros y Registradores deben considerar y atender razonablemente las solicitudes de divulgación lícita:
• Tiempo de respuesta para acusar recibo de una solicitud razonable de divulgación lícita. Sin demora indebida, pero no más de dos (2) días hábiles a partir de la recepción, a menos que las circunstancias mostradas no lo permitan.

Tareas:

- Confirmar las definiciones de los términos clave.
- Determinar la lista completa de preguntas de políticas y deliberar sobre cada una de ellas.
- Determinar las posibles soluciones o la recomendación propuesta, si las hubiera.
- Confirmar que todas las preguntas de la carta orgánica han sido abordadas y documentadas.

Fecha prevista de finalización: A confirmar

h) Requisitos de respuesta / expectativas, incluido el cronograma/SLA

Objetivo: Definir los requisitos de la política en torno a los requisitos de respuesta, incluido el tratamiento de preguntas como:

- incluido el tratamiento de preguntas como:
    - Si deben devolverse o no los datos completos de WHOIS cuando un usuario autentificado realiza una consulta.
    - ¿Cuáles deberían ser los compromisos del SLA para las respuestas a las solicitudes de acceso/divulgación?
    - ¿Cuáles son los requisitos mínimos para responder a las solicitudes, incluida la denegación de las mismas?

Preguntas relacionadas con los mapas conceptuales:

P1-Carta orgánica-a/c
a5) ¿Cuáles son los elementos de datos a los que cada usuario/parte debería tener acceso en base a su propósito?
a6) ¿En qué medida podemos determinar un conjunto de elementos de datos y el posible alcance (volumen) para terceros
y/o propósitos específicos?
c1) ¿Qué normas/políticas regirán el acceso de los usuarios a los datos?

Recomendación 3 de la fase 1
¿Cuáles son los elementos de datos a los que cada usuario/parte debería tener acceso?

Anexo de la Especificación Temporaria

2. Abordar la factibilidad de requerir contactos únicos para tener una dirección de correo electrónica anónima uniforme en las registraciones de nombres de dominio en un registrador determinado, mientras se garantiza la seguridad/estabilidad y se cumplen con los requisitos de la sección 2.5.1 del Apéndice A.

TSG-Final-Q#6
Describir los Requisitos de Nivel de Servicio (SLR) para cada componente del sistema, incluso si se hacen públicos esos SLR y las evaluaciones de los operadores de los componentes en su contra, y para la tramitación de los reclamos sobre el acceso.
TSG-Final-Q#7
Especificar las causas legítimas para denegar una solicitud.
TSG-Final-Q#8
Esbozar el respaldo a la correlación mediante una consulta seudonimizada como se describe en la Sección 7.2.

Materiales a revisar:

Descripción	**Enlace**	**Motivo del requisito**
Informe final de la Fase 1 Rec. 18 Plazo estipulado y criterios para las respuestas del Registrador y del Operador de Registro	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf p. 19	
Informe Final sobre las cuestiones de acreditación de los servicios de privacidad y representación (proxy) (7 de diciembre de 2015) ● Anexo B – Marco de Divulgación ilustrativo aplicable a las solicitudes de divulgación del titular de Derechos de Propiedad Intelectual – páginas 90 - 92	https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf	Sección del marco ilustrativo de divulgación de PPSAI en la que se detalla la respuesta mínima requerida.

Implementación de la Fase 1 del EPDP relacionada:

Recomendación n.° 18:

- Requisitos para la información que las respuestas deben incluir. Las respuestas en las cuales la divulgación de datos hubiese sido denegada (en forma total o parcial), deben incluir: justificación suficiente para que el Solicitante entienda los motivos de la decisión, incluido, por ejemplo, un análisis y una explicación de cómo se aplicó la prueba de equilibrio (si corresponde).
- Los registros de las solicitudes de divulgación, los acuses de recibo y las respuestas deben conservarse de acuerdo con las prácticas estándar de archivo comercial con el fin de mantenerlos disponibles para ser generados conforme sea necesario, incluyendo, en forma no taxativa, a los fines de auditoría por parte del equipo de Cumplimiento Contractual de la ICANN;
- La respuesta a un Solicitante se realizará sin demoras indebidas y, en ausencia de circunstancias excepcionales, el plazo estipulado para dicha respuesta será dentro de un máximo de 30 días. Dichas circunstancias pueden incluir la cantidad total de solicitudes recibidas. En forma periódica, las partes contratadas informarán la cantidad de solicitudes de divulgación recibidas a la ICANN para que se pueda evaluar la razonabilidad.
- Se considerará una línea de tiempo separada de [menos de X días hábiles] para la respuesta a las peticiones razonables de divulgación 'urgentes'; aquellas solicitudes de información no pública para las cuales se proporcione evidencia que demuestre una necesidad inmediata de divulgación de información [durante la implementación se estipulará el plazo y el conjunto de criterios para las solicitudes urgentes].

Tareas:

- Confirmar las definiciones de los términos clave.
- Determinar la lista completa de preguntas de políticas y deliberar sobre cada una de ellas.
- Determinar las posibles soluciones o la recomendación propuesta, si las hubiera.
- Confirmar que todas las preguntas de la carta orgánica han sido abordadas y documentadas.

Fecha prevista de finalización: Agosto

i) Política de uso aceptable

Objetivo: Definir los requisitos de la política en torno a lo siguiente:

1. ¿Cómo debería desarrollarse, evolucionar continuamente y aplicarse un código de conducta (si lo hubiera)?
2. Si la ICANN y sus partes contratadas desarrollan un código de conducta para terceros con intereses legítimos, ¿qué características y necesidades deberían considerarse?

3. ¿Existen flujos de datos adicionales que deban ser documentados fuera de lo que se documentó en la Fase 1?
¿Puede un código de conducta complementar o ser usado con lo que se implemente de la Recomendación 18 de la Fase 1 del EPDP?

Preguntas relacionadas con los mapas conceptuales:

P1-Carta orgánica-c
c1) ¿Qué normas/políticas regirán el acceso de los usuarios a los datos?
c2) ¿Qué normas/políticas regirán el uso de los datos de los usuarios una vez que tengan acceso?
c3) ¿Quién será responsable de establecer y hacer cumplir estas normas/políticas?
c4) ¿Cuáles son las sanciones o penas, si las hay, a las que se enfrentará un usuario en caso de uso indebido de los datos, incluidas las futuras
restricciones de acceso o indemnización a los titulares de datos cuyos datos hayan sido objeto de uso indebido
además de las sanciones ya previstas en la ley aplicable?
c5) ¿Qué tipo de conocimientos tendrán las Partes contratadas sobre los datos a los que se accede y cómo se utilizan?
c6) ¿Qué derechos tienen los titulares de los datos para determinar cuándo y cómo se accede y se utilizan sus datos?
c7) ¿Cómo puede un modelo de acceso de terceros dar cabida a los diferentes requisitos de notificación de titulares de los datos de la divulgación de datos?

Materiales a revisar:

Descripción	**Enlace**	**Motivo del requisito**
GDPR, Artículo 40, Código de conducta	https://gdpr-info.eu/art-40-gdpr/	
Carta del Grupo de Trabajo del Artículo 29 a la ICANN 11 de abril de 2018	https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf	

Bird & Bird - Código de conducta y material de referencia para la certificación (mayo de 2017)	https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/43--guide-to-the-gdpr--codes-of-conduct-and-certifications.pdf?la=en	
Ejemplo: Código de conducta para proveedores de nubes (CISPE) (enero de 2017)	https://cispe.cloud/code-of-conduct/	
Ejemplo: Código de conducta para proveedores de nubes (EU Cloud) (noviembre de 2018)	https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html	

Implementación de la Fase 1 del EPDP relacionada: Ninguna.

Tareas:

- Determinar la lista completa de preguntas de políticas y deliberar sobre cada una de ellas.
- Determinar las posibles soluciones o la recomendación propuesta, si las hubiera.
- Confirmar que todas las preguntas de la carta orgánica han sido abordadas y documentadas.

Fecha prevista de finalización: Agosto

j) Condiciones de uso / acuerdos de divulgación / políticas de privacidad

Objetivo: Definir los requisitos de la política en torno a las condiciones de uso para los terceros que procuren acceder a datos de registración sin carácter público:

- Como mínimo, ¿qué medidas se necesitan para proteger adecuadamente los datos personales que puedan ponerse a disposición de un usuario/tercero acreditado?
- ¿Qué procedimientos deberían establecerse para acceder a los datos?
- ¿Qué procedimientos deberían establecerse para limitar el uso de los datos a los que se accede adecuadamente?

- ¿Deberían exigirse Condiciones de uso aparte para los distintos grupos de usuarios?
- ¿Quién supervisaría y exigiría el cumplimiento de las Condiciones de uso?
- ¿Qué mecanismo se utilizaría para exigir el cumplimiento de las Condiciones de uso?

Preguntas relacionadas con los mapas conceptuales:

P1-Carta orgánica-c
c1) ¿Qué normas/políticas regirán el acceso de los usuarios a los datos?
c2) ¿Qué normas/políticas regirán el uso de los datos de los usuarios una vez que tengan acceso?
c3) ¿Quién será responsable de establecer y hacer cumplir estas normas/políticas?
c4) ¿Cuáles son las sanciones o penas, si las hay, a las que se enfrentará un usuario en caso de uso indebido de los datos, incluidas las futuras
restricciones de acceso o indemnización a los titulares de datos cuyos datos hayan sido objeto de uso indebido
además de las sanciones ya previstas en la ley aplicable?

TSG-Final-Q#4
Detallar si una categoría particular de Solicitantes o los Solicitantes en general, pueden descargar registros de su actividad.
TSG-Final-Q#10
Describir las condiciones, si las hubiera, en virtud de las cuales las solicitudes serían divulgadas a las Partes contratadas.
TSG-Final-Q#11
Proporcionar un análisis jurídico sobre la responsabilidad de los operadores de los diversos componentes del sistema.
TSG-Final-Q#12
Esbozar un procedimiento para presentar reclamos sobre divulgaciones inapropiadas y, en consecuencia, una Política de uso aceptable.

Materiales a revisar:

Descripción	Enlace	Motivo del requisito
Marco preliminar para un posible modelo de acceso unificado para el acceso continuo a la totalidad de Datos de WHOIS: ¿Cuál sería la función de las Condiciones de uso en un modelo de acceso unificado?	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf páginas 14-16	

Implementación de la Fase 1 del EPDP relacionada:

Tareas:

- Confirmar las definiciones de los términos clave.
- Determinar la lista completa de preguntas de políticas y deliberar sobre cada una de ellas.
- Determinar las posibles soluciones o la recomendación propuesta, si las hubiera.
- Confirmar que todas las preguntas de la carta orgánica han sido abordadas y documentadas.

Fecha prevista de finalización: Septiembre

k) Retención y destrucción de datos

Objetivo: Establecer requisitos mínimos de la política para la retención, eliminación y registro de los datos retenidos para las partes involucradas en el SSAD, incluidos, entre otros, los datos de registración de gTLD, información de cuentas de usuarios, registros de transacciones y metadatos como la fecha y hora de las solicitudes.

Preguntas relacionadas con los mapas conceptuales:

P1-Carta orgánica-c
c2) ¿Qué normas/políticas regirán el uso de los datos de los usuarios una vez que tengan acceso?

TSG-Final-Q#5
Describir los requisitos de retención de datos impuestos a cada componente del sistema.

Materiales a revisar:

Descripción	Enlace	Motivo del requisito
GDPR, Artículo 5(1)(e)	https://gdpr.algolia.com/gdpr-article-5	
Retención de datos en el modelo del TSG	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf página 26	

Implementación de la Fase 1 del EPDP relacionada: Recomendación n.° 15:
1. Para informar sus deliberaciones de la Fase 2, el Equipo responsable del EPDP recomienda que la Organización de la ICANN realice, como cuestión de urgencia, una revisión de todos sus procesos y procedimientos activos, a fin de identificar y documentar los casos en que se solicitan datos personales a un registrador más allá del período de 'vigencia de la registración'. Se deben identificar y documentar los períodos de retención para elementos de datos específicos y, en base a ello, establecer las expectativas de retención de datos mínimas relevantes y específicas requeridas para los registradores. El Equipo responsable del EPDP recomienda que se invite a los miembros de la comunidad a contribuir a este ejercicio de recopilación de datos, mediante el suministro de información sobre otros propósitos legítimos para los cuales diferentes períodos de retención pueden ser aplicables.

2. Mientras tanto, el Equipo responsable del EPDP ha reconocido que la Política de Resolución de Disputas Relacionadas con Transferencias ("TDRP") ha sido identificada como la que tiene el período de retención justificado más largo de un año y, por lo tanto, ha recomendado a los registradores que conserven únicamente aquellos elementos de datos considerados necesarios en virtud de la TDRP, por un período de quince meses posteriores a la vigencia de la registración, más tres meses para implementar la eliminación, es decir, 18 meses. Esta retención se basa en la estipulación de la política establecida en la TDRP que establece que los reclamos en virtud de la política pueden plantearse únicamente durante un período de 12 meses después del presunto incumplimiento (nota al pie: véase la sección 2.2 de la TDRP) de la Política de Transferencia (nota al pie: véase la sección 1.15 de la TDRP). Este período de retención no restringe la capacidad de los registros y registradores para retener los

elementos de datos dispuestos en las Recomendaciones 4 a 7 para otros fines especificados en la Recomendación 1, por períodos de tiempo más breves.

3. El Equipo responsable del EPDP reconoce que las Partes contratadas pueden, de acuerdo con la legislación local u otros requisitos, tener necesidades o requisitos para diferentes períodos de retención. El Equipo responsable del EPDP observa que nada en esta recomendación, o en una política separada de la ICANN, prohíbe a las partes contratadas establecer sus propios períodos de retención, los cuales pueden ser más extensos o más breves de lo especificado en la política de la ICANN.

4. El Equipo responsable del EPDP recomienda que la Organización de la ICANN revise su procedimiento para conceder exenciones de retención de datos vigente, con el fin de mejorar la eficiencia, los tiempos de respuesta de las solicitudes y el cumplimiento del GDPR; por ejemplo, si un Registrador de una determinada jurisdicción obtiene una exención de retención de datos, los Registradores en situaciones similares pueden aplicar la misma exención a través de un procedimiento de notificación y sin tener que presentar una solicitud por separado.

Tareas:

- Confirmar las definiciones de los términos clave.
- Determinar la lista completa de preguntas de políticas y deliberar sobre cada una de ellas.
- Determinar las posibles soluciones o la recomendación propuesta, si las hubiera.
- Confirmar que todas las preguntas de la carta orgánica han sido abordadas y documentadas.

Fecha prevista de finalización: Septiembre

l) Sostenibilidad financiera

Objetivo: Asegurar que todos los aspectos del SSAD sean financieramente sostenibles. Considerar cómo y quién asume los costos de la implementación y gestión del SSAD.

- Determinar si las ineficiencias del mercado existían antes de mayo de 2018 y si existe alguna en un mundo posterior a la Fase 1 del EPDP.
- ¿Deberían las partes contratadas y/o la ICANN asumir el costo de una solución estandarizada, incluso si la divulgación de los datos de registración se considera de interés público?
- Si la acreditación es una solución viable, ¿debería haber tarifas de solicitud asociadas o una estructura tarifaria en base al tipo (escalonado), tamaño o cuantificación de las divulgaciones?
- ¿Se debería o podría compensar a los titulares de los datos por la divulgación de sus datos?

Preguntas relacionadas con los mapas conceptuales: None

Materiales a revisar:

Descripción	Enlace	Motivo del requisito

Implementación de la Fase 1 del EPDP relacionada: None

Tareas:

- Confirmar las definiciones de los términos clave.
- Determinar la lista completa de preguntas de políticas y deliberar sobre cada una de ellas.
- Determinar las posibles soluciones o la recomendación propuesta, si las hubiera.
- Confirmar que todas las preguntas de la carta orgánica han sido abordadas y documentadas.

Fecha prevista de finalización: A confirmar

Anexo B – Antecedentes generales

Antecedentes de procesos y cuestiones

El 19 de julio de 2018, el Consejo de la GNSO inició un Proceso Expeditivo de Desarrollo de Políticas (EPDP) y creó la carta orgánica del equipo responsable del EPDP sobre la Especificación Temporaria para los Datos de Registración de los gTLD. A diferencia de otras iniciativas de Procesos de Desarrollo de Políticas de la GNSO, que están abiertos para cualquier persona, el Consejo de la GNSO optó por limitar la composición de los miembros de este EPDP, principalmente en reconocimiento de la necesidad de completar el trabajo en un período de tiempo relativamente breve, y de aportar recursos al esfuerzo de manera responsable. Se ha invitado a: los Grupo de Partes Interesadas de la GNSO, el Comité Asesor Gubernamental (GAC), la Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO), el Comité Asesor At-Large (ALAC), el Comité Asesor del Sistema de Servidores Raíz (RSSAC) y al Comité Asesor de Seguridad y Estabilidad (SSAC), a designar hasta una cantidad determinada de miembros y suplentes, conforme se describe en la carta orgánica. Además, la Junta Directiva de la ICANN y la Organización de la ICANN han sido invitadas a asignar una cantidad limitado de coordinadores de enlace para esta iniciativa. En julio, se emitió una convocatoria a voluntarios para los grupos antes mencionados, y el Equipo responsable del EPDP realizó su primera reunión el 1 de agosto de 2018.

○ Información de referencia sobre el tema

El 17 de mayo de 2018, la Junta Directiva de la ICANN aprobó la Especificación Temporaria para los Datos de Registración de los gTLD. La Junta Directiva tomó esta medida a fin de establecer requisitos temporarios sobre la modalidad en que la ICANN y sus partes contratadas continuarían cumpliendo con los requisitos contractuales de la ICANN que se encuentran vigentes, como también con las políticas desarrolladas por la comunidad en relación con el sistema de WHOIS, a la vez que cumplen con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea (UE). La especificación temporaria se adoptó según el procedimiento para políticas temporarias establecido en el Acuerdo de Registro (RA) y el Acuerdo de Acreditación de Registradores (RAA). Tras la adopción de la especificación temporaria, la Junta Directiva "actuará inmediatamente para implementar el proceso de desarrollo de políticas por consenso indicado en los Estatutos de la ICANN".[47] El proceso de desarrollo de políticas por consenso correspondiente a la especificación temporaria debe llevarse a cabo en el plazo de un año. Asimismo, el alcance incluye el análisis de un sistema de acceso estandarizado a los datos de registración sin carácter público.

[47] Véase la sección 3.1(a) del Acuerdo de Registro: https://www.icann.org/resources/unthemed-pages/org-agmt-html-2013-09-12-en

En su reunión del 19 de julio de 2018, el Consejo de la Organización de Apoyo para Nombres Genéricos (GNSO) inició un EPDP sobre la Especificación Temporaria para los Datos de Registración de los gTLD y adoptó la carta orgánica del Equipo responsable del EPDP. A diferencia de otras iniciativas de Procesos de Desarrollo de Políticas de la GNSO, que están abiertos para cualquier persona, el Consejo de la GNSO optó por limitar la composición de los miembros de este EPDP, principalmente en reconocimiento de la necesidad de completar el trabajo en un período de tiempo relativamente breve, y de aportar recursos al esfuerzo de manera responsable. Se ha invitado a: los Grupo de Partes Interesadas de la GNSO, el Comité Asesor Gubernamental (GAC), la Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO), el Comité Asesor At-Large (ALAC), el Comité Asesor del Sistema de Servidores Raíz (RSSAC) y al Comité Asesor de Seguridad y Estabilidad (SSAC), a designar hasta una cantidad determinada de miembros y suplentes, conforme se describe en la carta orgánica. Además, la Junta Directiva de la ICANN y la Organización de la ICANN han sido invitadas a asignar una cantidad limitado de coordinadores de enlace para esta iniciativa.

El Equipo responsable del EPDP publicó su Informe Inicial de la Fase 1 para Comentario público el 21 de noviembre de 2018. El Equipo responsable del EPDP incorporó los comentarios públicos en su Informe Final de la Fase 1, y el Consejo de la GNSO llevó a cabo una votación para adoptar las 29 recomendaciones del Informe Final de la Fase 1 del EPDP en su reunión del 4 de marzo de 2019. El 15 de mayo de 2019, la Junta Directiva de la ICANN adoptó el Informe Final de la Fase 1 del Equipo responsable del EPDP, con la excepción de partes de dos recomendaciones: 1) Propósito 2 de la Recomendación 1; y 2) la opción de eliminar los datos en el campo que especifica la Organización en la Recomendación 12. Conforme a los estatutos de la ICANN, se llevará a cabo una consulta entre el Consejo de la GNSO y la Junta Directiva de la ICANN para debatir las partes de las recomendaciones de la Fase 1 del EPDP que no fueron adoptadas por la Junta Directiva de la ICANN. Al mismo tiempo, un Equipo para la Revisión de la Implementación (IRT), formado por la organización de la ICANN y miembros de la comunidad de la ICANN, implementará ahora las recomendaciones aprobadas del Informe Final de la Fase 1 del Equipo responsable del EPDP. Para obtener más detalles sobre el estado de la implementación, consulte este enlace.

El 2 de mayo de 2019, el Equipo responsable del EPDP comenzó la Fase 2 de su trabajo. El alcance de la Fase 2 del EPDP incluye (i) el análisis de un sistema para el acceso/divulgación estandarizados a los datos de registración sin carácter público, (ii) las cuestiones señaladas en el Anexo a la Especificación Temporaria para los Datos de Registración de los gTLD ("Cuestiones importantes para posterior acción de la comunidad"), y (iii) las cuestiones diferidas de la Fase 1, por ejemplo, las personas jurídicas frente a las personas físicas y la censura del campo que especifica la ciudad, entre otros. Para obtener más detalles, consulte aquí.

Anexo C – Membresía y asistencia del Equipo responsable del EPDP

Membresía y asistencia del Equipo responsable del EPDP

Resumen de la actividad de la reunión:

Reuniones plenarias:

- 75 llamadas del plenario durante 155,5 horas
- 12 reuniones presenciales durante 77,5 horas
- 1 seminario web de 1 hora
- Índice de participación total 86 %

Reuniones de equipos pequeños:

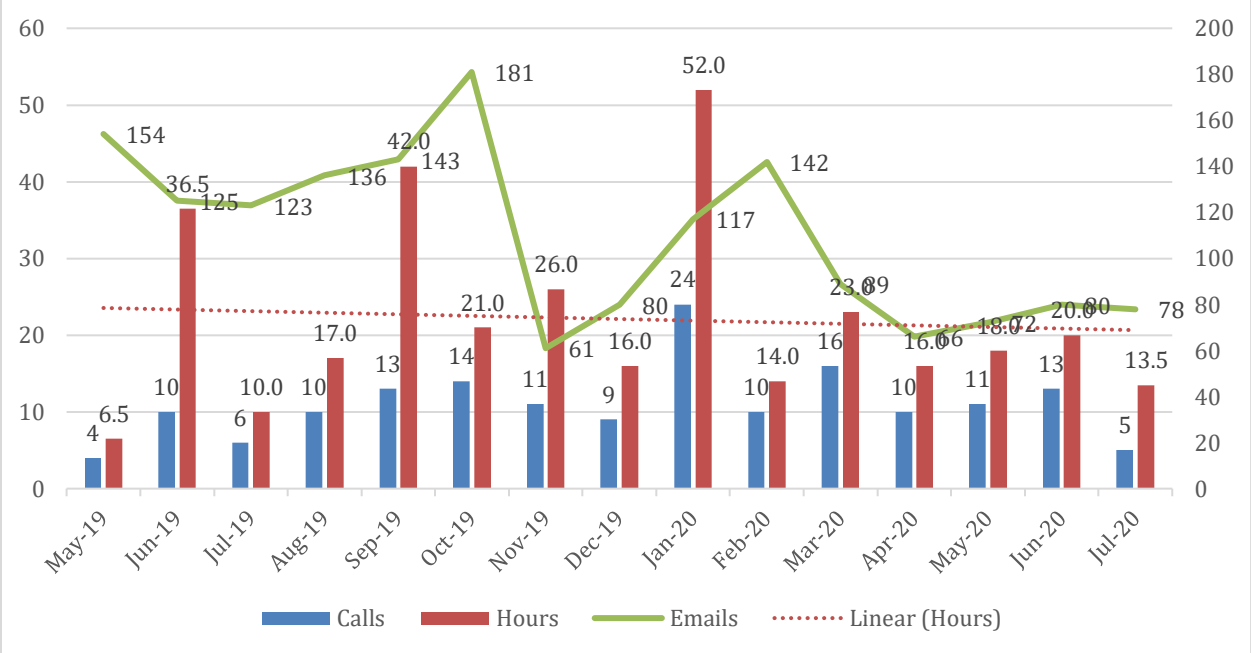
- 10 llamadas de subgrupos durante 18 horas

Reuniones del Comité jurídico:

- 19 llamadas de subgrupos durante 29,4 horas
- 1 reunión presencial durante 1,5 horas

Reuniones de líderes:

- 48 llamadas de líderes durante 47,5 horas
- 4 reuniones presenciales de líderes durante 20,5 horas



La lista detallada, las manifestaciones de interés y la asistencia se encuentran disponibles en https://community.icann.org/x/kBdIBg.

Los archivos de los mensajes de correo electrónico se encuentran disponibles en https://mm.icann.org/pipermail/gnso-epdp-team/.

Miembros activos del plenario del Equipo responsable del EPDP: (LC - sirvió en el Comité de Asuntos Jurídicos)

Tipo de miembro / Afiliación / Nombre	Manifestación de Interés (SOI)	Fecha de inicio	Asistió %	Función
Participante actual			87.9%	
Miembro				
Comité Asesor At-Large			97.7%	
Alan Greenberg	SOI	03/04/2019	97.7%	
Hadia El-Miniawi	SOI	03/04/2019	97.7%	LC
Unidad Constitutiva de Usuarios Comerciales y de Negocios			94.8%	
Margie Milam	SOI	03/04/2019	95.4%	LC
Mark Svancarek	SOI	03/04/2019	94.3%	
Consejo de la GNSO			98.3%	
Rafik Dammak	SOI	03/04/2019	98.3%	President e
Comité Asesor Gubernamental			93.6%	
Christopher Lewis-Evans	SOI	15/05/2019	96.6%	
Georgios Tselentis	SOI	03/04/2019	88.5%	
Laureen Kappin	SOI	21/10/2019	96.1%	LC
Junta Directiva de la ICANN			84.6%	
Becky Burr	SOI	09/09/2019	93.5%	LC
Chris Disspain	SOI	03/04/2019	78.2%	
Unidad Constitutiva de Propiedad Intelectual			91.0%	
Brian King	SOI	04/08/2019	88.5%	LC
Franck Journoud	SOI	12/01/2019	95.7%	
Corporación para la Asignación de Nombres y Números en Internet			95.9%	
Daniel Halloran	-	03/04/2019	94.3%	
Eleeza Agopian	-	06/12/2019	98.4%	
Unidad Constitutiva de Proveedores de Servicios de Internet y Servicios de Conectividad			65.5%	
Fiona Asonga	SOI	03/04/2019	44.8%	

Thomas Rickert	SOI	03/04/2019	86.2%	LC
Grupo de Partes Interesadas No Comerciales			78.9%	
Amr Elsadr	SOI	03/04/2019	67.8%	
Johan (Julf) Helsingius	SOI	03/04/2019	75.9%	
Milton Mueller	SOI	03/04/2019	81.4%	
Stefan Filipovic	SOI	21/05/2019	84.5%	
Stephanie Perrin	SOI	03/04/2019	86.2%	LC
<vacante>	-			
Grupo de Partes Interesadas de Registradores			85.0%	
James Bladel	SOI	03/04/2019	76.7%	
Matt Serlin	SOI	03/04/2019	86.2%	
Volker Greimann	SOI	16/04/2019	92.0%	LC
Grupo de Partes Interesadas de Registros			90.0%	
Alan Woods	SOI	03/04/2019	90.8%	
Marc Anderson	SOI	03/04/2019	95.4%	
Matthew Crossman	SOI	03/04/2019	83.1%	LC
Comité Asesor de Seguridad y Estabilidad			92.1%	
Ben Butler	SOI	03/04/2019	93.1%	
Tara Whalen	SOI	15/05/2019	90.9%	LC

Suplentes activos del plenario del Equipo responsable del EPDP:

Tipo de miembro / Afiliación / Nombre	Manifestación de Interés (SOI)	Fecha de inicio	Asistió %	Función
Suplente				
Comité Asesor At-Large				
Bastiaan Goslings	SOI	03/04/2019	50.0%	
Holly Raiche	SOI	03/04/2019	33.3%	
Unidad Constitutiva de Usuarios Comerciales y de Negocios				
Steve DelBianco	SOI	03/04/2019	100.0%	
Comité Asesor Gubernamental				
Olga Cavalli	SOI	22/05/2019	95.6%	
Rahul Gosain	SOI	03/04/2019	75.0%	
Ryan Carroll	SOI	18/12/2019	100.0%	

Unidad Constitutiva de Proveedores de Servicios de Internet y Servicios de Conectividad				
Suman Lal Pradhan	SOI	03/04/2019	33.3%	
Grupo de Partes Interesadas No Comerciales				
David Cake	SOI	03/04/2019	90.0%	
Tatiana Tropina	SOI	03/04/2019	77.8%	LC
Yawri Carr-Quiros	SOI	17/02/2020	100.0%	
Grupo de Partes Interesadas de Registradores				
Owen Smigelski	SOI	16/04/2019	100%	
Sarah Wyld	SOI	03/04/2019	98.7%	
Theo Geurts	SOI	03/04/2019	80.0%	
Grupo de Partes Interesadas de Registros				
Arnaud Wittersheim	SOI	03/04/2019	80.0%	
Beth Bacon	SOI	22/04/2019	95.7%	
Sean Baseri	SOI	06/11/2019	100.0%	
Comité Asesor de Seguridad y Estabilidad				
Greg Aaron	SOI	05/10/2019	77.8%	
Rod Rasmussen	SOI	03/04/2019	25.0%	

Personal de apoyo activo del plenario del Equipo responsable del EPDP:

Tipo de miembro / Afiliación / Nombre	Manifestación de Interés (SOI)	Fecha de inicio	Asistió %	Función
Personal de Apoyo				
ICANN (Corporación para la Asignación de Nombres y Números en Internet)				
Caitlin Tubergen		3-Abr-2019		LC
Marika Konings		3-Abr-2019		
Berry Cobb		3-Abr-2019		LC
Amy Bivens		3-Jun-2019		LC
Terri Agnew		3-Abr-2019		
Andrea Glandon		3-Abr-2019		
Julie Bisland		20-Jun-2019		
Michelle DeSmyter		20-Jun-2019		
Nathalie Peregrine		3-Abr-2019		

Exparticipantes del plenario del Equipo responsable del EPDP:

Tipo de miembro / Afiliación / Nombre	Manifestación de Interés (SOI)	Fecha de inicio	Asistió %	Función	Fecha de salida
Exparticipante	-				
Miembro	-				
Consejo de la GNSO	-				
Janis Karklins	SOI	3-Abr-2019	97.6%	Presidente	3-Jul-2020
Comité Asesor Gubernamental	-				
Ashley Heineman	SOI	3-Abr-2019	75.7%		21-Oct-2019
Junta Directiva de la ICANN	-				
Leon Felipe Sanchez Ambia	SOI	3-Abr-2019	88.5%	LC	9-Sep-2019
Unidad Constitutiva de Propiedad Intelectual	-				
Alex Deacon	SOI	3-Abr-2019	87.5%		1-Dic-2019
Corporación para la Asignación de Nombres y Números en Internet	-				
Trang Nguyen	-	3-Abr-2019	88.9%	LC	10-Abr-2019
Grupo de Partes Interesadas No Comerciales	-				
Ayden Fabien Férdeline	SOI	3-Abr-2019	73.5%		27-Ene-2020
Farzaneh Badiei	SOI	3-Abr-2019	69.2%		27-Ene-2020
Grupo de Partes Interesadas de Registros	-				
Kristina Rosette	SOI	22-Abr-2019	97.6%		7-Ago-2019
Suplente	-				
Unidad Constitutiva de Propiedad Intelectual	-				
Jennifer Gore	SOI	3-Abr-2019	97.6%		13-Feb-2020

Los registros de asistencia detallados se encuentran disponibles en https://community.icann.org/x/4opHBQ.

Los archivos de los mensajes de correo electrónico del Equipo responsable del EPDP se encuentran disponibles en https://mm.icann.org/pipermail/gnso-epdp-team/.

Anexo D – Designaciones por consenso

A continuación se indica la designación del Presidente en cuanto al nivel de consenso sobre cada recomendación del Informe Final del Equipo responsable del EPDP. Estas designaciones se realizaron siguiendo el proceso que se describe en este enlace y conforme a la sección 3.6 - Metodología estándar para la toma de decisiones de las Pautas para Grupos de Trabajo de la GNSO, así como la Carta orgánica del Equipo responsable del EPDP.

Recomendación n.°	**Designación propuesta por el Presidente**	**Grupos que no apoyan la recomendación o parte de la misma**
1 Acreditación	consenso total	
2 Acreditación de entidades gubernamentales	consenso total	
3 Criterios y contenido de las solicitudes	consenso total	
4 Acuse de recibo	consenso total	
5 Requisitos de respuesta	Fuerte respaldo pero oposición significativa	GAC (exactitud) IPC BC
6 Niveles de prioridad	Divergencia	GAC (no apoya el apartado 6.2) BC (no apoya el apartado 6.2) IPC (no apoya el apartado 6.2) ALAC (no apoya el apartado 6.2) SSAC
7 Propósitos del Solicitante	Consenso	NCSG (condicional a la eliminación de la nota al pie)
8 Autorización de Partes Contratadas	Fuerte respaldo pero oposición significativa	GAC (exactitud y objeción al apartado 8.17) IPC BC
9 Automatización del procesamiento del SSAD	Fuerte respaldo pero oposición significativa	IPC BC ALAC

10 Determinación de los SLA variables para los tiempos de respuesta para el SSAD	Fuerte respaldo pero oposición significativa	RrSG (no apoya los SLA para solicitudes urgentes) SSAC IPC BC
11 Términos y condiciones del SSAD	consenso total	
12 Requisitos de divulgación	Fuerte respaldo pero oposición significativa	GAC (exactitud) SSAC
13 Política de consultas	consenso total	
14 Sostenibilidad financiera	Divergencia	ALAC GAC SSAC IPC BC
15 Registro	consenso total	
16 Auditorías	consenso total	
17 Requisitos de informes	consenso total	
18 Revisión de la implementación de las recomendaciones de políticas relativas al SSAD mediante un Comité Permanente de la GNSO	Fuerte respaldo pero oposición significativa	ALAC BC IPC GAC
19 Visualización de información de proveedores de servicios de privacidad/representación afiliados	consenso total	
20 Campo que especifica la ciudad	Consenso	NCSG
21 Retención de datos	consenso total	
22 Propósito 2	Consenso	NCSG

Anexo E – Declaraciones minoritarias

Comité Asesor At-Large (ALAC)
Unidad Constitutiva de Negocios (BC) / Unidad Constitutiva de Propiedad Intelectual (IPC)
Comité Asesor Gubernamental (GAC)
Grupo de Partes Interesadas No Comerciales (NCSG)
Grupo de Partes Interesadas de Registradores (RrSG)
Grupo de Partes Interesadas de Registros (RySG)
Comité Asesor de Seguridad y Estabilidad (SSAC)

ES

AL-ALAC-ST-0720-04-01-EN
ORIGINAL: English
FECHA: 29 de julio de 2020
ESTADO: Ratificado

COMITÉ ASESOR AT-LARGE

Declaración del ALAC sobre el Proceso Expeditivo de Desarrollo de Políticas (EPDP)

Declaración del ALAC presentada para su inclusión en el Informe Final de la Fase 2 del Proceso Expeditivo de Desarrollo de Políticas (EPDP) sobre la Especificación Temporaria para los Datos de Registración de los gTLD

El ALAC entró en el EPDP y realizó la siguiente declaración:

1. El ALAC considera que el EPDP DEBE tener éxito y trabajará para lograr dicho fin.
2. Tenemos una estructura de apoyo que estamos organizando para asegurarnos de que nuestra comunidad comprenda lo que presentamos aquí y que contamos con su apoyo y sus aportes.
3. El ALAC considera que los registratarios individuales son usuarios y hemos trabajado regularmente en su representación (como en el PDP que iniciamos para proteger los derechos de los registratarios cuando sus dominios caducan), si las necesidades de los registratarios difieren de las de los cuatro mil millones de usuarios de Internet que no son registratarios, las necesidades de estos últimos tienen prioridad. Creemos que el GDPR y este EPDP están en una situación semejante.
4. Aunque algunos usuarios de Internet consultan WHOIS y no podrán hacerlo en algunos casos en el futuro, nuestra principal preocupación es el acceso de los terceros que trabajan para garantizar que Internet sea un lugar seguro para los usuarios, lo que significa que los organismos de aplicación de la ley, los investigadores en materia de ciberseguridad, los que combaten el fraude en los nombres de dominio y otros que ayudan a proteger a los usuarios contra el phishing, malware, spam, fraude y ataques de DDoS, entre otros, pueden trabajar con una reducción mínima del acceso a los datos de WHOIS. Todo ello dentro de las limitaciones del GDPR, por supuesto.

Hemos trabajado con valentía para apoyar el proceso del EPDP y trabajar en nombre de los ahora casi cinco mil millones de usuarios de Internet.

El objetivo de la Fase 2 del EPDP era desarrollar lo que ahora se denomina Sistema Estandarizado de Acceso/Divulgación a datos de registración sin carácter público

(SSAD), así como abordar una serie de cuestiones que no se completaron durante la Fase 1 del EPDP.

Se ha realizado una gran cantidad de trabajo, pero el ALAC considera que si se despliega el SSAD, y cuando se despliegue, la probabilidad de que cumpla los objetivos que necesitan las comunidades cuyos esfuerzos apoyamos será baja. Esas comunidades necesitan tener acceso a datos sin carácter público que sean específicos, exactos y utilizables, y los necesitan de manera oportuna y previsible.

Las metodologías clave para lograrlo incluyen:

- No expandir el alcance de la legislación sobre privacidad. Censurar únicamente los datos protegidos por dichas leyes.
- Asegurarse de que los datos sean precisos, y la información de contacto sea utilizable – es la única razón por la que la información de contacto está ahí.
- En la medida en que sea posible y legal, procesar las consultas de forma automatizada para obtener respuestas rápidas (casi instantáneas cuando sea posible).

Lamentablemente, el Informe Final no hace nada de esto con certeza alguna.

Específicamente:

- La Fase 1 permitió la censura de la información sobre las personas jurídicas (empresas) así como las personas físicas (personas) y la mayoría de los registradores y registros están realizando esa censura completa. También están censurando sin importar la ubicación geográfica.
- Se suponía que la Fase 2 abordaría plenamente la cuestión de persona jurídica vs. física, pero aunque hubo algún debate, la cuestión se ha remitido al Consejo de la GNSO para su posible tratamiento en algún momento futuro.
- El GDPR exige que los datos sean precisos para los fines en que se procesan. En el caso de los datos del RDS, eso es saber quién es el registratario y facilitar el contacto. Los estudios de exactitud de WHOIS han demostrado que, cuando la información estaba disponible públicamente, tenía inexactitudes lamentables. Se suponía que la Fase 2 debía debatir completamente el tema de la exactitud en relación con los datos ahora censurados. Eso no se ha hecho. El Consejo de la GNSO instruyó al PDP para que no abordara este tema y el Consejo de la GNSO considerará abordarlo de una manera aún no definida.

- El contacto con los registratarios se realiza actualmente por medio de métodos (principalmente formularios en la web) que, según los estudios realizados, no son eficaces y no proporcionan información al remitente sobre la medida en que el mensaje pueda haber llegado al registratario. Se remite el debate al Consejo de la GNSO para su posible tratamiento en el futuro.
- Existen algunos casos de uso a los que el SSAD responderá automáticamente. La intención era que, a medida que las leyes y la jurisprudencia y las cuestiones contractuales avanzaran, un mecanismo de "evolución" permitiera manejar más casos de uso de manera automatizada. El mecanismo de evolución recomendado es un Comité Permanente de la GNSO que exija que los nuevos casos de uso sean aprobados no solo por las partes contratadas (que pueden ser objeto de sanciones si no se hace correctamente), sino que también por el Consejo de la GNSO. El Comité Permanente puede recomendar tanto la implementación pura (que requiere la aprobación del Consejo de la GNSO para proceder a la implementación) como la Política (que requeriría un proceso de políticas de la GNSO, como un PDP, antes de poder proceder). No está claro si las nuevas recomendaciones de casos de uso de decisiones del SSAD se tratarían como implementación o si habría que constituir un nuevo PDP (o equivalente) para permitir realmente dicha automatización (agregando potencialmente años para permitir nuevos casos de uso).

  El ALAC, junto con varios otros grupos, aceptó el modelo actual del SSAD a pesar de las fuertes reservas porque nos aseguraron que el mecanismo de evolución permitiría el cambio de manera práctica y oportuna. Dichos cambios no estaban garantizados debido a cuestiones jurídicas y de responsabilidad, pero eran posibles. En base a lo que se sabe ahora sobre el mecanismo de evolución y a la falta de claridad sobre cómo funcionará y cómo será tratada su recomendación por parte del Consejo de la GNSO, el ALAC desde luego nunca hubiera estado de acuerdo con el modelo actual de SSAD.

  Además, aunque una recomendación del Comité Permanente requiere por defecto una mayoría simple de votos del Consejo de la GNSO, es posible que esto pueda modificarse para que se exija una mayoría calificada[48].

[48] Un voto por mayoría calificada permite que un solo Grupo de partes interesadas más otro miembro de la Cámara veten cualquier acción de la GNSO.

- El modelo financiero es problemático. A primera vista, tal vez no sea irrazonable que los usuarios del SSAD asuman una parte significativa de los costos operativos, pero al fijar los precios para intentar garantizarlo, es posible que se fijen tan altos que desalienten su uso. Esto no solo daría lugar a que no se cumplieran esos objetivos financieros, sino que anularía efectivamente toda la iniciativa. Debe haber flexibilidad en la fijación de precios para asegurar que el SSAD sea realmente utilizable. A tal fin, actualmente no está claro hasta qué punto la ICANN pueda necesitar subvencionar el servicio.

Todas estas cuestiones se deben a que, o bien el EPDP recibió instrucciones de no abordarlas, o bien decidió no hacerlo, o bien dejó la redacción de la recomendación lo suficientemente vaga como para no proporcionar ningún nivel de confianza en los resultados.

Todos estos temas PODRÍAN ser tratados adecuadamente por el Consejo de la GNSO mientras delibera sobre este Informe Final.

Por consiguiente, el ALAC apoya CONDICIONALMENTE este informe, con sujeción a las medidas del Consejo de la GNSO que se especifican a continuación.

Si no se pueden alcanzar estos resultados, el ALAC considera que este informe daría lugar a una implementación de varios años que resultaría en un sistema que sería efectivamente un sistema de tickets pretensioso, excesivamente complejo y muy costoso. Por lo tanto, el Informe Final, en su totalidad aunque excluidas las Recomendaciones 19 - 22, no contaría con nuestro apoyo[49].

Resultados del Consejo de la GNSO necesarios para que el ALAC apoye el Informe Final del EPDP:

1. El Consejo de la GNSO acuerda que cualquier recomendación del Comité Permanente de Evolución sobre casos de uso adicionales de decisiones del SSAD (que estén en plena conformidad con la Recomendación 9.3 de la Política del EPDP) se tratará como una implementación y no requerirá más deliberaciones de políticas.
2. Los temas de Distinción entre persona jurídica y persona física, Exactitud, Sistema de Informes sobre la Exactitud de los Datos de WHOIS y Correo electrónico de contacto anonimizado se abordarán en su totalidad con plena participación en todos los aspectos de los debates de los Comités Asesores de la ICANN que deseen participar. Si estos temas se consideran

[49] A los efectos de evitar dudas, si no se cumplen las condiciones, la ALAC seguirá apoyando las Recomendaciones 19 - 22 pero no el resto del informe.

cuestiones de política, deben ser abordadas por un grupo facultado para realizar recomendaciones de política, dirigido por un presidente cualificado y sin conflictos de intereses. El GAC, el ALAC y el SSAC deben participar en el establecimiento del mandato o carta orgánica de dichos grupos. El objetivo para la finalización de todos los trabajos debería ser dentro de un plazo no mayor a abril de 2021.

3. El Consejo de la GNSO está de acuerdo en que para ratificar las recomendaciones del Comité Permanente de Evolución solo se requerirá una mayoría de la GNSO, como se solicita actualmente en el Manual de Políticas de la GNSO.
4. El Consejo de la GNSO reconoce que las deliberaciones durante la implementación de fijación de precios del SSAD deben contar con la participación de los futuros usuarios potenciales del SSAD y no solo se debe considerar la recuperación de los costos, sino también la capacidad y la voluntad real de los usuarios del SSAD de pagar los precios que se fijen.

Aprobado por unanimidad por el ALAC, 29 de julio de 2020
Presentado en representación del ALAC por Alan Greenberg

Anexo a la Declaración Minoritaria del ALAC para el Informe Final de la Fase 2 del EPDP

Los miembros del Comité Asesor At-Large (ALAC) agradecen la oportunidad de presentar este Anexo a la declaración que se presentó el 29 de julio de 2020.

El ALAC, junto con su Equipo responsable del EPDP, ha tenido ahora la oportunidad de revisar y debatir las declaraciones presentadas por la BC/IPC, el GAC y el SSAC, junto con las que presentaron los demás grupos miembros del EPDP.

Aunque el ALAC y la BC, la IPC, el GAC y el SSAC adoptaron cada uno un enfoque algo diferente para abordar nuestras posiciones con respecto al informe, el ALAC está en general de acuerdo con las posiciones adoptadas en las declaraciones del GAC, el SSAC y la BC/IPC. En particular, el ALAC aprecia el análisis profundo y exhaustivo proporcionado por el GAC, el SSAC y la BC/IPC.

El disentimiento sobre los resultados de lo que ha sido más de un año de debates muy desafiantes no es algo que el ALAC haya tomado a la ligera. Para que quede claro, no se trata de una situación, como se ha insinuado, en la que estemos en desacuerdo porque "no nos hemos salido con la nuestra". Proceder sin abordar las cuestiones que creemos que son fundamentales para el éxito de un SSAD dará lugar a un sistema que no cumplirá con las necesidades de los usuarios del SSAD, con pocas oportunidades de corregir significativamente esos problemas en el futuro. Esperamos que la GNSO y, si corresponde, la Junta Directiva lo tengan en cuenta a medida que avance este proceso.

Ratificado por el ALAC, 24 de agosto de 2020.

Declaración Minoritaria de la Unidad Constitutiva de Negocios (BC) y la Unidad Constitutiva de Propiedad Intelectual (IPC) sobre el Informe Final de la Fase 2 del EPDP

El Informe Final de la Fase 2 del EPDP no ofrece un Sistema de Acceso Estandarizado que cumpla con las necesidades de sus usuarios. En consecuencia, la Unidad Constitutiva de Negocios (BC) y la Unidad Constitutiva de Propiedad Intelectual (IPC) deben disentir.

Como se señala en nuestra declaración sobre el Informe Final de la Fase 1 del EPDP, la BC y la IPC son firmes partidarias del modelo de múltiples partes interesadas de la ICANN ascendente y basado en el consenso, como lo demuestra nuestra participación activa y de buena fe en este EPDP. La Fase 2 del EPDP se constituyó para crear un sistema estandarizado, con el doble objetivo de proteger los datos personales de los registratarios y proporcionar a los usuarios un acceso consistente, oportuno y previsible a los datos de los registratarios cuando los usuarios tengan necesidad de procesarlos legalmente para sus fines legítimos. Debido a que el Informe Final de la Fase 2 no logra este objetivo, dicho informe es inaceptable.

Preocupaciones compartidas

La IPC y la BC apoyan la protección de la privacidad de los datos personales, y la ley de privacidad procura un equilibrio entre el derecho individual a la privacidad y otros intereses legítimos. Lamentablemente, el Informe Final de la Fase 2 no logra este equilibrio. Este fracaso va en detrimento de los que protegen sus propios derechos fundamentales y de los que actúan en beneficio del interés público u otros intereses legítimos. Los intereses de los miembros de la BC incluyen la promoción de la confianza de los usuarios en las comunicaciones en línea y en las interacciones comerciales (como se indica en la Directiva NIS de la UE, por ejemplo). Entre los intereses de los miembros de la IPC se incluye la protección de los consumidores contra el phishing, los productos falsificados peligrosos y otros fraudes, según lo dispuesto en el Artículo 38 de la Carta de los Derechos Fundamentales de la UE, así como la protección de la propiedad intelectual, según lo dispuesto en el Artículo 17, Sección 2, de la Carta de los Derechos Fundamentales de la UE.

La IPC y la BC señalan que el Informe Final de la Fase 2 no aborda varias de las preocupaciones planteadas por la Comisión Europea y la Autoridad de Protección de Datos (DPA) de Bélgica, así como por los propios comités asesores de la ICANN: el Comité Asesor Gubernamental (GAC), que representa los intereses de los organismos encargados del cumplimiento de la ley y la protección del consumidor, el Comité Asesor At-Large (ALAC), que representa los intereses de los usuarios finales de Internet, y el Comité Asesor de Seguridad y Estabilidad (SSAC), responsable de asesorar a la Junta Directiva de la ICANN sobre cuestiones relacionadas con la seguridad e integridad de los sistemas de asignación de nombres y direcciones de Internet.

Preocupaciones compartidas con la Comisión Europea y la DPA de Bélgica

La Comisión Europea[50] instó "*a la ICANN y a la comunidad a que desarrollen un modelo de acceso unificado que se aplique a todos los registros y registradores y que proporcione un método estable, previsible y viable para acceder a los datos de registración de gTLD sin carácter público para los usuarios con un interés legítimo u otro fundamento jurídico, conforme a lo dispuesto en el Reglamento General de Protección de Datos (GDPR)*". La Comisión Europea declaró que consideraba esto "*vital y urgente*" e instó a la ICANN a "*desarrollar e implementar un modelo de acceso pragmático y viable en el menor tiempo posible...*" La DPA de Bélgica, que es la autoridad supervisora de la ICANN debido a su constitución de la UE en Bélgica, se refirió al modelo centralizado como una "*mejor opción de 'sentido común' en términos de seguridad y para los titulares de los datos*".[51] Lamentablemente, el Informe Final de la Fase 2 no proporciona un método de acceso en absoluto y, mucho menos, un método que podría describirse como "*estable, predecible y viable*". Por el contrario, el Informe Final de la Fase 2 solo prevé una ubicación central para presentar las solicitudes. Al hacerlo, rechaza el asesoramiento de la DPA de Bélgica a favor de dejar la decisión sobre si divulgar o no los datos a discreción de más de dos mil partes contratadas separadas, ninguna de las cuales está obligada, en virtud de los contratos o políticas de la ICANN, a emplear un asesor jurídico, un delegado de protección de datos o un profesional en materia de privacidad.

Preocupaciones de la BC y la IPC que son compartidas por el GAC

También compartimos las preocupaciones del GAC por el hecho de que el Equipo responsable del EPDP no haya abordado las cuestiones sobre la exactitud de los datos y la distinción entre personas jurídicas y físicas. En su carta del 22 de junio al Consejo de la GNSO[52], el GAC señaló que "*Estas cuestiones son fundamentales para el interés público. Si no se abordan estas cuestiones como parte del actual EPDP se corre el riesgo de que el sistema sea incompleto y carezca de capacidades clave que promuevan la seguridad pública. Además, el hecho de que no se aborden estas importantes cuestiones arroja dudas sobre la legitimidad y la eficacia del proceso de elaboración de políticas de la GNSO para abordar cuestiones de importancia para las partes interesadas no pertenecientes a la GNSO y el interés público*". Lamentablemente, los alegatos del GAC fueron ignorados en la Fase 2. Aunque el GDPR requiere la exactitud de los datos, el Consejo de la GNSO eliminó la exactitud de la competencia del trabajo de la Fase 2 del EPDP, y el Informe Final de la fase 2 no abordó la necesidad de distinguir a los registratarios entre personas jurídicas y personas físicas.

[50] Véase: https://www.icann.org/en/system/files/correspondence/odonohue-to-marby-03may19-en.pdf
[51] Véase: https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority
[52] Véase: https://gac.icann.org/advice/correspondence/outgoing/GAC%20Chair%20letter%20to%20GNSO%20Council%20Chair%20-%20Next%20Steps%20on%20Key%20Policy%20Issues%20not%20Addressed%20in%20EPDP%20Phase%202.pdf

Preocupaciones de la BC y la IPC que son compartidas por el SSAC y el ALAC

El comentario del SSAC sobre el Informe Inicial de la Fase 1 del EPDP (SSAC 111[53]) suscitó numerosas preocupaciones en el sentido de que las recomendaciones "*estarían muy lejos de lo que el SSAC considera necesario y posible para abordar los problemas de seguridad y estabilidad en el ámbito de la ICANN*". Del mismo modo, el ALAC también expresó su preocupación por el hecho de que no se abordaran las cuestiones relacionadas con la distinción de los registratarios entre personas jurídicas y físicas y la exactitud, entre otras, en su Declaración del 5 de mayo de 2020 sobre el Anexo al Informe Inicial[54].

Errores significativos del Informe Final de la Fase 2 del EPDP

Además de las preocupaciones previamente declaradas por el GAC, el ALAC y el SSAC, los siguientes errores del Informe de la Fase 2 hacen que la BC y la IPC disientan.

- ***Falta de divulgación centralizada y mecanismos de evolución insuficientes***. Después de la Fase 1, esperábamos desarrollar una política de apoyo a la toma de decisiones centralizada. Las ineficiencias e incoherencias inherentes a la descentralización de la toma de decisiones son evidentes: mayores costos para las partes contratadas, tramitación más lenta de las solicitudes de divulgación y mayor probabilidad de que surjan controversias entre los solicitantes y los encargados de la divulgación, dado que cada parte contratada aplica su propio juicio subjetivo a cada solicitud.

  No obstante, en aras del compromiso acordamos considerar (aunque no aceptar) un modelo híbrido propuesto en el que las decisiones de divulgación serían inicialmente en su mayor parte descentralizadas y manuales, pero que evolucionaría hacia un procesamiento automatizado y centralizado sobre la base de la experiencia adquirida durante la implementación del SSAD y la creciente claridad jurídica en relación con la interpretación de los requisitos del GDPR.

  Con el transcurso del tiempo, esperábamos que el sistema, con las medidas de protección apropiadas, proporcionara automáticamente los datos de los registratarios solicitados para fines legítimos establecidos, a los solicitantes acreditados con sus propios fundamentos jurídicos. Por ejemplo, los solicitantes acreditados con pruebas razonables de ventas de falsificaciones o de infracción de los derechos de autor, presentadas bajo pena de perjurio, deberían recibir de manera rápida y previsible los datos de los registratarios para los nombres de dominio pertinentes. La claridad, la coherencia y la escalabilidad de dicho

[53] Véase: https://www.icann.org/en/system/files/files/sac-111-en.pdf
[54] Véase: https://atlarge.icann.org/advice_statements/13775

sistema aumentarían enormemente la confianza y la responsabilidad del DNS, como siempre lo ha hecho el acceso a esos datos, pero no está previsto en el Informe Final de la Fase 2.

El Informe de la Fase 2 no permite a la ICANN evolucionar hacia su función natural de responsable centralizado de la toma de decisiones. En cambio, tiene el efecto de proporcionar a las partes contratadas una discreción indebida para interpretar individualmente sus obligaciones en el marco del GDPR y sus contratos con la ICANN sin ningún requisito de razonabilidad, uniformidad u otras medidas de protección. Tampoco proporciona un mecanismo adecuado que permita la centralización y la automatización en el futuro. De este modo, bloquea permanentemente las ineficiencias de la descentralización de la toma de decisiones, como las que dan lugar a SLA excesivamente largos, incluso para las solicitudes urgentes relacionadas con amenazas inminentes a la vida o a la infraestructura crítica. Recomendaciones 9 y 18:

- ***No se distingue entre personas físicas y jurídicas***. Al proporcionar a las partes contratadas la exclusiva discreción de determinar si deben diferenciar entre personas físicas y jurídicas, el Informe de la Fase 2 no aporta claridad en cuanto al acceso a los datos de registratarios para *personas jurídicas* que no están contempladas por el GDPR. El Equipo responsable del EPDP procuró y recibió asesoramiento jurídico de Bird & Bird, el asesor jurídico externo que el EPDP había contratado para que proporcione asesoramiento sobre las obligaciones del GDPR, sobre cómo distinguir a los registratarios entre personas jurídicas y personas físicas. Pero luego no lo analizó, a pesar de las objeciones de la IPC, la BC, el GAC, el SSAC y el ALAC. La continua censura generalizada de los datos de contacto de las personas jurídicas no es exigida por el GDPR[55], y erosiona la confianza, la responsabilidad y la transparencia del DNS. Por lo tanto, esto representa un incumplimiento inaceptable del EPDP. (Recomendación 8)

- ***No se aborda la exactitud de los datos***. El Informe de la Fase 2 no aborda la cuestión fundamental de la exactitud de los datos de los registratarios, como acordó el EPDP en la Fase 1, a pesar de que hoy en día existen instrumentos adecuados para verificar la exactitud de los datos de los registratarios. La inexactitud de los datos de WHOIS ha sido problemática durante más de 20 años. El Equipo responsable del EPDP no siguió el asesoramiento jurídico que había solicitado con respecto a la interpretación de los requisitos de exactitud en virtud del GDPR. El Equipo responsable del EPDP tampoco siguió el asesoramiento de la Comisión Europea, que confirmó que la exactitud de los

[55] Los comentarios presentados por Afnic para el Anexo de la Fase 2 apoyan esta opinión. "*Quisiéramos compartir nuestra preocupación por el enfoque que propone no distinguir a los registratarios entre personas jurídicas y físicas. Como ya han señalado muchos comentaristas, creemos que se trata de una aplicación excesiva del GDPR. A pesar de que el GDPR no protege datos relativos a personas jurídicas, quisiéramos recordar a la ICANN que en su carta con fecha del 11 de diciembre de 2017, el WP29*

datos no es únicamente en beneficio del titular de los datos. Los datos evidentemente falsos no están protegidos por las leyes de privacidad de datos, y preservar la censura generalizada de datos falsos o ficticios de registratarios del DNS representa otro fracaso del EPDP, que erosiona aún más la confianza, la responsabilidad y la transparencia en el DNS. (Conclusión 2)

- ***Políticas de cumplimiento inadecuadas***. El Informe de la Fase 2 carece de responsabilidad contractual para que las partes contratadas proporcionen datos en respuesta a solicitudes legítimas. Como se ha mencionado anteriormente, el Informe de la Fase 2 no proporciona adecuadamente una base objetiva y un procedimiento consistente, previsible y escalable para que los usuarios acreditados obtengan de manera confiable datos precisos sobre los registratarios cuando existan fundamentos jurídicos y fines legítimos para solicitar y utilizar los datos, incluso cuando los datos no deberían haberse ocultado en primer lugar. El Informe de la Fase 2 no permite a la ICANN exigir el cumplimiento de las débiles recomendaciones realizadas en el Informe. Un SSAD descentralizado tiene poco valor si no existe un mecanismo que garantice el cumplimiento de la Política de consenso. Lamentablemente, este Informe solo contempla la fiscalización de los requisitos de procedimiento y no permite que el departamento de Cumplimiento de la ICANN revise las denegaciones indebidas de solicitudes legítimas. Esto socava y deslegitima toda la política. Recomendaciones 5 y 8:

El resultado es un Informe de la Fase 2 que recomienda un sistema y unas políticas totalmente inadecuadas para cumplir los objetivos declarados y acordados de un SSAD, incluidas las necesidades de sus usuarios. Como resultado, el Informe de la Fase 2 no mantiene la confianza, la seguridad y la resiliencia del DNS.

Al elaborar esta política es esencial que la comunidad de la ICANN apoye los esfuerzos para hacer frente al creciente uso indebido de los nombres de dominio que amenaza la seguridad, la estabilidad y la resiliencia del DNS y del ecosistema de Internet en general, incluida la seguridad de sus usuarios finales. Recientemente, Neustar, una parte contratada, que aborda el crecimiento general del tráfico de Internet debido a la pandemia de COVID-19 y los ciberataques que la acompañan, informó que "*Neustar esperaba un aumento, pero estamos viendo un dramático repunte en los ataques usando prácticamente todas las métricas que medimos. Hemos observado un aumento en el número total de ataques, así como en la gravedad de los mismos...*"[56] Además de señalar que ha "*mitigado más del doble el número de ataques en el primer trimestre de 2020 que en el primer trimestre de 2019*", Neustar informó de "*un aumento en los casos de secuestro del DNS, una técnica en la que la configuración del DNS redirige al usuario a un sitio web que puede parecer el mismo en la superficie pero que a menudo contiene malware disfrazado de algo útil*"

[56] Véase: https://www.home.neustar/resources/whitepapers/covid-19-online-traffic-and-attack-data-report

Designaciones de consenso

La IPC y la BC recuerdan al Consejo de la GNSO y a la Junta Directiva de la ICANN que el Informe Final de la Fase 2 del EPDP define la política para un **sistema** único (a saber, el SSAD). Si bien la convocatoria al consenso tiene lugar en función de cada recomendación, las recomendaciones están intrínsecamente interrelacionadas e interconectadas debido a su impacto e influencia en el conjunto del SSAD. Por lo tanto, el resultado de la convocatoria al consenso debería considerarse de manera integral a nivel del sistema, en lugar de hacerlo estrictamente en función de cada recomendación.

Recomendación n.°	
1 Acreditación	Support (Ayuda)
2 Acreditación de entidades gubernamentales	Support (Ayuda)
3 Criterios y contenido de las solicitudes	Support (Ayuda)
4 Acuse de recibo	Support (Ayuda)
5 Requisitos de respuesta	Oposición
6 Niveles de prioridad	Oposición
7 Propósitos del Solicitante	Support (Ayuda)
8 Autorización de Partes Contratadas	Oposición
9 Automatización del procesamiento del SSAD	Oposición
10 Determinación de los SLA variables para los tiempos de respuesta para el SSAD	Oposición
11 Términos y condiciones del SSAD	Support (Ayuda)
12 Requisito de divulgación	Support (Ayuda)
13 Política de consultas	Support (Ayuda)
14 Sostenibilidad financiera	Oposición
15 Registro	Support (Ayuda)
16 Auditorías	Support (Ayuda)
17 Requisitos de informes	Support (Ayuda)
18 Revisión de la implementación de las recomendaciones de políticas relativas al SSAD mediante un Comité Permanente de la GNSO	Oposición

19 Visualización de información de proveedores de servicios de privacidad/representación afiliados	Support (Ayuda)
20 Campo que especifica la ciudad	Support (Ayuda)
21 Retención de datos	Support (Ayuda)
22 Propósito 2	Support (Ayuda)

Además, la IPC y la BC se oponen al texto empleado en las siguientes secciones de no recomendación:

- Sección 1.2 y 2.3 (descripción de "artículos no tratados"). No apoyamos la descripción del resultado de la distinción entre persona jurídica y física.
- Sección 3.1 (descripción de cómo llegamos al modelo "híbrido"). Nuestra aceptación del paso a un modelo híbrido estaba condicionada a la capacidad de trasladar las decisiones centralizadas al Administrador de la puerta de enlace central (CGM) a lo largo del tiempo utilizando un Mecanismo de evolución que respaldara eso.
- Conclusión - Exactitud (página 60).

Evaluación del valor general para los Solicitantes

Si bien el equipo de la Fase 2 del EPDP dedicó mucho tiempo y esfuerzo a analizar la sostenibilidad financiera del propio SSAD, creemos que es igualmente importante analizar los costos y beneficios desde el punto de vista de los usuarios (es decir, los usuarios del sistema que procuran la divulgación de los datos de los registratarios). Esto es crucial dado que la política de la Fase 2 establece que los solicitantes paguen la mayor parte, si no la totalidad, de los costos del funcionamiento y el mantenimiento del SSAD, por lo tanto, prevemos que las tarifas de acreditación y solicitud que pagarán los solicitantes serán significativas.

Además, la política del SSAD, tal como está definida actualmente, tendrá un impacto material más allá de los costos directos en aquellos que históricamente han confiado en los datos de WHOIS. Estos costos indirectos están relacionados con los siguientes aspectos:

- **Respuesta no oportuna**: Debido a las errores descritos anteriormente, el plazo de respuesta a las solicitudes de divulgación será inaceptablemente largo, lo que repercutirá en la eficiencia de los procesos relacionados con la investigación y la gestión de las cuestiones de uso indebido e ilegalidad.

- **Incompletitud**: Debido a que ya no existe la posibilidad de realizar las denominadas búsquedas "inversas", ahora es más difícil identificar todos los dominios asociados a un evento o ataque.

- **No atribución**: La supresión de las búsquedas inversas interfiere con la capacidad de atribuir una actividad delictiva o de uso indebido con un registratario (actor) en una ventana de respuesta significativa (si la hay). Los solicitantes, especialmente los primeros en responder a los ataques cibernéticos, dependerán en mayor medida de factores de proximidad en lugar de atribución para desplegar contramedidas o mitigar los ataques.

- **Inexactitud**: No existe garantía que los datos devueltos sean exactos, ni existen disposiciones para que partes independientes auditen los datos de registración para comprobar su exactitud. Los solicitantes deben cargar con el costo de las solicitudes de divulgación sin tener la certeza de la utilidad o el valor de la respuesta.

- **No contención**: La incapacidad de realizar una enumeración oportuna y completa de los dominios asociados a una actividad delictiva o de uso indebido retrasa la mitigación de la primera respuesta a los ciberataques. Por lo tanto, los ataques persistirán mucho más allá de los objetivos históricos de mitigación de 1 a 4 horas. Los SLA, tal como se definen actualmente, son insuficientes para abordar cuestiones como el phishing, que tiene una duración de horas en lugar de días, o los ataques de malware que infligen costos o pérdidas graves y directas a sus víctimas.

- **Imprevisibilidad**: Un modelo de divulgación descentralizado y distribuido dará lugar a un sistema imprevisible y poco confiable de acceso y divulgación. De esta forma, se bloquean los esfuerzos de los solicitantes que tratan de obtener información de múltiples partes contratadas para un gran número de dominios asociados a una sola actividad de ciberdelincuencia o uso indebido.

Siempre hemos reconocido la necesidad de pagar tarifas de acreditación para utilizar el SSAD. Sin embargo, queda claro que el valor y los beneficios del SSAD, definidos en el Informe Final de la Fase 2, no se acercan a la justificación de los costos (directos e indirectos) de la utilización del SSAD.

Conclusión

Cuando la Junta Directiva de la ICANN adoptó la Especificación Temporaria en mayo de 2018, señaló que *"se prevé que las acciones de la Junta Directiva tengan un impacto inmediato en la seguridad, estabilidad o flexibilidad continuas del DNS, dado que ayudará a mantener a WHOIS en la mayor medida posible mientras la comunidad trabaja para desarrollar una política de consenso".*[57] En la reunión ICANN66 de noviembre de 2019 en Montreal, la Junta Directiva y el Director Ejecutivo de la ICANN reiteraron en el foro abierto la importancia del acceso escalable a los datos de los registratarios para garantizar la seguridad de Internet y de sus usuarios. Los resultados

[57] Véase: https://www.icann.org/resources/board-material/resolutions-2018-05-17-en

de más de dos años de intensa labor del Equipo responsable del EPDP no son más que la afirmación del *statu quo* [previo al EPDP]: los elementos de los datos de WHOIS necesarios para identificar a los propietarios y usuarios de los nombres de dominio son en gran medida inaccesibles para las personas y entidades que sirven a intereses públicos y privados legítimos.

Por los motivos expuestos, las misiones y propósitos aprobados por la Junta Directiva nos obligan a disentir del conjunto de recomendaciones de políticas expuestas en el Informe Final de la Fase 2.

A pesar de las mejores intenciones de la IPC y de la BC, el experimento del EPDP ha fracasado. Se ha demostrado incapaz de manejar una cuestión puramente jurídica creada por el GDPR. Los reguladores y legisladores deberían tener en cuenta que el modelo de múltiples partes interesadas de la ICANN no logró satisfacer las necesidades de protección del consumidor, ciberseguridad y aplicación de la ley. Por consiguiente, es necesario contar con una orientación normativa clara para el GDPR, y buscar enfoques jurídicos y regulatorios alternativos.

Sobre la BC y la IPC

La misión de la Unidad Constitutiva Empresarial y de Usuarios Comerciales (BC), aprobada por la Junta de la ICANN, es "*asegurar que la ICANN sea responsable y transparente en el desempeño de sus funciones y que sus posiciones políticas sean coherentes con el desarrollo de una Internet que... promueva la confianza de los usuarios en las comunicaciones en línea y las interacciones comerciales...*".

El propósito de la Unidad Constitutiva de Propiedad Intelectual (IPC), aprobada por la Junta Directiva de la ICANN, es "*representar las opiniones e intereses de los titulares de propiedad intelectual en todo el mundo, con especial énfasis en los derechos de marcas comerciales, derechos de autor y derechos de propiedad intelectual relacionados y su efecto e interacción con los sistemas de nombres de dominio (DNS), y garantizar que estas opiniones, incluidos los puntos de vista de la minoría, se reflejen en las recomendaciones formuladas por el Consejo de la GNSO a la Junta Directiva de la ICANN*".

Declaración Minoritaria del Comité Asesor Gubernamental sobre el Informe Final de la Fase 2 del EPDP sobre Datos de Registración de gTLD

Nota: *El Comité Asesor At-Large (ALAC), la Unidad Constitutiva de Negocios (BC) y la Unidad Constitutiva de Propiedad Intelectual (IPC) apoyan las opiniones expresadas en este comentario.*

Introducción

El GAC aprecia sinceramente los esfuerzos de todo el Equipo responsable del EPDP, sus dedicados Presidentes y el personal de apoyo de la ICANN durante los últimos 23 meses y reconoce el considerable tiempo y compromiso invertidos en la elaboración de estas complejas e importantes recomendaciones de política relativas al acceso y la divulgación de los datos de registración de nombres de dominio (anteriormente conocido como WHOIS). Los Estatutos de la ICANN reconocen que los datos de WHOIS son esenciales para "las necesidades legítimas de aplicación de la ley" y para "promover la confianza de los consumidores".[58] El GAC también ha reconocido reiteradamente estos importantes propósitos y ha señalado que los datos de WHOIS se utilizan para varias actividades legítimas, entre ellas: ayudar a las autoridades de aplicación de la ley en las investigaciones; ayudar a las empresas a combatir el fraude y el uso indebido de la propiedad intelectual, proteger los intereses del público; y contribuir a la confianza de los usuarios en Internet como medio confiable de información y comunicación.[59]

En reconocimiento de estos propósitos cruciales, la Especificación Temporaria para los Datos de Registración de los gTLD de la ICANN tenía como objetivo "garantizar la disponibilidad continua de WHOIS en la mayor medida posible, manteniendo al mismo tiempo la seguridad y la estabilidad del sistema de identificadores únicos de Internet".[60] Las Recomendaciones finales contienen elementos útiles que constituyen una mejora respecto de la actual Especificación Temporaria que rige el acceso a los datos de registración de nombres de dominio. No obstante, el GAC debe abstenerse de apoyar ciertas recomendaciones que en su forma actual no logran el equilibrio adecuado entre la protección de los derechos de quienes suministran los datos a los registros y registradores y la protección del público de los daños asociados a los actores maliciosos que tratan de explotar el sistema de nombres de dominio.[61] A este respecto, el GAC destaca que el sistema de nombres de dominio es un recurso público

[58] Estatutos de la ICANN, Revisión de Servicios de Directorio de Registración, §4.6(e).
[59] *Véase, por ejemplo, el Comunicado del GAC de Abu Dabi*, Sección VII.3 p.11 y los Principios del GAC de 2007 en relación con los servicios de WHOIS.
[60] *Véase la* página web *de la ICANN sobre Cuestiones de protección de datos/privacidad:* https://www.icann.org/dataprotectionprivacy
[61] El GAC (junto con otros grupos de partes interesadas) objetó las siguientes recomendaciones: 5 - Requisitos de respuesta; 6 - Niveles de prioridad; 8 - Autorización de la parte contratada; 14 - Sostenibilidad financiera; 18 - Revisión de la implementación de las recomendaciones de políticas relativas al SSAD utilizando un Comité Permanente de la GNSO. *Véase* Designaciones por consenso en el Anexo D del Informe Final de la Fase 2 del EPDP.

mundial que debe atender las necesidades de todos sus usuarios, incluidos los consumidores, las empresas, los registratarios y los gobiernos.

En esta Declaración Minoritaria, el GAC proporciona aportes sobre sus preocupaciones en materia de políticas públicas con respecto a las formas en que las Recomendaciones Finales:

1) Concluyeron actualmente con un sistema de divulgación fragmentado en lugar de centralizado.
2) No contienen normas de obligado cumplimiento para revisar las decisiones de divulgación.
3) No abordan suficientemente las preocupaciones relativas a la protección y la confianza del consumidor.
4) No contienen mecanismos confiables para que el Sistema Estandarizado de Acceso/Divulgación (SSAD) evolucione en respuesta a una mayor claridad jurídica.
5) Pueden imponer condiciones financieras que pongan en riesgo un SSAD que exija costos desproporcionados para sus usuarios, incluidos los que detecten y actúen ante las amenazas a la ciberseguridad.

Además, como se destaca en nuestro Comentario del GAC sobre el Anexo al Informe Inicial de la Fase 2 del EPDP, el Informe Final no aborda actualmente ciertas cuestiones clave (en particular, la exactitud de los datos, el enmascaramiento de los datos de las entidades jurídicas no protegidas por el GDPR y el uso de correos electrónicos anonimizados). El modelo también podría mejorarse a partir de nuevas instancias de aclaración sobre el estado y la función de cada uno de los responsables y encargados del tratamiento de datos. El GAC solicita al Consejo de la GNSO que se asegure de que estas importantes cuestiones se aborden con prontitud en este EPDP como una próxima y última Fase 3.

Sistema de divulgación fragmentado

Aunque las Recomendaciones finales proporcionan un sistema centralizado para presentar solicitudes, carece de esa centralización en lo que respecta a la divulgación de datos. Las recomendaciones actuales crean un sistema fragmentado que podría dar lugar a un acceso inadecuado a los datos de registración y podría retrasar las investigaciones de los organismos encargados del cumplimiento de la ley, la propiedad intelectual y la seguridad cibernética. El GAC advirtió contra la creación de "un sistema fragmentado para proporcionar acceso que consistiría en miles de políticas distintas en función del registrador de que se trate", señalando que "la falta de políticas consistentes para acceder a información sin carácter público provoca retrasos" que pueden impedir las investigaciones y permitir que conductas potencialmente

perjudiciales sigan perjudicando al público.[62] En la opinión del GAC, este resultado no es consistente con la expectativa del GAC de "un mecanismo de acceso estable, previsible y viable para la información de WHOIS sin carácter público"[63]. En particular, la Autoridad de Protección de Datos de Bélgica reconoció los beneficios potenciales de un modelo centralizado y reconoció explícitamente que el PIBR no prohíbe la automatización de diversas funciones en un modelo de divulgación. [64]

No obstante, las recomendaciones de divulgación:

- dependen casi enteramente de las evaluaciones y decisiones individuales de los más de 2000 registradores acreditados por la ICANN;[65]
- no abordan suficientemente la función de la automatización y solo prevén dos categorías de respuestas automatizadas;[66] y

- no abordan suficientemente los mecanismos confiables para ampliar las categorías de solicitudes adecuadas para la divulgación automatizada en respuesta a futuros asesoramientos jurídicos o incluso a cambios en la legislación aplicable en materia de privacidad.[67]

El sistema de divulgación actualmente fragmentado, combinado con un marco relativamente incierto para considerar y recomendar una futura centralización, puede obstaculizar la estabilidad y la previsibilidad del SSAD.

Falta de normas exigibles para revisar las decisiones de divulgación

El GAC reconoce que, en virtud de las normas de protección de datos aplicables, incluido el GDPR, es probable que las Partes contratadas sigan siendo responsables de la decisión de divulgar los datos de registración de nombres de dominio, y que puedan enfrentar ciertos riesgos de responsabilidad relacionados con esa decisión. El GAC entiende que las Partes contratadas han tratado, por lo tanto, de mantener el control sobre la decisión de divulgar o no los datos de registración del nombre de dominio. Sin embargo, el GAC señala que esas decisiones descentralizadas sobre la divulgación de

[62] Comunicado del GAC pronunciado en Barcelona (Sección IV.2 Otras cuestiones - en referencia a la Especificación Temporaria, p.6).
[63] Comunicado del GAC pronunciado en Panamá, véase Fundamento del Asesoramiento consensuado del GAC a la Junta Directiva de la ICANN (Sección V.1, p. 7)
[64] https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority
[65] Recomendación (Rec.) 8
[66] Rec. 9.41 y 9.42
[67] Rec. 8.17 y 18

datos están en gran medida exentas de impugnación y de medidas de aplicación, en particular a través de Cumplimiento de la ICANN.[68]

Los datos de registración son importantes para la seguridad y la estabilidad del DNS y existe una preocupación real de que las partes contratadas puedan, inadvertidamente o deliberadamente, no sopesar debidamente el interés público de que el solicitante obtenga esos datos. El Director Ejecutivo de la ICANN transmitió recientemente esta misma preocupación al Comité Europeo de Protección de Datos, y señaló que "debido a la falta de certeza jurídica, es probable que los registradores, en su calidad de responsables del tratamiento de datos, evalúen la privacidad y la protección de los datos en términos absolutos, sin tener en cuenta otros derechos e intereses legítimos, para evitar posibles sanciones regulatorias o un juicio en su contra".[69] La denegación de solicitudes legítimas de acceso a los datos de registración de los nombres de dominio tiene consecuencias reales. El GAC señaló en su Comunicado pronunciado en Barcelona que las encuestas y los estudios indicaban que la implementación de la Especificación Temporaria en respuesta al GDPR tenía un efecto negativo en la capacidad de los organismos encargados del cumplimiento de la ley y los profesionales de ciberseguridad para investigar y mitigar la delincuencia utilizando la información que antes era de dominio público en el sistema WHOIS.[70]

Las recomendaciones actuales no prevén un mecanismo de revisión de las decisiones de divulgación. El sistema propuesto no incluye en esta etapa una función para que el departamento de Cumplimiento de la ICANN revise las impugnaciones sustantivas a las decisiones de divulgación. En cambio, el departamento de Cumplimiento de la ICANN desempeña una función limitada en la revisión de los reclamos relativos al incumplimiento de los requisitos de *procedimiento* o al uso indebido sistémico.[71] En consecuencia, las Recomendaciones del SSAD promueven un sistema que corre el riesgo de fomentar un enfoque conservador de las decisiones de divulgación para

---

68 Rec. 8, Rec. 5.3 y 5.4. ***Véase también*** la carta del 22 de mayo de 2020 del Director Ejecutivo de la ICANN al Comité Europeo de Protección de Datos, https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf.

69 *Véase* la carta del 22 de mayo de 2020 del Director Ejecutivo de la ICANN al Comité Europeo de Protección de Datos, https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf ("La incertidumbre sobre cómo equilibrar los intereses legítimos de acceso a los datos con los intereses del titular de los datos deja mucho al juicio subjetivo y a la discreción del registrador, en su calidad de responsable del tratamiento de datos que recibe una solicitud de acceso, sobre si conceder o denegar el acceso a los datos de registración de gTLD sin carácter público".).

70 *Véase* también la sección 5.2.1 en el Informe Final del Equipo de Revisión 2 de Servicios de Directorio de Registración (3 de septiembre de 2019) y la encuesta conjunta de los Grupos de Trabajo de Anti-phishing y de Anti-Abuso de Mensajes, Malware y Móvil (18 de octubre de 2018).

71 Rec. 5.3-5.5. Además, las pautas para la implementación ni siquiera exigen a las partes contratadas que ajusten su análisis relativo a las decisiones de divulgación "para abordar la jurisprudencia aplicable que interprete el GDPR, las directrices publicadas por el EDPB o las revisiones al GDPR u otras leyes de privacidad aplicables que puedan surgir en el futuro". *Véase* Rec. 8.17. La Guía utiliza la palabra "DEBERÍA" en lugar de "DEBE" y, por lo tanto, no es exigible (véase el correo electrónico al Equipo responsable del EPDP del 19 de diciembre de 2019 de los representantes de la ICANN en el que se habla de la exigibilidad de "DEBERÍA" y "DEBE").

reducir los riesgos de responsabilidad y no prevé adecuadamente una revisión sólida de las decisiones de divulgación en el marco de los mecanismos de cumplimiento efectivo de la ICANN. Conceder a las partes contratadas plena discreción en la revisión de las solicitudes de divulgación puede socavar la obligación de garantizar la viabilidad permanente de los datos de registración de dominios como instrumento para reivindicar los derechos e intereses del público, de los organismos encargados de proteger al público y de las unidades constitutivas comerciales y de propiedad intelectual. El GAC cree que este enfoque propuesto actualmente puede obstaculizar la estabilidad y la previsibilidad del SSAD.

Priorizar las solicitudes que generan preocupación en materia de protección del consumidor

Al GAC le preocupa la inadecuada priorización de las solicitudes de protección del consumidor (con el planteo de cuestiones relacionadas con el phishing, el malware y el fraude)[72], que generan importantes preocupaciones públicas que a menudo requieren una acción inmediata.[73] Las recomendaciones actuales sitúan las solicitudes de protección del consumidor en el más bajo de los tres niveles de prioridad. Además, los correspondientes requisitos de nivel de servicio que rigen los tiempos de respuesta a las solicitudes de Prioridad 3 prevén tiempos de respuesta prolongados: en cinco días durante los primeros seis meses de implementación y luego el tiempo de respuesta se duplica a 10 días a partir de entonces.[74] Esta falta de priorización y los largos tiempos de respuesta podrían provocar importantes daños que los fraudes y los ciberataques pueden causar rápidamente. El GAC recomendaría designar las solicitudes de protección del consumidor como Prioridad 2.

Aunque se aceptara la actual designación de Prioridad 3, la operación sugerida de la Recomendación 6 es motivo de preocupación. El GAC celebra el hecho de que la Recomendación exija la capacidad del solicitante para indicar solicitudes que planteen problemas de protección del consumidor ("Los solicitantes DEBEN tener la capacidad de indicar que la solicitud de divulgación refiere a una cuestión de protección del consumidor. . .").[75] Sin embargo, la Recomendación no incluye un requisito igualmente exigible para que las partes contratadas prioricen a las solicitudes relacionadas con la protección del consumidor sobre otras con el mismo nivel de prioridad. En lugar de utilizar la palabra "DEBEN", las Recomendaciones establecen que las partes contratadas "DEBERÁN" priorizar a estas solicitudes.[76] However, ICANN Compliance expressly informed the EPDP team that the use of the word “SHOULD”

[72] El GAC también observa que la definición propuesta de solicitudes de protección del consumidor parece indebidamente restrictiva y solicita que la propuesta de paréntesis se interprete como ilustrativa en lugar de exhaustiva.

[73] *Véase* Comentario del SSAC sobre el Informe Inicial de la Fase 2 del Proceso Expeditivo de Desarrollo de Políticas sobre la Especificación Temporaria para los Datos de Registración de los gTLD *(*SAC 111) en págs. 9 y 10.

[74] Rec. 6.2 y Rec. 10.4 y 10.11.

[75] Rec. 6.2.

[76] Rec. 6.2

does not create an enforceable obligation[77]. Por lo tanto, esta Recomendación es internamente incoherente en el sentido de que requiere la capacidad de identificar las cuestiones de protección del consumidor, pero no exige que las partes contratadas actúen al respecto de esta designación. Los debates del Equipo responsable del EPDP sobre este tema reflejaron que este objetivo podría lograrse simplemente mediante el uso de un mecanismo de clasificación. Las solicitudes relacionadas con la protección del consumidor plantean cuestiones que afectan a la seguridad general del DNS y, por lo tanto, el GAC recomienda que esta priorización sea obligatoria en lugar de optativa.

Mecanismos confiables para que el SSAD mejore

El SSAD, como todo sistema nuevo, se enfrentaría a desafíos en su ejecución y aplicación y tendría que responder de manera oportuna. Los mecanismos pueden requerir ajustes, las demandas de los solicitantes de datos pueden fluctuar y pueden surgir usos nuevos e imprevistos de los datos, especialmente en el ámbito de la ciberseguridad. Por consiguiente, es fundamental que el potencial del SSAD mejore con el tiempo, se ajuste a los nuevos obstáculos y responda a los nuevos asesoramientos jurídicos.

En cuanto al tema de la automatización, la Recomendación final sobre decisiones de divulgación automatizada exige la automatización para cualquier categoría de solicitudes para las que se determine que la automatización "es un proceso técnica y comercialmente factible y legalmente permitido".[78] Aunque el Equipo responsable del EPDP consideró una serie de casos de uso para la automatización, solo pudo llegar a un acuerdo sobre dos de ellos para incluirlos en el Informe Final.[79] Algunos grupos de partes interesadas, entre ellos el GAC, habían previsto un SSAD que incluía más automatización y centralización porque, como reconocieron los representantes de la Autoridad de Protección de Datos de Bélgica, un modelo centralizado "parece ser una opción mejor y de 'sentido común' en términos de seguridad y para los titulares de los datos".[80] No obstante, el GAC y algunos otros grupos de partes interesadas estuvieron de acuerdo con este modelo "híbrido" en lugar de centralizado, siempre que las recomendaciones finales incluyeran un mecanismo que proporcionara la flexibilidad necesaria para que el SSAD evolucionara y cambiara sin tener que emprender un nuevo esfuerzo de PDP para cada ajuste que fuera coherente con el Informe Final.

En la recomendación 18, se crea un Comité Permanente integrado por representantes de todos los grupos interesados que participaron en el EPDP para que se ocupe de estas decisiones. Sin embargo, el GAC considera que la Recomendación 18, que prevé la revisión de la implementación de las recomendaciones de políticas, no parece

77 *Véase nota al pie 14, anterior*
78 Rec. 9.3.
79 *Véase* Rec. 9.41 y 9.42 (9.43 y 9.44 se refieren a las categorías restringidas de solicitudes únicamente para el campo que especifica la ciudad o los registros que no contienen datos personales).
80 https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority

cumplir el objetivo de proporcionar un mecanismo eficiente para que el SSAD evolucione. En particular, no queda suficientemente claro si los nuevos casos de uso para la automatización comprenden una nueva política o la implementación de la política existente. El GAC observa que si cada nuevo caso de uso se considera una nueva política que requiere un nuevo PDP, no queda claro en esta etapa que el SSAD evolucione efectivamente y, en particular, que avance hacia una mayor centralización. En este escenario, el SSAD podría permanecer fragmentado con todas las preocupaciones que conlleva dicha fragmentación. Por lo tanto, el GAC solicita que la GNSO se asegure de que las recomendaciones del EPDP proporcionen suficiente certidumbre a este respecto y permitan la automatización de otros elementos siempre que se pruebe que es un proceso "técnica y comercialmente factible y legalmente permitido".

Otros requisitos para incluso proponer un cambio incluyen no solo el consenso del Comité Permanente, sino también la aprobación de las partes contratadas. Las recomendaciones necesitarían entonces la aprobación del Consejo de la GNSO (que carece de representación de los Comités Asesores) antes de poder ser adoptadas. Este proceso de "evolución" podría llegar a ser complejo y prolongado, y no es adecuado para abordar cuestiones de implementación que requieran una acción rápida y decisiva.

Sostenibilidad financiera

Las Recomendaciones podrían crear un sistema demasiado costoso para los usuarios a los que está destinado, incluidos los usuarios del SSAD que investigan y combaten las amenazas a la ciberseguridad. Las Recomendaciones establecen que "Los titulares de los datos NO DEBEN sufragar los costos de divulgación de sus datos a terceros; los Solicitantes de los datos del SSAD deberían sufragar principalmente los costos de mantenimiento de este sistema".[81] Si bien el GAC reconoce el atractivo de no cobrar a los registratarios cuando otros desean acceder a sus datos, el GAC también señala que los registratarios asumen los costos de los servicios de registración de dominios en su conjunto cuando registran un nombre de dominio. Como señaló recientemente el SSAC:

> Dichos costos deberían incluir la divulgación a terceros con derecho a obtener datos censurados a fin de llevar a cabo actividades legítimas de seguridad, estabilidad y flexibilidad (SSR) y potencialmente otras actividades jurídicas (por ejemplo, la protección de derechos) que quedan fuera del ámbito de actividades del SSAC. La SSR general del DNS requiere la capacidad de acceder a esos datos para permitir la comunicación con los propietarios de los recursos comprometidos, así como la

[81] Rec. 14.2.

> determinación de actividades fraudulentas y maliciosas que permita la suspensión de los servicios de registración que obtienen los delincuentes.[82]

Además, el GAC señala que gran parte del gasto del SSAD se relaciona con su uso generalizado del procesamiento manual (frente al automatizado), un enfoque con una escalabilidad inherentemente limitada y un costo intrínsecamente elevado. La sostenibilidad financiera del SSAD no puede separarse de su dependencia del procesamiento manual. La reducción del procesamiento manual en la medida de lo posible contribuirá a la sostenibilidad financiera del SSAD.[83] En su conjunto, las Recomendaciones relativas a la financiación del SSAD podrían ser difíciles de implementar y plantean más preguntas de las que responden, en particular: 1) en qué medida puede la ICANN ayudar a subvencionar el sistema; 2) en qué medida pueden los registradores trasladar los costos del SSAD a sus clientes; 3) qué papel tendrían los solicitantes en la fijación y aprobación de las tarifas del sistema, etc. El GAC considera que es aconsejable "una evaluación formal de las repercusiones en los usuarios y de las repercusiones en la seguridad y la estabilidad".[84]

Cuestiones no abordadas en el Informe Final de la Fase 2 del EPDP

Exactitud de los datos

En la Carta orgánica del EPDP se encomendaba al equipo que evaluara "el marco (o marcos) de divulgación [...] para abordar (i) las cuestiones relacionadas con el uso indebido de las registraciones de nombres de dominio, incluidos, entre otros, la protección del consumidor, la investigación del ciberdelito, el uso indebido del DNS y la protección de la propiedad intelectual, [y] (ii) las necesidades de una aplicación de la ley adecuada. . . ” La eficacia de los datos del Registración de nombres de dominio para estos fines (de hecho, para cualquier fin, incluida la capacidad de las partes contratadas de contactar a sus clientes) depende de la exactitud de los datos. Además, la exactitud de los datos de registración es un requisito esencial del GDPR y en el Informe Final de la Fase 1 del EPDP se declaró que: “se prevé considerar más el tema de la exactitud en cuanto al cumplimiento del GDPR . . .” Por lo tanto, al GAC le preocupa la ausencia de recomendaciones sobre este tema vital en el Informe Final.

Como el GAC ha enfatizado anteriormente:

> La exactitud de los datos de registración de nombres de dominio es fundamental tanto para el GDPR como para el objetivo de mantener un DNS seguro y resiliente. El GDPR, así

[82] SAC 111.

[83] Otro tema que alentaría un procesamiento menos manual sería estudiar qué mecanismos permitidos legalmente podrían implementar las partes contratadas para permitir que los titulares de los datos presenten libremente su consentimiento u objeción a la divulgación de sus datos en el momento de la registración del nombre de dominio. Esto facilitaría el mantenimiento de las bases de datos de información protegida frente a la no protegida, abriendo las bases de datos no protegidas a un procesamiento automatizado de menor costo.

[84] *Véase SAC 111.*

> como otros regímenes de protección de datos y el Acuerdo de Acreditación de Registradores de la ICANN, requieren la exactitud de los datos y dicha exactitud es fundamental para el mandato de la ICANN de garantizar la seguridad, estabilidad, confiabilidad y resiliencia del DNS. Como se indica en la carta de la Comisión Europea a la ICANN del 7 de febrero de 2018: "*según lo estipulado en el marco jurídico de protección de datos de la Unión Europea y de conformidad con las obligaciones de las partes contratadas en virtud de sus contratos con la ICANN, los datos personales serán exactos y se mantendrán actualizados. Se deben tomar todas las medidas razonables para garantizar que los datos personales que sean inexactos, teniendo en cuenta los fines para los que se procesan, se borren o rectifiquen sin demoras [...]. Para cumplir con el principio de calidad de los datos, deben tomarse medidas razonables para garantizar la exactitud de cualquier dato personal obtenido*".[85]

De acuerdo con el GDPR, es esencial que se garantice la exactitud y calidad de los datos en relación "con la finalidad para la cual [los datos] se procesan".[86] La divulgación de datos inexactos sería contraria al propósito del SSAD y significaría un riesgo de infringir las normas de protección de datos. La exactitud es un principio básico de protección de datos en la mayoría de las leyes de protección de datos de todo el mundo. En particular, el requisito de exactitud está estipulado en el Artículo 5 del GDPR.

La eficacia de los actuales requisitos contractuales vigentes para promover la exactitud de WHOIS parece ser incierta. Los recientes informes del equipo de revisión plantean preguntas sobre la eficacia de los procedimientos de verificación, como los informes del Equipo de Revisión del RDS y del Equipo de Revisión de CCT, ambos avalados por el GAC.[87] Además, desde 2014, la exactitud de WHOIS comprende la categoría de reclamos más grande entre los reclamos comunicados al departamento de Cumplimiento de la ICANN en relación con los Registradores.[88]

---

85 Comentario del GAC sobre el Anexo de la Fase 2.

86 *Véase GDPR Art. 5(1)(d). Consulte también* la Guía de la Oficina de la Comisión de Información del Reino Unido sobre el GDPR, Orientación para las organizaciones, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/

87 *Véase, por ejemplo,* Informe Final de la Revisión de Servicios de Directorio de Registración (RDS)-WHOIS2 págs. 49 - 61 (que señala que los índices de inexactitud de WHOIS siguen siendo elevados y probablemente no se informen suficientemente); Comentarios del Comité Asesor Gubernamental sobre el Informe Final del Equipo de Revisión RDS-WHOIS2, con fecha del 23 de diciembre de 2019, págs. 5 - 7; Informe Final del Equipo de Revisión de Competencia, Confianza y Elección de los Consumidores págs. 103-06. *Véase también* el Informe del Equipo de Revisión de WHOIS (11 de mayo de 2012), págs. 11 - 13 ("el bajo nivel de datos precisos de WHOIS es inaceptable y disminuye la confianza en WHOIS de los consumidores, en la industria que coordina la ICANN y para la cual la establece normas y, por tanto, en la propia ICANN").

88 *Véase* los Informes Anuales de Cumplimiento Contractual de la ICANN, Detalles del informe sobre registradores, 2014-2019, https://features.icann.org/compliance/dashboard/report-list.

Por lo tanto, el GAC insta al Consejo de la GNSO que solicite al actual EPDP que se ocupe de esta cuestión para que la exactitud de los datos se incluya como componente integral del SSAD.

Persona Física/Jurídica

En el Comunicado del GAC de la reunión ICANN68 del 27 de junio de 2020, el GAC había solicitado una actualización de la GNSO, lo antes posible, sobre sus avances en la elaboración de un plan específico para continuar el proceso de desarrollo de políticas para abordar la cuestión no resuelta relacionada con la distinción entre personas físicas y jurídicas. Esta cuestión es importante porque las normas de protección de los datos personales, incluido el GDPR, únicamente se aplican y protegen el procesamiento de los datos personales de las personas físicas.[89] La información relativa a las personas jurídicas no se considera como datos personales en virtud de las normas de protección de datos personales, incluido el GDPR, si no permite la identificación de personas. Por lo tanto, las partes contratadas podrían poner dichos datos a disposición del público sin que ello suscitara preocupaciones en materia de protección de datos. No obstante, como se refleja en el Informe Final, los Registradores y Operadores de registros siguen estando *autorizados* pero no *obligados* a diferenciar las registraciones de personas jurídicas de las físicas.[90] Esta práctica no "garantiza la disponibilidad continua de WHOIS en la mayor medida posible"[91] y la falta en el Informe Final de procedimientos recomendados aplicables a esta distinción no cumple la directiva expresa de la Fase 1 del Equipo responsable del EPDP y la Carta orgánica del Equipo responsable del EPDP[92].

El efecto de ocultar los datos que legalmente se permite que permanezcan a disposición del público es significativo debido al gran número de dominios registrados a entidades jurídicas. Un estudio encargado por la ICANN en 2013 indicó que **las entidades jurídicas constituían la categoría de mayor porcentaje de registratarios de nombres de dominio**.[93] Consultar la información de registración de nombres de

---

89 El GDPR no abarca el procesamiento de datos personales que se refieran a personas jurídicas y, en particular, a empresas establecidas como personas jurídicas, incluidos el nombre y la forma de la persona jurídica y los datos de contacto de la persona jurídica (Considerando 14) GDPR. “Si bien los datos de contacto de una persona jurídica quedan fuera del ámbito del GDPR, los datos de contacto relativos a las personas físicas están dentro del ámbito del GDPR, así como cualquier otra información relativa a una persona física identificada o identificable" (*Véase la* carta del EDPB a la ICANN de 5 de julio de 2018).

90 *Véase* la Sección 2.3 del Informe Final de la Fase 2 del EPDP, Temas de Prioridad 1 y Prioridad 2.

91 *Véase la* página web *de la ICANN sobre Cuestiones de protección de datos/privacidad:* https://www.icann.org/dataprotectionprivacy

92 *Véase la Carta orgánica del Equipo responsable del EPDP:* https://gnso.icann.org/sites/default/files/file/field-file-attach/temp-spec-gtld-rd-epdp-19jul18-en.pdf(que incluía indicaciones para que el equipo considere si se debería permitir o exigir a las partes contratadas que traten a las personas físicas y jurídicas de manera diferente, y qué mecanismo se necesita para garantizar una determinación confiable del estado).

93 *Véase el Estudio de identificación de registratarios de WHOIS:* https://gnso.icann.org/sites/default/files/filefield_39861/registrant-identification-summary-23may13-en.pdf (En base a en nuestro análisis de los registros de WHOIS obtenidos de una muestra aleatoria de 1600 dominios de los cinco principales gTLD,

- El 39 % (± 2,4 %) parece estar registrado por personas jurídicas.
- El 33 % (± 2,3 %) parece estar registrado por personas físicas.

dominio a disposición del público, que debería incluir los datos de las entidades jurídicas, es un método para que el público evalúe la legitimidad de un sitio web y para que las autoridades encargadas del cumplimiento de la ley puedan saber qué entidades están detrás de dicho sitio web.

Es significativo que el Equipo responsable del EPDP haya recibido un asesoramiento jurídico que sugiere varias medidas para reducir el riesgo de responsabilidad.[94] La implicación de este asesoramiento es que podría haber una variedad de medidas para asegurar que los registratarios se designen a sí mismos con precisión como entidades jurídicas. Cabe señalar que algunos ccTLD (incluidos los ccTLD con sede en la UE) ya ponen a disposición del público ciertos datos de registratarios de entidades jurídicas, lo que demuestra que esa distinción es legalmente permitida y factible.[95]

La distinción entre el tratamiento de los datos de personas jurídicas y físicas también está estrechamente relacionada con la cuestión del procesamiento automatizado. Como se ha señalado anteriormente, las personas jurídicas no están protegidas por el GDPR. Por lo tanto, la distinción entre personas jurídicas y físicas durante el proceso de registro se podría incluir la asignación de las personas jurídicas en la categoría de personas cuyos datos deberían procesarse automáticamente.[96]

El GAC cree que resolver la cuestión de la distinción entre personas jurídicas y físicas es fundamental para que todo el modelo del SSAD cumpla su propósito y, al mismo tiempo, se ajuste a las leyes de protección de datos aplicables. Por lo tanto, el GAC solicita al Consejo de la GNSO que realice todos los esfuerzos posibles para abordar esta cuestión. A ese respecto, el GAC reitera su solicitud para que el Equipo responsable del EPDP se centre en el asesoramiento jurídico proporcionado para elaborar políticas razonables que permitan que la información de las entidades jurídicas siga siendo pública.

Correo electrónico anonimizado

- El 20 % (± 2,0 %) se registró usando un servicio de privacidad o proxy.
- No pudimos clasificar el restante 8 % (± 1,4 %) utilizando los datos disponibles de WHOIS.

94 *Véase el* Asesoramiento sobre la responsabilidad en relación con la autoidentificación de un registratario como persona física o no física de conformidad con el Reglamento General de Protección de Datos (Reglamento (UE) 2016/679) ("GDPR") de Bird & Bird (los métodos aconsejados incluían la elaboración de un texto de notificación claro para que los registratarios eviten errores; garantizar que los registratarios comprendan las consecuencias de registrarse como entidad jurídica; y verificar de que la información de contacto no contenga datos personales).

95 Véase, por ejemplo, Bélgica (.BE), Unión Europea (.EU), Estonia (.EE), Finlandia (.FI), Francia (.FR), Noruega (.NO), etc.

96 Como resguardo, las personas con mayores protecciones jurídicas podrían ser asignadas a grupos de consulta no automatizada. Esto podría incluir a las personas jurídicas protegidas por la legislación nacional (como las leyes sobre el secreto bancario), las personas físicas con protecciones jurídicas específicas como las órdenes de protección de los tribunales, el estatus de vulnerable de un titular de los datos (por ejemplo, los niños, los solicitantes de asilo, otras clases protegidas), y poblaciones nacionales enteras en jurisdicciones que otorgan un derecho afirmativo a la privacidad personal de forma predeterminada.

El uso de correos electrónicos anonimizados puede ser una solución para proteger la identidad del registratario y, al mismo tiempo, servir a algunos de los propósitos legítimos de los solicitantes de acceso a los datos de registración de nombres de dominio. El Informe Final incluye entre los elementos de Prioridad 2 a la "factibilidad de contactos únicos para tener una dirección de correo electrónico anonimizada uniforme".[97] El Equipo responsable del EPDP recibió asesoramiento jurídico que indicaba que la anonimización así como la seudonimización es "una útil técnica de mejora de la privacidad/medida de privacidad por diseño".[98] Como se reconoce en el mismo asesoramiento jurídico, el GAC desea señalar que la información anonimizada queda fuera del ámbito del GDPR.[99] Si bien el GAC reconoce la posibilidad de que se pueda crear un vínculo entre la información anónima y los datos personales, está de acuerdo con el asesoramiento jurídico en cuanto a que la anonimización es una técnica útil para mejorar la privacidad y, por lo tanto, debería examinarse más a fondo.

Habida cuenta de lo mencionado anteriormente, el GAC considera que se necesita un mayor análisis de factibilidad para comprender mejor los beneficios y riesgos de esta opción, en lugar de descartarla sin proceder a un examen complementario.

Responsabilidad del tratamiento

La posible responsabilidad conjunta del tratamiento entre las partes contratadas y la organización de la ICANN se menciona en el Informe Final. Sin embargo, el GAC esperaría mayor claridad sobre el estatus y la función de cada uno de los responsables y encargados del tratamiento de datos en el modelo del SSAD. En particular, el hecho de contar con acuerdos concretos de procesamiento de datos demostraría más claramente cómo se distribuiría la responsabilidad entre las partes contratadas y la organización de la ICANN para las diferentes operaciones de procesamiento de datos. El GAC instaría al Consejo de la GNSO a que solicite al EPDP que siga tratando este asunto.

Conclusión

El GAC aplaude los esfuerzos de buena fe de las partes interesadas, el personal y los Presidentes del EPDP que participan en la Fase 2 del EPDP por su constante dedicación y compromiso en estos importantes asuntos de política pública. Hay muchos aspectos encomiables en el Informe Final. Sin embargo, el GAC opina que ciertas recomendaciones clave y temas no abordados requieren un trabajo adicional y que, en consecuencia, el Consejo de la GNSO debería solicitar al EPDP que finalice el trabajo al

97 Informe Final de la Fase 2 del EPDP, pág. 3.

98 Bird & Bird Asesoramiento jurídico, "'Segundo lote' de preguntas sobre un Sistema Estandarizado de Acceso/Divulgación ("SSAD"), Servicios de privacidad/representación (proxy) y correos electrónicos seudonimizados" (4 de febrero de 2020).

99 *Véase* el Considerando 26 del GDPR.

respecto de acuerdo con los puntos planteados en esta Declaración Minoritaria. El GAC espera seguir colaborando con nuestros colegas en estas importantes cuestiones.

Declaración Minoritaria del Grupo de Partes Interesadas No Comerciales (NCSG)

El NCSG no ha aceptado las Recomendaciones 22, 20 y 7, por las razones que se exponen a continuación.

Recomendación n.° 22: Propósito 2

El propósito 2 de la Recomendación 22 actualmente expresa: *"Contribuir al mantenimiento de la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio de acuerdo con la misión de la ICANN".*

El NCSG se opone firmemente a este propósito. Es demasiado vago y abierto, y permite a la ICANN procesar los datos de registración de gTLD de la forma que considere conveniente. Todo lo que se requeriría por parte de la organización de la ICANN, es adivinar un motivo consistente con su interpretación de sus Estatutos, como admitió Becky Burr en un correo electrónico enviado al Equipo responsable del EPDP en nombre de la Junta Directiva de la ICANN.

En ese correo electrónico, Burr expresa lo siguiente: *"el SSR, según su definición en los Estatutos, *es* la misión de la ICANN. El Artículo 1, Sección 1.1 de los Estatutos de la ICANN, establece claramente que la misión de la ICANN es asegurar el funcionamiento estable y seguro (SSR) de los sistemas de identificadores únicos de Internet . Los propios Estatutos continúan y proporcionan detalles significativos sobre el alcance de esa misión en el contexto de los nombres, el sistema de servidores raíz, los números y los protocolos".*

En la Fase 1, desarrollamos hojas de trabajo para cada propósito de la ICANN que detallan las bases legales y las actividades de procesamiento para todos ellos. En la Fase 2 esto no se hizo. En consecuencia, este Propósito 2 reformulado no indica por qué habría que divulgar los datos, ni a quién, ni tampoco indica por qué habría que conservarlos ni por cuánto tiempo. El Propósito 2, tal como está redactado actualmente en el Informe Final de la Fase 2, también contradice el principio de limitación del propósito del GDPR - Artículo 5(1)(b), que requiere que los datos "*serán recolectados con fines específicos, explícitos y legítimos, y no se los procesará en modo alguno que sea incompatible con los fines indicados*". Garantizar el funcionamiento estable y seguro (SSR) de los sistemas de identificadores únicos de Internet no es algo ni específico ni explícito, y la interpretación de la Junta Directiva de la ICANN sobre la SSR dentro de las competencias de la ICANN lo hace aún menos.

El NCSG ha solicitado en reiteradas ocasiones que el Equipo responsable del EPDP llegue a un entendimiento común de lo que implica la misión de la ICANN en relación con la SSR, y cómo se aplica eso al procesamiento de los datos de registración de gTLD por parte de la ICANN. Estas solicitudes fueron denegadas sistemáticamente, a pesar

de que se les exigía cumplir con la obligación legal de la ICANN como Responsable del tratamiento de datos para este propósito.

El Equipo responsable del EPDP no ha logrado comprender cómo la SSR dentro de la misión de la ICANN es aplicable a este propósito, ni la ICANN ha indicado que posea ninguna información al respecto. Sin embargo, como ocurre con otros fundamentos jurídicos en el GDPR, el Artículo 6.1.(f) crea obligaciones adicionales por parte del responsable del tratamiento de datos con respecto al titular de los datos, incluida la protección de sus derechos e intereses.

En sus directrices sobre la utilización del Artículo 6.1.(f) como fundamento jurídico, la Oficina del Comisionado de Información del Reino Unido indica que la utilización de este fundamento jurídico es más apropiada cuando (entre otras circunstancias) la utilización de los datos de las personas se realiza en formas que estas podrían esperar razonablemente y que tienen un impacto mínimo en la privacidad. Es virtualmente imposible para los Registratarios de gTLD tener alguna expectativa sobre por qué o cómo la ICANN divulgaría o retendría sus datos en base al Propósito 2. Estas circunstancias desconocidas no han sido identificadas por la ICANN ni por el Equipo responsable del EPDP, y el único medio por el cual un Registratario puede tener alguna forma de comprensión de esto es si el registro de un nombre de dominio de gTLD requiere que el Registratario también adquiera experiencia en la interpretación y aplicación de los Estatutos de la ICANN. Dicha expectativa no es realista; está más allá de la capacidad del propio personal de la ICANN, de los miembros de la Junta Directiva y de los miembros del Equipo responsable del EPDP.

El NCSG cree que este propósito no es realmente necesario para que la ICANN cumpla su misión; fue puesto allí para que la organización de la ICANN pueda satisfacer los deseos de terceros, a pesar de que la referencia a los intereses legítimos de los terceros fue eliminada de la recomendación revisada. La Junta Directiva de la ICANN parece creer que esta base jurídica le proporciona una cobertura ante la responsabilidad, lo que probablemente no sea así, mientras que ignora por completo los intereses de los titulares de los datos, a quienes el GDPR está destinado a empoderar.

Para que este propósito sea justo para los Registratarios, es necesario desglosarlo en múltiples propósitos claramente establecidos que identifiquen actividades de procesamiento claramente establecidas, que se deberían comunicar y explicar a los Registratarios de una manera que puedan comprender fácilmente.

Recomendación n.° 20: Campo que especifica la ciudad

El NCSG no cree que se haya presentado un caso convincente que la recomendación realizada sobre el "campo que especifica la ciudad" en la Fase 1 del EPDP se cambie de DEBE censurar a PUEDE censurar. La recomendación anterior que requería la censura

de este campo se basaba en el asesoramiento jurídico de Bird and Bird en el que se expresaba lo siguiente:

> *"3.16 Teniendo en cuenta todo lo anterior, las partes relevantes pueden cumplir con la prueba de los intereses legítimos para la publicación del campo "ciudad". Sin embargo, no nos queda claro por la información disponible hasta ahora. En particular:*
>
> *a) se requerirá más información para demostrar que los beneficios para los titulares de derechos son suficientemente significativos como para justificar la publicación universal del campo que especifica la ciudad, en lugar de ser de utilidad en casos muy limitados; y*
>
> *b) se necesita más información sobre las posibles repercusiones en los derechos e intereses de los titulares de los datos.*
>
> *3.17 Las partes relevantes tendrían entonces que realizar una evaluación detallada de los hechos y circunstancias para determinar si los intereses que se persiguen superan los de los titulares de los datos".*

Esto indica claramente que sería necesario realizar una prueba de equilibrio para sopesar los intereses legítimos del tercero que solicite la divulgación de los datos de registración de gTLD con los derechos del Registratario implicado. El NCSG tiene la firme convicción de que esto debe llevarse a cabo como parte del procesamiento de una solicitud de divulgación a través del SSAD, y no debería confundirse con los propósitos de la ICANN en el procesamiento de los datos de registración de gTLD, que es lo que cubrían las recomendaciones de la Fase 1 del EPDP.

Esta conclusión de Bird and Bird fue reafirmada en su correo electrónico a Kurt Pritz, en el que indicaron lo siguiente: *"El análisis jurídico es claro: se trata de datos personales; en principio, la publicación podría justificarse sobre la base de los intereses legítimos de los titulares de los derechos, a menos que los intereses de las personas prevalezcan sobre esto.*

La forma en que esto se aplica a los hechos, establecer si existe un interés suficiente para los titulares de derechos y equilibrar esto con los intereses de los titulares de nombres registrados, no está clara".

Todo esto es muy sugerente para que el campo que especifica la ciudad en los datos de registración de gTLD sea tratado como cualquier otra información personal, y DEBE ser censurado.

Recomendación n.° 7: Propósitos del Solicitante

El NCSG mantiene su desacuerdo con la inclusión de una nota al pie en la que se especifique la Directiva NIS de la UE como ejemplo legislativo que establece obligaciones para las entidades reguladas aplicables. Este ejemplo se agregó a la recomendación durante una etapa del trabajo del Equipo responsable del EPDP en la que se estaban perfeccionando el informe final y las recomendaciones para lograr el mayor apoyo posible y, según la opinión del NCSG, no se le dio tiempo ni atención suficientes para incluirlo en el Informe Final, ni se tuvieron suficientemente en cuenta las consecuencias para una política que permitiera la divulgación a terceros.

Además, el NCSG no cree que la exclusión de este ejemplo tenga impacto significativo alguno en la capacidad de las entidades aplicables reguladas por la Directiva NIS, u otra legislación similar, de solicitar la divulgación de datos de registración de gTLD censurados por el SSAD.

Declaración Minoritaria del Grupo de Partes Interesadas de Registradores (RrSG)

El Informe Final de la Fase 2 del EPDP representa la culminación de años de trabajo en colaboración con la Comunidad de la ICANN. El RrSG sigue creyendo que redunda en todos nuestros intereses crear políticas y un sistema que equilibre los requisitos de protección de datos del registrador con las necesidades de quienes dependen del acceso a datos de registración sin carácter público para fines legítimos y lícitos.

Los registradores han expresado preocupaciones significativas a lo largo de este proceso de la Fase 2 del EPDP sobre la legalidad, la factibilidad técnica y los costos asociados con el desarrollo, despliegue y funcionamiento del SSAD. Si bien los registradores apoyan más algunas recomendaciones que otras, todas ellas son muy interdependientes y deben considerarse de manera holística, y reconocemos que el resultado final es mayor que la suma de sus partes.

Por lo tanto, en el espíritu de compromiso permanente con los intereses de otras partes interesadas, apoyamos el resultado de la Fase 2 del EPDP y las recomendaciones de este Informe Final, y cumpliremos con las Políticas de consenso resultantes.

Consideramos que las recomendaciones finales ofrecen suficiente orientación para basar un sistema estandarizado y previsible, que se ajuste a las recomendaciones de la Fase 1 del EPDP y que, al mismo tiempo, permita la flexibilidad necesaria para que cada registrador lleve a cabo sus operaciones del SSAD de la manera que considere más acorde con sus obligaciones jurídicas y de privacidad, que a menudo son multijurisdiccionales.

Instamos al Consejo de la GNSO y a la Junta Directiva de la ICANN a que adopten todas las recomendaciones del informe, de modo que podamos pasar al trabajo de implementación y a un rápido lanzamiento del SSAD.

Declaración del Grupo de Partes Interesadas de Registros sobre el Informe Final de la Fase II del EPDP

El Grupo de Partes Interesadas de Registros ("RySG") aprecia la labor realizada en la Fase II, reconoce la utilidad de un SSAD para terceros y apoya las recomendaciones que figuran en el Informe Final. Las recomendaciones reflejan el mejor esfuerzo del Equipo responsable del EPDP para desarrollar una solución para el acceso a los datos personales que equilibre los derechos de privacidad de los titulares de los datos con los intereses legítimos de terceros. Aunque esta declaración aborda las preocupaciones sobre ciertos aspectos del Informe Final, aceptamos los compromisos que constituyen la base de las recomendaciones del SSAD. Seguimos siendo optimistas sobre el futuro desarrollo del SSAD.

Durante más de un año de diligencia, los Registros se han mantenido firmes en los principios que indican que este sistema debe (i) reflejar la realidad de la ley de protección de datos tal como es hoy en día, (ii) priorizar y proteger apropiadamente los datos personales de un registratario antes que los intereses de terceros, y (iii) retener nuestra capacidad como responsables del tratamiento de datos para cumplir con nuestras obligaciones legales de proteger los datos personales. Algunos han señalado su insatisfacción con un sistema basado en estos principios. Sin embargo, nos sentimos cómodos defendiendo estos principios como la mejor manera de proteger los datos personales de los registratarios y de cumplir nuestras obligaciones en virtud de la ley.

El RySG participó de buena fe

El EPDP fue constituido para "determinar si la Especificación Temporaria para los Datos de Registración de los gTLD debe convertirse en una Política de Consenso de la ICANN, tal como está o con modificaciones, y que a la vez cumpla con el GDPR y otras leyes relevantes de privacidad y protección de datos".[100] La carta orgánica reconoce que el trabajo secundario de evaluar un sistema en beneficio de terceros para acceder a los datos personales de un registratario comenzaría únicamente una vez que las cuestiones primarias "fueran resueltas y finalizadas en preparación del informe inicial de la Especificación Temporaria".[101] El 19 de febrero de 2019, se publicó un Informe Final para la Fase I, que incluía una recomendación detallada y exigible para estandarizar el proceso para que terceros obtengan datos personales de un registratario.[102]

El RySG participó en la Fase II de buena fe para desarrollar un sistema en beneficio de terceros que tengan un interés legítimo en acceder a los datos personales de un registratario. Los registros no necesitamos ese sistema para cumplir con nuestras obligaciones para proteger los datos personales de un registratario y responder a las

[100] Carta orgánica adoptada final del EPDP – 19 de julio de 2018 disponible en este enlace.
[101] Carta orgánica adoptada final del EPDP – 19 de julio de 2018 disponible en este enlace.
[102] *Véase* el Informe Final de la Fase I del EPDP, Recomendación 18, disponible en este enlace.

solicitudes de terceros para obtener esos datos personales. Nuestros miembros responden de forma periódica y responsable a las solicitudes de datos hoy en día sin un sistema SSAD, de acuerdo con los requisitos del informe de la Fase I y nuestras obligaciones conforme a la ley. Continuaremos haciéndolo incluso una vez que el SSAD esté operativo. Lamentablemente, en muchos aspectos, el SSAD dificultará nuestra labor al introducir un procesamiento adicional y riesgos para los datos personales de un registratario.

Hemos escuchado con una mente abierta a las comunidades que insisten en un mayor acceso a los datos personales y participamos en este proceso para encontrar soluciones. Si bien apoyamos el Informe Final y los diversos compromisos que el grupo ha realizado, por los motivos que se enumeran a continuación, tenemos preocupaciones significativas que requerirán una diligencia continua para avanzar a medida que la comunidad aborde la implementación.

El RySG priorizó la protección de datos

Nuestro punto de partida en estos debates siempre ha sido los principios de protección de datos. La protección de datos en general, y el GDPR en particular, "protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales".[103] Como reiteró recientemente la Comisión de la Unión Europea: "el objetivo final del GDPR es cambiar la cultura y el comportamiento de todos los actores involucrados en beneficio de las personas"[104] En pocas palabras, el objetivo de la protección de datos es proteger los datos personales de las personas. Aunque esto no debería ser controvertido, nuestra experiencia de los últimos dos años sugiere lo contrario.[105]

En la práctica, priorizar la protección de datos significa poner al titular de los datos en primer lugar al considerar el impacto de cómo y quién procesa sus datos. Significa adoptar la minimización de datos y la privacidad predeterminada como referencia de base a fin de evitar el procesamiento innecesario de los datos personales de una persona. Significa asegurarnos de no aplicar requisitos de la política que restrinjan nuestra capacidad como responsables del tratamiento de datos para cumplir con nuestra obligación legal de cuidar adecuadamente los datos personales que las personas nos confían.

[103] GDPR, Artículo 1 (2).
[104] Comunicación de la Comisión ante el Parlamento Europeo y el Consejo, Comisión Europea, con fecha del 24 de junio de 2020, p. 5 (énfasis agregado), disponible en este enlace.
[105] Si bien el Artículo 17 de la Carta de Derechos Fundamentales reconoce que "se protegerá la propiedad intelectual", el Parlamento Europeo ha aclarado que el ejercicio de ese derecho "no debería obstaculizar . . . la protección de los datos personales, incluso en Internet". Véase la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, del 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual, disponible en este enlace.

Sobre la base de estos principios, hemos continuado mostrando flexibilidad de forma reiterada y hemos trabajado para incorporar los intereses de terceros, incluso si eso nos exigía realizar concesiones que podían aumentar el riesgo para las partes contratadas. Si bien a algunas partes les hubiera gustado llegar más lejos, debemos trazar los límites cuando se nos pide que cedamos en ámbitos en los que hemos recibido información reiteradas veces (por parte del asesor jurídico independiente de la Fase II, las autoridades de protección de datos y nuestros propios miembros de la CPH con experiencia en protección de datos de la UE) que algo no está legalmente permitido o presenta riesgos significativos para el titular de los datos.

El objetivo de la Fase II era estandarizar el proceso para que los terceros soliciten datos personales de un registratario. Sin embargo, la insistencia continua para encontrar un camino que permita el acceso prácticamente automático a los datos personales no es, después de muchos meses de análisis, beneficiosa para los titulares de los datos. Nos preocupa que los intentos de lograr el acceso automático a cualquier precio acaben por socavar la legalidad y la viabilidad futura del SSAD.

El modelo híbrido refleja la realidad jurídica y práctica

El modelo híbrido (es decir, recepción centralizada con toma de decisiones descentralizada) es una solución práctica que creemos que resolverá muchas de las cuestiones que los solicitantes citan con el método del *statu quo* para solicitar acceso a los datos personales de registratarios. Lo más importante es que el modelo híbrido refleja la realidad de lo que es posible en el derecho actual.

Bird & Bird confirmó que la responsabilidad recae en los responsables del tratamiento de datos, e incluso, suponiendo un sistema totalmente centralizado y automatizado que eliminara la discreción de las partes contratadas, "el resultado más probable (y, por cierto, la posición de partida de la mayoría de las autoridades supervisoras) es que las partes contratadas sean responsables del tratamiento de datos".[106] Además, la Autoridad de Protección de Datos de Bélgica subrayó que la función de la responsabilidad del tratamiento es una función fáctica que las partes "no son libres de simplemente 'designar'" y, del mismo modo, "a la cual no pueden renunciar . . . en virtud de un acuerdo conjunto".[107]

Aceptamos el asesoramiento de Bird & Bird y la DPA sobre este asunto, y ya en enero advertimos que "más deliberaciones sobre un modelo totalmente centralizado solo nos distraen y nos retrasan en el cumplimiento de nuestro trabajo de manera oportuna y rentable".[108] Lamentablemente, incluso en las últimas etapas del EPDP, continuamos escuchando sugerencias sobre cómo se podría centralizar cierta toma de decisiones

[106] Phil Bradley-Schmieg y Ruth Boardman (Bird & Bird LLP), "Preguntas 1 y 2: Responsabilidad, medidas de protección, responsable y encargado del tratamiento", 9 de septiembre de 2019, p. 6, 2.18.
[107] Autoridad de Protección de Datos (Bélgica), Carta a Göran Marby, 4 de diciembre de 2019, pág. 3, disponible en este enlace.
[108] Carta sobre próximos pasos de la CPH, con fecha del 7 de enero de 2020.

sobre los datos personales de los registratario y cómo se podría asignar la responsabilidad del tratamiento mediante nuestras recomendaciones de políticas.[109]

Nada ha cambiado desde que el EPDP acordó rechazar la centralización por no cumplir el requisito previo de disminuir la responsabilidad de las partes contratadas.[110] Nos preocupa que algunas partes no entiendan o ignoren deliberadamente el asesoramiento jurídico que no se ajusta a los resultados de sus políticas preferidas. Cualquiera de los dos escenarios no es ideal para encontrar un consenso sobre recomendaciones de políticas implementables.

Ni siquiera el término "centralización" refleja con precisión lo que realmente han propuesto los defensores de dicho modelo. Solo la toma de decisiones, y no los datos en sí, ha formado parte alguna vez del debate sobre un sistema "centralizado". Sin poseer los datos subyacentes, no se trata de un sistema "centralizado" que limitaría el procesamiento innecesario y aumentaría la seguridad de los titulares de los datos. En cambio, dicho sistema agrega pasos de procesamiento adicionales innecesarios y es incompatible con los principios básicos de minimización de datos y de privacidad por defecto.

Seguimos preocupados por la continua insistencia en que la "centralización" de la divulgación de datos personales está legalmente permitida o es realista en el ecosistema de la ICANN, a pesar de que no se han producido cambios en los hechos que nos llevaron a rechazar la centralización en primer lugar. Si bien apoyamos los esfuerzos de la ICANN para encontrar respuestas sobre la asignación de responsabilidad en un sistema centralizado, todavía no hay ninguna pauta que indique que el cambio de responsabilidad como requisito previo sea legalmente posible.

Comité Permanente de la GNSO

El RySG apoya el concepto de que el SSAD debería ser flexible y capaz de recalibrarse en función de las nuevas circunstancias legales o prácticas. Reconocemos que el SSAD debe ser ágil y capaz de adaptarse a un panorama en constante cambio de pautas

[109] Véase, por ejemplo, los comentarios de categoría del 2 de julio de 2020 sobre la Recomendación 9, IPC/BC que proponen "el concepto de no automatizar la toma de decisiones centralizada en el Administrador de la puerta de enlace central (CGM)" a pesar del asesoramiento jurídico y el acuerdo sobre un modelo híbrido: "De acuerdo con el asesoramiento jurídico obtenido, el Equipo responsable del EPDP recomienda que los siguientes tipos de solicitudes de divulgación estén legalmente permitidos en el marco del GDPR para la evaluación centralizada de la divulgación (tanto la toma como el procesamiento de la decisión de divulgación) en el Administrador de la puerta de enlace central cuando se sometan a revisión y procesamiento manual desde el principio:
· Decisiones de divulgación automatizadas para solicitudes claras de "dominios que coinciden con marcas comerciales".
· Decisiones de divulgación automatizada para casos claros de phishing
La organización de la ICANN es el responsable del tratamiento cuando se procesa esta decisión de divulgación".

[110] "Y eso significa que, en esencia, para tener cualquier modelo de acceso unificado, o bien se llega a un acuerdo con 2500 partes contratadas sobre lo que consideren que es el riesgo legal que tienen, o bien se presenta una mociones [sic] donde se disminuyan las responsabilidades legales de las partes contratadas". Göran Marby, Transcripción de la reunión presencial del EPDP, 25 de septiembre de 2018, pág. 2, disponible en este enlace.

administrativas, decisiones de los tribunales y nuevos reglamentos en diversas jurisdicciones. Rechazamos, sin embargo, la noción de que el trabajo del Comité Permanente de la GNSO debe tener un resultado predeterminado. Es decir, no podemos aceptar la suposición de que el SSAD evolucionará inevitablemente hacia una mayor centralización y automatización de la divulgación de datos personales en el futuro. El SSAD debe evolucionar en base a hechos y datos en lugar de suposiciones y conjeturas.

Como ya se ha expresado, el modelo híbrido refleja lo que es legalmente posible hoy en día. No estuvimos de acuerdo con el modelo híbrido siempre y cuando algún día evolucione hacia un modelo centralizado porque no tenemos fundamentos para saber en qué dirección irán las leyes. Estuvimos de acuerdo con el modelo híbrido como una solución para mejorar el *statu quo* y, al mismo tiempo, proteger de forma adecuada los datos personales de las personas.

Los miembros del grupo de trabajo para el EPDP deberían establecer expectativas adecuadas dentro de sus grupos de partes interesadas sobre cómo puede cambiar el SSAD con el transcurso del tiempo. Si bien este sistema puede avanzar en la dirección que desean algunos de los miembros del EPDP, es igualmente probable (si no más) que el sistema tenga que ser más restrictivo, menos automatizado o más descentralizado.[111] Proponer la evolución como un camino de un solo sentido en lugar de responder a los hechos y datos predispone a este sistema al fracaso según la opinión de algunos miembros de la comunidad.

Del mismo modo, si bien en general hemos apoyado el alcance del trabajo del Comité Permanente de la GNSO, nos preocupa mucho cualquier iniciativa por estructurar este mecanismo de manera que ceda el control de nuestras obligaciones legales como responsables del tratamiento de datos. Nos hemos resistido a los esfuerzos por afirmar categóricamente que ciertos cambios, como la adición de nuevos casos de uso de automatización, corresponden a la implementación o a las políticas, porque no podemos predecir la forma que podrían adoptar las futuras directrices sobre estas cuestiones. A menos que la Comisión Europea proporcione directrices perfectas, definitivas e incuestionables sobre un tema, las propuestas de automatización basadas en nuevas directrices probablemente tendrán un riesgo residual, obligaciones adicionales o requerirán revisiones contractuales para las partes contratadas o el Administrador de la puerta de enlace central (CGM).

[111] Muchas de las decisiones y pautas recientes más importantes en esta área parecen sugerir la imposición de nuevas restricciones y la aplicación de medidas coercitivas en lugar de una relajación de los requisitos. *Véase, por ejemplo*, el Caso C-311/18, Comisario para la Protección de Datos contra Facebook Ireland Limited y Maximillian Schrems ("Schrems II"), en el que se invalidó el sistema de protección de privacidad de la Unión Europea y los Estados Unidos; *véase también* la Comunicación de la Comisión al Parlamento Europeo y al Consejo, Comisión Europea, con fecha del 24 de junio de 2020, en la que se solicita una mayor aplicación del GDPR en lugar de una relajación de las restricciones, disponible en este enlace.

Podemos imaginar fácilmente casos en los que incluso una simple orientación permisible sobre automatización adicional podría requerir cambios de políticas. Por ejemplo, si se publican nuevas directrices en el sentido de que siempre se permita la plena automatización, siempre que cualquier entidad que tenga alguna función en el tratamiento de los datos cuente con un Delegado de protección de datos designado, como se define en el GDPR. En la actualidad, nuestras recomendaciones no requieren que ninguna de las partes (CGM, Autoridad de acreditación, Registros, Registradores, Solicitantes) tenga un Delegado de Protección de Datos. En este escenario, si se forzara a las partes contratadas a utilizar más casos de uso de automatización a través de la implementación, ello podría aumentar considerablemente los riesgos jurídicos de las partes contratadas si alguna de las partes que intervienen en el procesamiento no designara a un Delegado de protección de datos.

Este ejemplo ilustra lo importante que es que no predeterminemos que los cambios que probablemente impliquen un riesgo jurídico son categóricamente cuestiones de implementación y no de política. Como responsables del tratamiento de datos, necesitamos la capacidad de responder a las obligaciones que tenemos con las personas cuyos datos personales procesamos.

La automatización completa solo es posible en circunstancias limitadas

El RySG respalda el concepto de automatización cuando sea un proceso "técnica y comercialmente factible y legalmente permitido".[112] Consideramos que esos criterios constituyen las medidas de protección necesarias para garantizar que los titular de los datos no sean objeto de un procesamiento automatizado irrazonable de sus datos.

Como punto de partida, no debería ser objeto de controversia el hecho de que la automatización a gran escala de las decisiones que afectan a los titulares de los datos, pero de las que no reciben ningún beneficio, no suele redundar en beneficio del titular de los datos. Como afirma el GDPR: "el titular de los datos tendrá derecho a no ser objeto de una decisión basada únicamente en un procesamiento automatizado, incluida la definición de perfiles, que produzca efectos jurídicos que le conciernan o que lo afecten de forma similar y significativa".[113] Bird & Bird nos confirmó que, cuando se le presentaron todos los posibles casos de uso de automatización propuestos por el equipo, solo cuatro no produjeron efectos legales o igualmente significativos para el titular de los datos.[114]

[112] Informe Final del EPDP, Fase II, 9.3.

[113] GDPR, Artículo 22.

[114] Informe Final del EPDP, Fase II, 9.4: (i) Las solicitudes de los organismos encargados del cumplimiento de la ley en las jurisdicciones locales o de otra índole aplicables con 1) un fundamento jurídico confirmado por la sección 6(1)e del GDPR, o 2) el procesamiento que se llevará a cabo conforme una exención en virtud del Artículo 2 del GDPR; (ii) La investigación de una infracción de la legislación de protección de datos presuntamente cometida por la ICANN/Partes contratadas que afecte al registratario por parte de una autoridad de protección de datos; (iii) Solicitud únicamente del campo que especifica la ciudad, para evaluar si se interpondrá un reclamo o con fines

Nuestra conclusión de ese asesoramiento jurídico es que solo un conjunto muy limitado de decisiones no crea un efecto jurídico o de importancia similar para titulares de los datos. Del mismo modo, el memorando solo evalúa estos casos de uso en el marco del GDPR. Por consiguiente, deberíamos tener cuidado con sacar conclusiones amplias sobre la permisividad jurídica que obligará a las partes contratadas a implementar requisitos que aumentarán su riesgo jurídico.

También nos preocupa que estos cuatro casos de uso sean ahora necesarios para la automatización completa el primer día del SSAD,[115] a pesar de que el Equipo responsable del EPDP ni siquiera ha empezado a participar en ningún debate técnico sobre cómo un algoritmo puede, de manera confiable, (i) identificar las solicitudes que son apropiadas para la automatización, o (ii) tomar decisiones de manera confiable, precisa y transparente. Acordamos como plenario que la automatización debía cumplir tres criterios: (i) técnicamente factible, (ii) comercialmente factible y (iii) legalmente permitida.[116] Al exigir la automatización de los casos de uso en la sección 9.4 en base a su permisividad legal, hemos colapsado estas tres importantes medidas de protección en una evaluación singular de la legalidad de estos casos de uso.

De hecho, lo más cerca que hemos llegado a cualquier consideración sustantiva de cómo un algoritmo podría evaluar y tomar estas decisiones es la sugerencia de que el CGM pueda proporcionar recomendaciones sobre la divulgación a las partes contratadas, y que el algoritmo aprendería de la retroalimentación sobre si la decisión de una parte contratada de divulgar la información coincide con la recomendación automatizada.[117] Esto no solo representa un malentendido de la forma en que funciona generalmente el aprendizaje automático, sino que tenemos serias dudas sobre la confiabilidad de las recomendaciones realizadas por un sistema que no posee la información subyacente que es la base de nuestras propias decisiones. Incluso si nuestras decisiones "coinciden" con suficiente regularidad, esa correlación no significa que el algoritmo esté de hecho tomando decisiones precisas y confiables.

Se necesita un enfoque mucho más sofisticado para el aprendizaje automático y capacitación en algoritmos para evaluar si estos casos de uso son técnicamente factibles. Por ello, el requisito de la factibilidad técnica como factor independiente es una parte importante de la consideración de los casos de uso de automatización. Si las partes que ahora deben dedicarse realmente al trabajo de determinar la factibilidad técnica y crear un algoritmo no pueden hacerlo con éxito, no deberíamos estar ya

estadísticos; iv) Ningún dato personal en el acta de la registración que haya sido divulgado previamente por la Parte contratada.

[115] Informe Final del EPDP, 9.4: "Según el asesoramiento jurídico obtenido . . . el Equipo responsable del EPDP recomienda que los siguientes tipos de solicitudes de divulgación, para los cuales se ha indicado la autorización legal en virtud del GDPR para la automatización completa (tanto la toma como el procesamiento de la decisión de divulgación) DEBEN automatizarse desde el momento del lanzamiento del SSAD . . ."

[116] Informe Final del EPDP, Fase II, 9.3.

[117] Informe Final del EPDP, Fase II, 5.1.1, 5.5.

encerrados en la automatización obligatoria porque no se haya cumplido el requisito de factibilidad técnica.

La sostenibilidad financiera requiere atención

Desde los inicios de la Fase II, el RySG abogó por una evaluación financiera de un SSAD propuesto con el fin de proporcionar datos importantes para orientar la toma de decisiones del Equipo responsable del EPDP. Agradecemos el trabajo que el equipo de la ICANN realizó al proporcionarnos una evaluación de los costos. Habida cuenta de los significativos costos estimados de la ICANN para desarrollar y mantener el SSAD propuesto, nos preocupa que esta evaluación quede relegada a una sola nota al pie en el Informe Final, especialmente a medida que seguimos observando la resistencia de otras unidades constitutivas sobre la premisa de que los usuarios del SSAD deberían sufragar los costos de funcionamiento del sistema.

Para reiterar una cuestión que planteamos reiteradamente durante las deliberaciones, bajo ninguna circunstancia un titular de los datos debería subsidiar la capacidad de un tercero para acceder a sus datos personales. El SSAD tiene por objeto proporcionar un acceso previsible y estandarizado a los datos y debería ser financiado por quienes se beneficien directamente de dicho servicio.

Además, apoyamos a la ICANN en la realización de un análisis de costo-beneficio para determinar la factibilidad financiera de dicho sistema. Teniendo en cuenta la amplia labor realizada en la Fase I para establecer un proceso estandarizado para que los terceros soliciten datos directamente a las partes contratadas (Recomendación 18), ninguna parte (el titular de los datos ni el tercero solicitante) carece de un proceso previsible para solicitar datos personales. Además, todo usuario que no desee pagar por el servicio del SSAD sigue teniendo la opción de presentar solicitudes de divulgación según lo establecido en la Fase 1, lo cual no tiene costo alguno para el solicitante.

En nuestra opinión, la falta de análisis de costo-beneficio también apunta a un problema mayor: el EPDP nunca estableció, más allá de anécdotas y conjeturas, cuál era el problema real que este sistema pretende resolver. No hemos visto ningún dato confiable que demuestre que las respuestas de las partes contratadas a las solicitudes de divulgación sean un problema. En realidad, los datos sugieren que se responde a la mayoría de las preguntas formuladas de manera apropiada y que la falta de respuesta suele estar relacionada con: (i) solicitudes inapropiadas de datos protegidos por servicios de privacidad/representación (proxy), o (ii) la falta de respuesta de los solicitantes cuando se requiere información adicional.[118] La SSAD no solucionará ninguno de estos errores de los solicitantes.

[118] *Véase* Privacidad y acceso legítimo a datos personales en Tucows, 13 de marzo de 2020, disponible en este enlace.

Se abordaron las cuestiones de prioridad 2

Aunque el RySG apoya el trabajo adicional en los temas de Prioridad 2 de Exactitud, Personas jurídicas vs. físicas, y Factibilidad de contactos únicos, discrepamos con la narrativa de que estos temas no se abordaron durante la Fase II. De hecho, cada uno de estos temas se trató en profundidad, incluido un análisis detallado de Bird & Bird que apoya la idea de mantener el *statu quo*. Recomendamos que el trabajo posterior sobre estos temas no empiece de cero, sino que se incorpore el importante trabajo que el Equipo responsable del EPDP ha realizado sobre estos temas. Creemos que es importante asegurarnos de que somos transparentes y precisos en nuestro tratamiento de estas cuestiones para evitar conceptos erróneos en la comunidad. Estas son algunas de sus ideas:

Exactitud: Bird & Bird confirmó que la exactitud en virtud del GDPR es un derecho del titular de los datos (y no de terceros) y una obligación de los responsables del tratamiento de datos.[119] Además, Bird & Bird confirmó que los procedimientos existentes en el Acuerdo de Acreditación de Registradores para confirmar los datos de los registratarios no son insuficientes para cumplir los requisitos de exactitud en virtud del GDPR.[120]

Personas jurídicas vs. físicas: no discutimos que el GDPR se aplica a los datos de las personas físicas y no a los de las personas jurídicas. Hemos insistido en que el desafío práctico consiste en determinar de manera confiable si los datos entran en alguna de las dos clasificaciones, y cómo manejar los registros de personas jurídicas que puedan contener los datos de personas físicas. Si bien algunos han sugerido recurrir al consentimiento como mecanismo para reducir el riesgo, Bird & Bird confirmó que depender del consentimiento no es una solución fácil y que aún implica un riesgo significativo de responsabilidad para las partes contratadas.[121]

Factibilidad de contactos únicos: recibimos un asesoramiento jurídico preciso sobre esta cuestión en el que se reconoce que, si bien la seudonimización y la anonimización son medidas útiles para mejorar la privacidad, la publicación de correos electrónicos enmascarados no cumpliría esas normas porque están destinados específicamente a garantizar la posibilidad de contactar a las personas.[122] Además, observamos que el texto de la recomendación propuesta sobre esta cuestión se presentó en la sesión

[119] Ruth Boardman y Katerina Tassi (Bird & Bird LLP), “Asesoramiento sobre el principio de exactitud en el marco del Reglamento General de Protección de Datos (Reglamento (UE) 2016/679) (“GDPR”): consultas de seguimiento sobre los memorandos 'Persona jurídica vs. física' y 'Exactitud'," con fecha del 9 de abril de 2020.
[120] Ruth Boardman y Gabe Maldoff (Bird & Bird LLP), “Asesoramiento sobre el significado del principio de exactitud de conformidad con el Reglamento General de Protección de Datos (Reglamento (UE) 2016/679) ("GDPR")", con fecha del 8 de febrero de 2019.
[121] Ruth Boardman (Bird & Bird LLP), “Asesoramiento sobre las opciones de consentimiento con el fin de hacer públicos los datos personales en el RDS y los requisitos del Reglamento General de Protección de Datos (Reglamento (UE) 2016/679) ("GDPR")", con fecha de marzo de 2020.
[122] Ruth Boardman (Bird & Bird LLP), “"Segundo lote" de preguntas del GDPR sobre un Sistema Estandarizado de Acceso/Divulgación ("SSAD"), Privacidad/Proxy y correos electrónicos seudonimizados", con fecha del 4 de febrero de 2020.

plenaria del 12 de marzo de 2020 y no recibió ninguna objeción, solo para ser omitido posteriormente en el Informe Final.[123]

Los responsables del tratamiento de datos necesitan flexibilidad para cumplir sus obligaciones

Apoyamos los compromisos necesarios para llegar a un acuerdo sobre la Recomendación 8 (Autorización de la Parte contratada), pero nos preocupa que el marco se haya vuelto demasiado prescriptivo. Lo que comenzó como pautas para que la entidad encargada de la divulgación PUDIERA tomar una determinación se ha vuelto algo rígido en cuanto a cómo DEBE tomar una determinación. Si bien los Registros apoyan el principio de estandarización establecido por el grupo de trabajo, no hay manera de que esta política tenga en cuenta todas las variaciones en las jurisdicciones locales con diferentes leyes y reglamentos en materia de privacidad, en particular cuando las solicitudes se hacen de forma transfronteriza. Al implementar y exigir el cumplimiento de esta recomendación se debe tener cuidado de que la entidad encargada de la divulgación tenga suficiente flexibilidad para dar cuenta de sus obligaciones jurídicas y jurisdiccionales específicas, a fin de evitar que esta recomendación sea inexigible.

Propósito 2

El nuevo texto del Propósito 2 de la Recomendación 22 sustituye al Propósito 2 original de la Recomendación 1 de la Fase 1 del EPDP que no fue acordado o adoptado por la Junta Directiva de la ICANN. Reiteramos nuestra preocupación de la Fase 1[124] en la que señalamos que este propósito no se califica como un "Propósito" legal según la definición del GDPR.[125] No queda claro que cuando se dice "contribuir al mantenimiento de la seguridad, estabilidad y resiliencia del Sistema de Nombres de Dominio de acuerdo con la misión de la ICANN" un titular de los datos entenderá cómo se procesarán sus datos ni por qué es necesario. Teniendo en cuenta lo anterior y el

[123] "El Equipo responsable del EPDP aceptó el texto preliminar de la recomendación para la factibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme y para la censura del campo que especifica la ciudad. Apoyo del personal para incluir estas recomendaciones preliminares en el anexo sobre los temas de Prioridad 2, que se publicará para comentario público". Correo electrónico de Caitlin Tubergen al Equipo responsable del EPDP de la GNSO con fecha del 12 de marzo de 2020.
[124] Informe Final de la Fase I del EPDP, Declaración Minoritaria del RySG de la Fase I, pág. 166, disponible en este enlace.
[125] Directrices de la Oficina del Comisionado de Información (ICO) sobre limitación del propósito: "Este requisito tiene por objeto garantizar que usted sea claro y abierto sobre sus motivos para obtener datos personales y que lo que haga con los datos esté en consonancia con las expectativas razonables de las personas en cuestión. Especificar sus propósitos desde el principio le permite asumir la responsabilidad de su procesamiento y le permite evitar "desviaciones de uso". También ayuda a las personas a comprender cómo se utilizan sus datos, tomar decisiones sobre si están dispuestos a compartir sus detalles y a ejercer sus derechos sobre los datos cuando corresponda. Es fundamental para generar una confianza pública en la forma en que se utilizan los datos personales". Disponible en este enlace.

apoyo de la Junta Directiva para este propósito[126] y el espíritu con el que creemos que se plantea, el RySG ha acordado no oponerse a este propósito.

Conclusión

El RySG se comprometió a participar activamente y de buena fe en la elaboración de recomendaciones de políticas consensuadas adecuadas en torno al acceso a los datos de los registratarios. Nos hemos centrado en asegurar que dichas recomendaciones proporcionen un camino claro hacia el cumplimiento del GDPR, sean comercialmente razonables e implementables, tengan en cuenta nuestros diferentes modelos comerciales y no dificulten la innovación. En consonancia con estos principios, y teniendo en cuenta las preocupaciones detalladas anteriormente, ofrecemos nuestro apoyo consensuado a las recomendaciones del Informe Final. Esperamos que el Consejo de la GNSO lo examine y lo apruebe.

[126] Carta de Martin Botterman a Keith Drazek, con fecha del 11 de marzo de 2020, disponible en este enlace.

SSAC: Declaración minoritaria sobre el Informe Final de la Fase 2 del Proceso Expeditivo de Desarrollo de Políticas (EPDP) sobre la Especificación Temporaria para los Datos de Registración de los gTLD – SSAC 112

Prefacio

Esta es una Declaración Minoritaria del Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN sobre el Informe Final de la Fase 2 del Proceso Expeditivo de Desarrollo de Políticas (EPDP) sobre la Especificación Temporaria para los Datos de Registración de los gTLD.

El SSAC se centra en cuestiones relativas a la seguridad y la integridad de los sistemas de asignación de nombres y direcciones de Internet. Esto incluye las cuestiones operativas (por ejemplo, las relacionadas con el funcionamiento correcto y fiable del sistema de publicación de la zona raíz), cuestiones administrativas (por ejemplo, las relativas a la asignación de direcciones y números en Internet) y cuestiones de registración (por ejemplo, las relacionadas con los servicios de registro y registrador). El SSAC participa en la evaluación continua de amenazas y análisis de riesgos de los servicios de asignación de números y direcciones en Internet, para entender dónde residen las principales amenazas a la estabilidad y la seguridad, y asesora a la comunidad de la ICANN en consecuencia. El SSAC no tiene la facultad de regular, ejecutar o adjudicar. Esas funciones pertenecen a otras partes, y el asesoramiento brindado aquí debe ser evaluado según sus propios méritos.

Resumen Ejecutivo

El SSAC no puede respaldar el Informe Final de la Fase 2 del Proceso Expeditivo de Desarrollo de Políticas sobre la Especificación Temporaria para los Datos de Registración de los gTLD[127] (en adelante, "El Informe Final") en su estado actual.

En primer lugar, creemos que es posible un sistema mucho mejor dentro de las limitaciones impuestas por el Reglamento General de Protección de Datos (GDPR) y que el EPDP *no* ha proporcionado resultados que sean razonablemente adecuados para la seguridad y la estabilidad.

En segundo lugar, el Informe Final no recomienda el compromiso de terminar los artículos de la carta orgánica sin abordar. El SSAC condicionó su participación y apoyo de la Fase 2 del EPDP a la promesa de que se examinarían varias cuestiones de la Fase 1. Lamentablemente, no se examinaron y siguen sin abordarse.

En tercer lugar, además de las cuestiones analizadas anteriormente, hay algunas recomendaciones específicas a las que el SSAC se opone, a saber:

[127] Véase https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-31jul20-en.pdf.

- *Recomendación n.° 6: Niveles de prioridad.* La clasificación de las amenazas de ciberseguridad como "Prioridad 3" es insuficiente para hacer frente a la realidad de las graves amenazas en línea.
- *Recomendación n.° 10: Determinación de los SLA variables para el tiempo de respuesta para el SSAD* Al SSAC le preocupan los largos tiempos de respuesta, que el cumplimiento de los Acuerdos de nivel de servicio no sea prácticamente exigible y que el asesoramiento sobre la implementación pueda dar lugar a que las partes contratadas respondan a las solicitudes de datos con mayor lentitud a lo largo del tiempo.
- *Recomendación n.° 12: Requisito de divulgación.* Al SSAC le preocupa que las partes contratadas puedan, a su discreción, revelar la identidad de los solicitantes de datos, en lugar de hacerlo únicamente cuando lo exija la ley de protección de datos. Revelar la identidad de los solicitantes de datos puede ponerlos en peligro y comprometer las investigaciones.
- *Recomendación n.° 14: Sostenibilidad financiera.* La recomendación contiene un texto erróneo que transfiere injustamente los costos a las víctimas, es incongruente con las prácticas comerciales normales y va en contra de las recomendaciones anteriores del SSAC a la Junta Directiva de la ICANN. La recomendación no se redactó de acuerdo con los procedimientos de la GNSO, no está respaldada por pruebas y puede que no cumpla con el GDPR.

El sistema estandarizado de acceso/divulgación a datos de registración sin carácter público (SSAD) previsto en la Fase 2 puede convertirse en una mejora con respecto al *statu quo*, si se modifican algunas de las recomendaciones y si la GNSO se compromete a completar el trabajo que formaba parte de la carta orgánica del EPDP pero que sigue sin abordarse. Una vez que la GNSO pueda garantizar que las cuestiones de las personas físicas vs. personas jurídicas, los servicios de privacidad/proxy y la exactitud de los datos se examinarán rápidamente mediante la elaboración de políticas formales, el SSAC podrá aprobar el Informe Final.

1 Introducción

El SSAC ha participado en el EPDP con un espíritu de profesionalidad y buena fe, dedicando miles de horas de voluntariado en ambas fases y trabajando diligentemente con nuestros colegas de toda la comunidad de la ICANN.

Como se indica en el documento SAC111:

> El SSAC se ha comprometido en muchos asuntos, como la mayoría de los participantes, en el interés de avanzar y poner un sistema en línea. A los efectos de evitar dudas, el Informe de la Fase 2 y sus recomendaciones actualmente están muy lejos de lo que el SSAC considera que es necesario y posible para

> abordar los problemas de seguridad y estabilidad dentro de la competencia de la ICANN. El SSAC no cree que la versión inicial del Sistema Estandarizado de Acceso/Divulgación (SSAD) entregue los datos de una manera y a una velocidad que satisfaga muchas necesidades de seguridad operacional. Creemos que un mejor sistema es posible dentro de las limitaciones impuestas por el GDPR. Para que las cosas avancen en la actualidad, el SSAC apoya la creación de una base sólida que pueda ser mejorada de manera oportuna en lugar de esperar un sistema ideal.[128]

El SSAC mantiene su declaración. No podemos avalar los resultados generales de la Fase 2 tal y como están actualmente.

Creemos que es posible un sistema mucho mejor dentro de las limitaciones impuestas por el GDPR y que el EPDP no ha proporcionado resultados que sean razonablemente adecuados para la seguridad y la estabilidad. Además, el Informe Final no recomienda el compromiso de terminar los elementos sin abordar de la carta orgánica. El SSAC condicionó su participación y apoyo a la Fase 2 a la promesa de que se examinarían varias cuestiones de la Fase 1. Lamentablemente, no se examinaron y siguen sin abordarse.

De las 22 recomendaciones del Informe Final, el SSAC objeta cuatro de ellas, a saber:

- *Recomendación n.° 6: Niveles de prioridad.* La clasificación de las amenazas de ciberseguridad como "Prioridad 3" es insuficiente para hacer frente a la realidad de las graves amenazas en línea.
- *Recomendación n.° 10: Determinación de los SLA variables para el tiempo de respuesta para el SSAD* Al SSAC le preocupan los largos tiempos de respuesta, que el cumplimiento de los Acuerdos de nivel de servicio no sea prácticamente exigible y que el asesoramiento sobre la implementación pueda dar lugar a que las partes contratadas respondan a las solicitudes de datos con mayor lentitud a lo largo del tiempo.
- *Recomendación n.° 12: Requisito de divulgación.* Al SSAC le preocupa que las partes contratadas puedan, a su discreción, revelar la identidad de los solicitantes de datos, en lugar de hacerlo únicamente cuando lo exija la ley de protección de datos. Revelar la identidad de los solicitantes de datos puede ponerlos en peligro y comprometer las investigaciones.
- *Recomendación n.° 14: Sostenibilidad financiera.* La recomendación contiene un texto erróneo que transfiere injustamente los costos a las víctimas, es incongruente con las prácticas comerciales normales y va en contra de las recomendaciones anteriores del SSAC a la Junta Directiva de la ICANN. La

[128] Véase SAC111, página 5, en: https://www.icann.org/en/system/files/files/sac-111-en.pdf.

recomendación no se redactó de acuerdo con los procedimientos de la GNSO, no está respaldada por pruebas y puede que no cumpla con el GDPR.

No nos oponemos al resto de las recomendaciones del Informe Final. Eso no significa que estemos entusiasmados con todas ellas. Por ejemplo, el SSAC apoya la idea de la acreditación del SSAD, porque la acreditación es una medida de protección destinada a cumplir con el GDPR, que proporciona confianza y permite documentar las solicitudes legítimas. Sin embargo, no sabemos si la acreditación será una herramienta efectiva. Conforme a la política propuesta, el hecho de que se revelen o no los datos dependerá enteramente de la decisión de cada registrador y operador de registro, que variará enormemente en sus métodos y normas de evaluación, y dará lugar a resultados desiguales, subjetivos e impredecibles. Es posible que la política propuesta no ofrezca un recurso eficaz a los solicitantes de datos a quienes se les denieguen sus solicitudes legítimas demostrables. Por lo tanto, independientemente de la solidez del programa de acreditación que se establezca, puede que no dé resultados y no justifique los buenos esfuerzos de los solicitantes de datos. Este no es un resultado confiable y ofrece menos de lo que permite el GDPR.[129]

Varias de las recomendaciones del Informe Final no han recibido el consenso y han recibido la oposición formal de una cantidad notable de organismos participantes. Sin embargo, algunos miembros de la comunidad afirman que el Consejo de la GNSO debe realizar ahora una votación "a favor o en contra" sobre todo el Informe Final, para aprobar todas las recomendaciones o ninguna en absoluto. Creemos que ese enfoque de "todo o nada" eludiría el proceso de consenso. También infringiría el procedimiento de la GNSO, que indica que: "En caso de que el Informe Final incluya recomendaciones que no lograron el consenso [sic] dentro del Equipo responsable del PDP, el Consejo de la GNSO debería deliberar sobre si adoptarlas o devolver las recomendaciones para un mayor trabajo y análisis".[130]

Observamos que, si bien las recomendaciones tratan de crear un programa general, no existe una interdependencia tan estrecha entre todas ellas que haga necesario un voto de "todo o nada". Sin dudas queda margen para modificar las recomendaciones. Algunas recomendaciones (y, por cierto, algunas de las diversas subrecomendaciones) podrían ser rechazadas pero el resto podrían quedar intactas. La idea de que el trabajo completo se desentrañará sin que se aprueben todas las recomendaciones o sin que se apruebe como está redactado actualmente, es una historia falsa. Los procedimientos de la GNSO indican además que: "el Consejo de la GNSO puede adoptar todas o

[129] En julio de 2018, el Comité Europeo de Protección de Datos le escribió a la Organización de la ICANN y afirmó que "los datos personales procesados en el contexto de WHOIS pueden ponerse a disposición de terceros que tengan un interés legítimo en acceder a los datos, siempre que se establezcan las medidas de protección adecuadas para garantizar que la divulgación sea proporcionada y se limite a lo que sea necesario y se cumplan los demás requisitos del GDPR...", carta a Göran Marby del Comité Europeo de Protección de Datos, https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

[130] Manual del Proceso de Desarrollo de Políticas de la GNSO, sección 13 "Deliberación del Consejo", página 8. Este procedimiento también se aplica a los EPDP. https://gnso.icann.org/sites/default/files/file/field-file-attach/annex-2-pdp-manual-24oct19-en.pdf

cualquier parte de las recomendaciones contenidas en el Informe Final" y puede supervisar el trabajo de revisión de las recomendaciones. Puede que sea necesario trabajar arduamente, pero esa es la obligación del Consejo de la GNSO y de la Junta Directiva de la ICANN, que también tendrán que considerar los resultados. La legitimidad de la ICANN y su proceso de múltiples partes interesadas están bajo el microscopio aquí.

El resto de esta declaración detalla las áreas clave de preocupación del SSAC.

2 Temas pendientes de la carta orgánica

En el documento SAC111, el SSAC manifestó su preocupación por el hecho de que había temas de la Carta orgánica del EPDP que no estaban recibiendo tratamiento ni decisiones. Señaló que "importantes cuestiones relacionadas con las áreas temáticas sobre las personas físicas vs. personas jurídicas, el servicio de privacidad/proxy y la exactitud de los datos corren el riesgo de no ser abordadas por el EPDP".[131] Esos temas fueron postergados en la Fase 1. El SSAC condicionó su participación y apoyo de la Fase 2 a la promesa de que se examinarían esas cuestiones. Lamentablemente, no se examinaron y siguen sin abordarse. Por ejemplo,

- En el Informe Final, no se menciona ningún compromiso para examinar la cuestión de personas físicas vs. jurídicas a través de un PDP.
- El Informe Final establece lo siguiente: "Conclusión – Exactitud y Sistema de Informes sobre la Exactitud de WHOIS: de acuerdo con las instrucciones del Consejo de la GNSO, el Equipo responsable del EPDP no seguirá examinando este tema; en cambio, se prevé que el Consejo de la GNSO forme un equipo de estudio para explorar más a fondo las cuestiones relacionadas con la exactitud y el ARS para ayudar a fundamentar una decisión sobre los próximos pasos apropiados para abordar las posibles cuestiones identificadas". Un equipo de exploración no es una promesa de llevar a cabo ningún trabajo. Aquí se necesita una toma de decisiones a nivel de PDP.
- Cuestiones de privacidad/representación (proxy): En el trabajo sobre las cuestiones relativas a la acreditación de servicios de representación (PPSAI) de 2016 no se abordan las cuestiones importantes que plantea el GDPR y que son competencia del EPDP, y las áreas de trabajo de la PPSAI y el EPDP siguen estando aisladas. Hay que seguir trabajando.
    - Es necesario analizar cómo las partes afectadas pueden solicitar los datos de contacto del dominio subyacente a los proveedores de privacidad/representación (proxy) acreditados por la ICANN, que son los

[131] SAC111: Comentario del SSAC sobre el Informe Inicial de la Fase 2 del Proceso Expeditivo de Desarrollo de Políticas (EPDP) sobre la Especificación Temporaria para los Datos de Registración de los gTLD, 4 de mayo de 2020, página 8. https://www.icann.org/en/system/files/files/sac-111-en.pdf

responsables del tratamiento de datos. La capacidad de solicitar esos datos de registración es la razón de ser del EPDP y el SSAD. El Informe Final implica que la ICANN está dejando todos los dominios protegidos por privacidad/proxy fuera del SSAD, y fuera de sus SLA y mecanismos de responsabilidad.

- Esto estaba dentro de la carta orgánica del EPDP. La sección sobre la misión y el alcance de la carta orgánica del EPDP establece lo siguiente: "El Equipo responsable del EPDP deberá considerar qué recomendaciones subsidiarias podría hacer para el trabajo futuro de la GNSO, que podrían ser necesarias para garantizar que las políticas de consenso relevantes, incluidas aquellas relacionadas con los datos de registración, se vuelvan a evaluar para que sean coherentes con la ley aplicable".[132] El EPDP no lo ha hecho en este tema.

La cuestión sobre diferenciación de personas físicas y jurídicas sigue sin abordarse en parte debido a la inexplicable falta de realización de investigaciones en el momento oportuno. En el informe de la Fase 1 del EPDP se recomendó que la ICANN realizara "lo antes posible" una investigación en la que se considerara la factibilidad y los costos de la diferenciación entre personas jurídicas y físicas, la forma en que otras industrias y organizaciones han diferenciado con éxito a las personas jurídicas de las físicas, y los riesgos para la privacidad de los titulares de nombres registrados de la diferenciación de personas jurídicas y físicas (recomendación 17.2).[133] El 15 de mayo de 2019, la Junta Directiva de la ICANN aceptó esa recomendación e instruyó al personal de la ICANN que ejecutara el proyecto como aporte al trabajo de la Fase 2 del EPDP.[134]

Hubo dos errores:

1. El informe de investigación fue entregado al EPDP el 8 de julio de 2020, *después* de que se realizara el Informe Final, demasiado tarde en el proceso para permitir que el tema de personas jurídicas vs. personas físicas tenga su debida consideración.
2. En el informe de investigación no se examinaron algunos de los ejemplos más pertinentes y obvios, como la forma y el motivo por los que se recopilan y publican los datos de las personas físicas y jurídicas en los registros inmobiliarios, los registros de empresas y los registros de marcas comerciales

[132] Carta orgánica adoptada final del EPDP - 19 de julio de 2018. Disponible en: https://community.icann.org/display/EOTSFGRD/EPDP+Team+Charter?preview=/88574674/90767676/EPDP%20FINAL%20Adopted%20Charter%20-%2019%20July%202018.pdf.
[133] https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf.
[134] Véase la Resolución de la Junta Directiva de la ICANN del 15 de mayo de 2019, https://features.icann.org/consideration-gnso-epdp-recommendations-temporary-specification-gtld-registration-data y la tabla de clasificación de la Junta Directiva de la ICANN que la acompaña, Recomendación 17, página 5, https://www.icann.org/en/system/files/files/epdp-scorecard-15may19-en.pdf

dentro de la UE; y la forma en que esos registros fuera de la UE manejan los datos de los titulares que residen en la UE. Si bien en el informe se afirmó que "la mayoría de los operadores de ccTLD de la UE siguen publicando algunos (y a veces todos) los campos de datos de contacto de los dominios registrados por personas jurídicas"[135], el informe no proporcionó los detalles, como una lista de qué ccTLD publican qué datos.

El SSAC solicita que el Consejo de la GNSO y la Junta Directiva de la ICANN expliquen por qué el informe llegó tan tarde y por qué no se cumplió la resolución de la Junta Directiva para los beneficiarios previstos: los participantes de la comunidad en el EPDP. Para fundamentar la adopción de decisiones en el futuro, tal vez sea necesario revisar el informe a fin de que proporcione el análisis que falta, mencionado anteriormente, y otra información pertinente.

Como se señala en el documento SAC111: "La GNSO crea cartas orgánicas explícitamente para que los grupos de trabajo y los participantes en ellos comprendan los resultados previstos. La GNSO cuenta con normas y procedimientos de grupos de trabajo diseñados para llevar a cabo el trabajo de manera predecible y justa, y los grupos que participan en los grupos de trabajo deberían ser capaces de cumplir con los compromisos que asumen entre sí... Cuando los procesos establecidos fallan y no se abordan los elementos fundamentales, se amenaza la legitimidad de la elaboración de políticas de la ICANN sobre cuestiones fundamentales de interés global".[136]

3 Cuestiones generales sobre priorización y capacidad de respuesta para las solicitudes

Estas dos recomendaciones están estrechamente relacionadas, dado que en la Recomendación 6 se establece un concepto de "Prioridad" de las solicitudes de divulgación de datos, y en la Recomendación 10 se define de forma muy precisa la capacidad de respuesta que se espera de las partes contratadas pertinentes para dichas solicitudes. Resulta útil formular recomendaciones de políticas que establezcan prioridades diferenciadas para los diversos tipos de solicitudes de divulgación de datos, dado que algunos datos pueden necesitarse casi de inmediato para mitigar cuestiones que son urgentes y/o de gran repercusión, mientras que otros no presentan necesidades urgentes o apremiantes. Proporcionar orientación en materia de políticas a las partes contratadas y otras personas que participan en el proceso de divulgación sobre los plazos previstos para las respuestas (incluido el estado de las solicitudes y los

[135] Diferenciación entre personas jurídicas y físicas en los Servicios de Directorio de Datos de Registración de Nombres de Dominio. https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20200708/5f72ece1/Rec17.2_Legal-Natural_8jul201-0001.pdf.

[136] SAC111: Comentario del SSAC sobre el Informe Inicial de la Fase 2 del Proceso Expeditivo de Desarrollo de Políticas (EPDP) sobre la Especificación Temporaria para los Datos de Registración de los gTLD, 4 de mayo de 2020, página 8. https://www.icann.org/en/system/files/files/sac-111-en.pdf

datos solicitados, si se aprueban) también es muy útil para crear un sistema con coherencia y responsabilidad.

Lamentablemente, las recomendaciones resultantes fueron mucho más allá de las recomendaciones de política necesarias y prescribieron detalles de implementación muy específicos para esas políticas. Esos detalles son rígidos, insuficientemente matizados y mal diseñados para abordar muchas de las necesidades más urgentes de acceso a los datos de RDS, en particular en el ámbito de la ciberseguridad. Si bien tiene buenas intenciones, la puesta en práctica de un plan de implementación tan detallado en la política puede tener el efecto neto de crear un sistema complejo y difícil de aplicar que sobrecargue a las partes contratadas en muchas categorías de solicitudes, al tiempo que deja a muchos solicitantes de datos con un servicio deficiente lamentable para otros tipos de solicitudes.

El SSAC apoya los objetivos de alto nivel de crear un marco de prioridades y expectativas de respuesta. Sin embargo, el trabajo de implementación debería dejarse en manos del equipo de implementación. Ese equipo debería incluir representantes de las partes contratadas que proporcionarán datos para las solicitudes, las partes que realizan solicitudes de datos con mayor frecuencia y el personal de la ICANN que se encargará de la gestión del SSAD y la supervisión. Las prioridades y los tiempos de respuesta pueden ser elaborados por este equipo y deberían reflejar los casos de uso que se suelen ver y su relativa urgencia con respecto al oportunismo, el impacto y/u otros factores que se determinen de mutuo acuerdo. La lista que figura en la Recomendación 6.1.1 para las solicitudes de Prioridad 1 en el informe constituye un punto de partida para dichos debates, pero no es una lista completa en absoluto. Las recomendaciones finales para que la implementación apoye este marco deberían ser revisadas y aprobadas por el Consejo de la GNSO. Con el transcurso del tiempo, estos factores pueden revisarse y ajustarse utilizando el mecanismo evolutivo previsto en la Recomendación 18 o el equivalente que finalmente se adopte.

4 Objeción a la Recomendación 6 sobre los niveles de prioridad

Ante la falta de un mejor enfoque para la cuestión de las prioridades y los SLA como se ha señalado anteriormente, el SSAC se opone a las recomendaciones 6.1 y 6.2.

La clasificación de las amenazas de ciberseguridad como "Prioridad 3" es lamentablemente deficiente a la hora de abordar las amenazas en línea actuales. Estas clasificaciones no abordan algunos de los ataques en línea más graves perpetrados hoy en día que requieren respuestas ágiles. Dichos ataques generan enormes impactos financieros y exponen millones de registros personales confidenciales en línea, por ejemplo, ransomware, redes de exfiltración de datos y ataques de DDoS masivos de extorsión. Es necesario seguir trabajando en este sistema de clasificación para reflejar el oportunismo y los efectos de las diversas formas de ataques. Como mínimo, dicho sistema proporcionaría un marco normativo que podría orientar los procesos de

implementación práctica para atender a la necesidad de disponer de datos oportunos en función de diversos factores. Si no se actualiza la recomendación 6 para tener en cuenta la necesidad de responder oportunamente a los diversos ataques, se necesitarán límites más estrictos en virtud de la recomendación 10 (Determinación de los SLA variables para el tiempo de respuesta para el SSAD) a fin de proporcionar datos para apoyar los esfuerzos de respuesta ante dichos ataques. El SSAC ha esbozado previamente otros fundamentos para este enfoque en el documento SAC111, Sección 3.2.[137]

5 Objeción a la Recomendación 10 sobre Determinación de los SLA variables para los tiempos de respuesta para el SSAD

A falta de un mejor enfoque de la cuestión de las prioridades y SLA, como se ha señalado anteriormente, el SSAC objeta la Recomendación 10. Aunque la recomendación tiene un buen objetivo, el SSAC no apoya esta recomendación tal como está redactada. Su lógica es errónea, y no proporciona un SLA razonable para responder a las amenazas a la seguridad. Esto se debe, en parte, a la clasificación de las amenazas a la seguridad como "Prioridad 3" en la recomendación 6 (Niveles de prioridad)[138]. Esto es demasiado lento para abordar los incidentes de ciberseguridad.[139]

El objetivo del SLA en la Fase 1 es de cinco (5) días. Pero luego, la Sección 10.11 establece lo siguiente: "En la fase 2, los objetivos de cumplimiento de las Partes contratadas para las solicitudes de Prioridad 3 del SSAD serán diez (10) días hábiles. Lamentablemente, no hay ningún SLA vinculante en absoluto en la Fase 1, y un SLA vinculante con una penalización solo entra en vigencia en la Fase 2. El SLA de la Fase 2 permite a las partes contratadas responder *más lentamente* que en la Fase 1, en lugar de hacerlo más rápidamente a medida que adquieren experiencia. Diez días es simplemente demasiado tiempo para la seguridad y la estabilidad. Esta propuesta no ha cambiado significativamente desde el informe preliminar, y en su momento, el SSAC señaló su objeción a este enfoque contradictorio en la Sección 3.2 del documento SAC111:

> Estos objetivos están desalineados con los motivos por los que se está creando el SSAD. Las solicitudes sobre ciberseguridad son generalmente de prioridad alta. Por lo general, serán de carácter operacional y refieren a la prevención de daños activos y continuos a múltiples víctimas del público durante los ataques (por ejemplo, malware y phishing). Las solicitudes de ciberseguridad operacional tampoco son menos urgentes que las solicitudes del URS. Además, en el modelo general del SSAD se supone que las solicitudes de ciberseguridad

[137] https://www.icann.org/en/system/files/files/sac-111-en.pdf

[138] Aparte del índice de casos que implican "una amenaza inminente a la vida, lesiones corporales graves, infraestructura crítica (dentro y fuera de Internet) o explotación infantil".

[139] Solo un porcentaje mínimo de los problemas de seguridad y los ciberdelitos alcanzará el alto nivel para su tratamiento como Prioridad 1, que requiere "una amenaza inminente a la vida, lesiones corporales graves, infraestructura crítica (dentro y fuera de Internet) o explotación infantil".

serán presentadas por partes acreditadas, dentro de un sistema de rendición de cuentas, con lo que se mitiga la necesidad de una revisión prolongada. El SSAC recomienda que las solicitudes de seguridad operacional (de partes acreditadas) se trasladen a la Prioridad 2. Si el volumen de solicitudes de ciberseguridad es motivo de preocupación para las partes contratadas, sería razonable llegar a un compromiso para responder en un plazo de tres (3) días hábiles.

Los solicitantes y las partes contratadas obtendrán confianza y mejorarán su eficiencia conforme avanza tiempo y, por lo tanto, no existen motivos para que los tiempos de respuesta sean más largos y relajados con el transcurso del tiempo. Por lo tanto, no tiene sentido aumentar el plazo de tiempo que un responsable del tratamiento de datos tiene para responder (definido en el SLA) de la Fase 1 a la Fase 2 para cualquier nivel de prioridad de las solicitudes; deberían permanecer iguales o disminuir entre las fases para la misma prioridad.

Al SSAC le preocupa que los SLA no sean prácticamente exigibles y que el asesoramiento para la implementación presente problemas. El SLA de tiempo de respuesta implica un promedio móvil de todos los tiempos de respuesta. Una parte contratada podría rechazar rápidamente todas las solicitudes de datos, o podría solicitar más información para todas las solicitudes inmediatamente. Esto generará un tiempo promedio de respuesta muy bajo para la parte contratada. Entonces, esto permitiría a la parte contratada retrasar otras solicitudes durante períodos de tiempo prolongados antes de infringir el SLA de respuesta. Dichas acciones automatizadas no están prohibidas por la Recomendación 8.1. Por consiguiente, es importante que el Departamento de Cumplimiento de la ICANN pueda determinar si las partes contratadas están examinando las solicitudes y han respondido en cumplimiento de la Recomendación 8. No estamos seguros de cómo el personal de la organización de la ICANN podría determinar esto y, por lo tanto, no estamos seguros de que los SLA sean prácticamente exigibles.

6 Objeción a la Recomendación 12 sobre el requisito de divulgación

La recomendación 12.2 permitirá a las partes contratadas revelar la identidad de los solicitantes de datos cuando lo deseen, incluso permitiendo la "salida" de los solicitantes de datos como procedimiento rutinario y automatizado. Por lo tanto, la recomendación puede exceder o infringir el asesoramiento proporcionado a la ICANN por el Comité Europeo de Protección de Datos (EDPB), que indicó que no es necesario trasladar las identidades de los solicitantes de datos a los titulares de los datos (registratarios). Revelar la identidad de los solicitantes de datos comprometerá las investigaciones y puede poner en peligro la seguridad y los derechos de los solicitantes de datos, y puede desalentar el uso de las solicitudes del Artículo 6, lo cual seguramente no era la intención del GDPR. Es posible que la parte contratada tenga que cumplir una prueba de equilibrio para revelar la identidad del solicitante, porque

los terceros que solicitan datos son titulares de datos y tienen también derechos en virtud del GDPR.

En la recomendación 12, se debería prohibir a las partes contratantes que revelen la identidad de los solicitantes de datos, a menos que y hasta que lo *exija* la ley aplicable. Recomendamos que los responsables del tratamiento de datos cumplan con la ley y no hagan más que eso. En reiteración de los documentos SAC055 y SAC101v2, "el SSAC cree que los encargados del cumplimiento de la ley y la seguridad tienen una necesidad legítima de acceder a la verdadera identidad de las partes responsables de un nombre de dominio. Dicho acceso debe cumplir con los requisitos legales".

En su carta del 10 de mayo de 2018, la ICANN preguntó al comité Europeo de Protección de Datos (EDPB) lo siguiente:

> "a) ¿Debe exigirse que la identidad de la persona/entidad que presenta una consulta de WHOIS sea visible para el registratario o para otros terceros?"...
>
> b) ¿Debe exigirse que las solicitudes de los organismos encargados del cumplimiento de la ley para acceder a datos de WHOIS sin carácter público sean visibles para el registratario o para terceros?".

En respuesta, el EDPB expresó lo siguiente:

> "Garantizar la capacidad de rastrear el acceso mediante mecanismos de registro adecuados no requiere necesariamente la comunicación activa (traslado) de la información de registro [las identidades de los solicitantes de datos] al registratario o a terceros. Corresponde a la ICANN y a otros responsables del tratamiento de datos que participan en el sistema WHOIS garantizar que la información de registro no se revele a entidades no autorizadas, en particular, con el objetivo de no poner en peligro las actividades legítimas de cumplimiento de la ley".[140]

El GDPR exige que los responsables del tratamiento de datos, al ofrecer servicios, informen en general a los titulares de los datos sobre los *tipos* de partes que pueden procesar sus datos. El GDPR no exige que se notifique activamente a los titulares de los datos cuando sus datos hayan sido solicitados. El GDPR solo puede exigir que los responsables del tratamiento de datos entreguen a los titulares de los datos la identidad de los terceros que soliciten datos, *siempre y cuando el titulares de los datos solicite esa información*.

Revelar la identidad de un solicitante de datos plantea algunos problemas a las Partes contratadas. Revelar las identidades de los solicitantes de datos perjudica y desalienta el uso de las solicitudes del Artículo 6 del GDPR. Puede perjudicar gravemente la

[140] Carta de Andrea Jelinek, Presidenta del EDPB, a Göran Marby, Director Ejecutivo de la ICANN, 5 de julio de 2018. https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

obtención de los datos que se requieren para fines legítimos en virtud del GDPR, como la mitigación del ciberdelito, la defensa de las víctimas y las investigaciones que puedan dar lugar a causas judiciales o a medidas coercitivas. Al parecer, existe una excepción en el GDPR en relación con el derecho de un titular de los datos a ser informado, cuando la revelación o la notificación puedan menoscabar la capacidad de una parte (como un tercero solicitante) para lograr sus fines legítimos.[141] Esto puede ocurrir en el contexto de una investigación.[142]

Estas cuestiones no fueron examinadas por el EPDP, y el EPDP no recibió un asesoramiento jurídico adecuado al respecto. Nos preguntamos qué derechos tienen los solicitantes de datos, dado que también son titulares de datos y sus datos también están protegidos por el GDPR. Para realizar una solicitud conforme al Artículo 6.1.(f), ¿puede obligarse a un solicitante de datos a renunciar a sus derechos de privacidad ante el titular de los datos o el responsable del tratamiento de los datos? (El GDPR estipula que ningún titular de datos puede ser obligado a renunciar a sus derechos de privacidad como condición de un contrato). ¿Y no sería justo que la parte contratada indicara al solicitante de los datos que la parte contratada ha compartido la identidad del solicitante con el registratario, y notificar así a ambas partes?

El SSAC presentó preguntas sobre estas cuestiones al EPDP y a su subequipo jurídico, y propuso que las preguntas se enviaran para recibir asesoramiento jurídico externo. El EPDP denegó esta solicitud y las preguntas nunca se enviaron a Bird & Bird. Como consecuencia, el EPDP no está completamente informado y está permitiendo excesos que no son necesarios y que serán perjudiciales.

7 Objeción a la Recomendación 14 sobre la sostenibilidad financiera

El SSAC rechaza las Recomendaciones 14.2 y 14.6.

La siguiente redacción en la sección 14.2 es inaceptable:

> El objetivo es que el SSAD sea financieramente autosuficiente sin causar ningún cargo adicional a los registratarios. Los titulares de los datos NO DEBEN sufragar los costos de divulgación de sus datos a terceros; los Solicitantes de los datos del SSAD deberían sufragar principalmente los costos de mantenimiento de este sistema. Asimismo, los Titulares de los datos NO DEBEN sufragar los costos del procesamiento de las solicitudes de divulgación de datos, que han sido denegadas por las Partes contratadas tras la evaluación de las solicitudes presentadas por los usuarios del SSAD. La ICANN PUEDE contribuir a la

[141] GDPR, Artículo 14, párrafo 5.
[142] Oficina del Comisionado de Información, "El derecho a ser informado: ¿Hay alguna excepción?" https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/#:~:text=There%20is%20no%20automatic%20exception,a%20specific%20exception%20or%20exemption.

cobertura (parcial) de los costos de mantenimiento de la Puerta de enlace central. Para mayor claridad, el Equipo responsable del EPDP entiende que los registratarios son, en última instancia, la fuente de gran parte de los ingresos de la ICANN. Estos ingresos no infringen *per se* la restricción que indica que "los titulares de los datos NO DEBEN sufragar los costos de divulgación de sus datos a terceros".

1) Los solicitantes de datos no deberían sufragar principalmente los costos de mantenimiento del sistema.[143] Los solicitantes ciertamente deberían pagar el costo de acreditarse y mantener su acceso al sistema. Pero el texto actual de la sección 14.2 hace que las víctimas y los defensores cubran los costos de funcionamiento del sistema, lo cual es injusto y potencialmente peligroso para la seguridad de Internet. Como señaló el SSAC en el documento SAC101v2: "Un sistema no gratuito [en el que los solicitantes de datos deben pagar tarifas por las consultas] podría hacer que el costo de las consultas necesarias para detectar y mitigar el uso indebido de los dominios fuera prohibitivamente caro y muy difícil desde el punto de vista operativo".

2) Este pronunciamiento es amplio y todavía puede ser mal interpretado: "Los titulares de los datos NO DEBEN sufragar los costos de divulgación de sus datos a terceros". Luego, fue modificado con el siguiente texto: “Para mayor claridad, el Equipo responsable del EPDP entiende que los registratarios son, en última instancia, la fuente de gran parte de los ingresos de la ICANN. Estos ingresos no infringen *per se* la restricción que indica que "los titulares de los datos NO DEBEN sufragar los costos de divulgación de sus datos a terceros".

Esa redacción todavía impide que los registradores trasladen los costos del programa del SSAD a sus registratarios en el desarrollo normal de las actividades comerciales. Las partes contratadas generalmente ejecutan sus responsabilidades básicas como parte del costo de su actividad comercial y pueden trasladar los costos a sus clientes.[144] Pero la sección 14.2 lo prohíbe. Ninguno de los anteriores PDP ha protegido a los registratarios de que se les transfieran los costos asociados a los servicios "básicos" de registración o a la implementación de políticas de consenso. Ninguno de los anteriores PDP ha tratado de manipular el funcionamiento de las fuerzas del mercado como se propone en la Recomendación 14.

Si el objetivo es simplemente prohibir que los registradores cobren una tarifa de servicio a un registratario cuando un tercero solicite realmente los datos de ese registratario, entonces solo basta con decirlo, de forma clara y concisa.

3) El SSAD no debería ser necesariamente "autosuficiente desde el punto de vista financiero", y no existen suficientes motivos que haya proporcionado el EPDP para

[143] Véase Recomendación 14.6.
[144] Véase SAC101v2, sección 5.4.

exigirlo. Como se ha establecido anteriormente,[145] el SSAC cree que el inicio de los cargos por el acceso al RDDS, o cualquier cambio futuro significativo en las tarifas por el acceso al RDDS, debe incluir una evaluación formal de las repercusiones en los usuarios y las repercusiones en la seguridad y la estabilidad. El EPDP no estudió los problemas asociados como se le solicitó, y no ha justificado la recomendación de política como lo exige el procedimiento de la GNSO. El texto de la sección 14.2 también ignora el asesoramiento del SSAC a la Junta Directiva de la ICANN, que la Junta Directiva transmitió a la GNSO. Todos estos factores hacen que la Recomendación 14 sea prematura.

El 23 de junio de 2019, la Junta Directiva de la ICANN consideró el documento SAC101v2 y remitió sus recomendaciones al Consejo de la GNSO para que las considerara para su inclusión en el trabajo de la Fase 2 del EPDP. El asesoramiento establecía lo siguiente: "El inicio de los cargos por el acceso al RDDS, o cualquier cambio futuro significativo en las tarifas por el acceso al RDDS, debe incluir una evaluación formal de las repercusiones en los usuarios y las repercusiones en la seguridad y la estabilidad, y debe ser llevada a cabo como parte de un Proceso de Desarrollo de Políticas (PDP) formal. Y: "La Junta Directiva de la ICANN debería garantizar que se lleve a cabo una evaluación formal de los riesgos de seguridad de la política de datos de registración como aporte al Proceso de Desarrollo de Políticas. También se debería realizar una evaluación aparte de los riesgos de seguridad en relación con la implementación de la política".[146]

Esas evaluaciones de las repercusiones en los usuarios y en la seguridad nunca se llevaron a cabo en ninguna parte. Es inapropiado que el EPDP asigne costos a los solicitantes de datos del SSAD sin evaluar las repercusiones que tiene en ellos, y sin evaluar las repercusiones en la seguridad del DNS.

Cuando el EPDP creó la Recomendación 14.2, no siguió los procedimientos de la GNSO y por lo tanto, no se justifica como propuesta de política. El Manual para Procesos de Desarrollo de Políticas de la GNSO establece específicamente que: "El Equipo responsable del PDP debe considerar cuidadosamente los impactos presupuestarios, la aplicabilidad y/o la viabilidad de sus solicitudes de información propuestas y/o recomendaciones posteriores". El Manual para Procesos de Desarrollo de Políticas de la GNSO también exige que se incluya en el Informe Inicial "una declaración sobre el debate del grupo de trabajo relativo a las repercusiones de las recomendaciones propuestas, que podría considerar áreas como la económica, la competencia, las operaciones, la privacidad y otros derechos, la escalabilidad y la factibilidad".

[145] Véase SAC101v2 y SAC111.

[146] Resolución de la Junta Directiva de 23 de julio de 2019, en: https://features.icann.org/consideration-ssac-advisory-regarding-access-domain-name-registration-data-sac101

Pero el EPDP no examinó las repercusiones presupuestarias y de aplicabilidad en los *solicitantes de datos*. El EPDP no examinó las repercusiones presupuestarias y de aplicabilidad en general, salvo para recibir una estimación vaga e indocumentada de los costos de la puesta en marcha del sistema central proporcionada por el personal de la organización de la ICANN. El EPDP nunca estudió las dimensiones de las operaciones ni la competencia, y no evaluó cómo los cargos de acceso afectarán a la seguridad y la estabilidad. El texto de la sección 14.2 no ha sido estudiado ni justificado adecuadamente.

Después de los amplios pronunciamientos de política de la Recomendación 14.2, el Informe Final establece que todos los detalles deben tratarse en la fase de implementación. La fase de implementación es un lugar inapropiado para considerar esas cuestiones de políticas fundamentales, y cualquier implementación tendrá que seguir los principios erróneos e injustificados que figuran actualmente en la sección 14.2.

4) No es necesario forzar a los solicitantes de datos a "sufragar principalmente los costos de mantenimiento del sistema". El uso de los fondos de la ICANN es una alternativa viable.

El SSAD es el sistema de acceso escalonado que la comunidad de la ICANN ha anticipado desde hace tiempo como una característica del sistema de RDS.[147] Los servicios de datos de registración siempre han sido una oferta de servicios básicos proporcionada por las partes contratadas como un recurso público.[148] Como se había previsto desde hace algunos años, el acceso escalonado/diferenciado ha sido necesario ahora debido a los cambios en la ley. El SSAD servirá a una necesidad básica que es en beneficio del interés público. Por lo tanto, es inusual que la Recomendación 14 prohíba básicamente que las tarifas de registración de dominios de la ICANN se utilicen para apoyar el funcionamiento del sistema.

El uso de los fondos de la ICANN parece sumamente congruente con la misión de la ICANN. La Especificación Temporaria también nos recuerda que "la ICANN está generalmente comprometida a "mantener el sistema WHOIS existente en la mayor medida posible", y "la misión de la ICANN implica directamente la facilitación del procesamiento de datos por parte de terceros para fines legítimos y proporcionados relacionados con el cumplimiento de la ley, la competencia, la protección del consumidor, la confianza, la seguridad, la estabilidad, la resiliencia, el uso indebido malicioso, la soberanía y la protección de los derechos". Para obtener más información

[147] La comunidad de la ICANN ha pensado en el acceso escalonado o diferenciado como una próxima característica de los Servicios de Directorio de Datos de Registración. Por ejemplo, el protocolo RDAP se diseñó específicamente para proporcionar un acceso escalonado/diferenciado, porque la comunidad entendió que las leyes de privacidad podrían exigir que ciertos tipos de datos se compartieran únicamente con usuarios autorizados. Ahora, se está contemplando el SSAD como la forma de proporcionar datos sensibles (y puede o no emplear el RDAP).
[148] Véase SAC101v2, sección p.4.

sobre los compromisos pertinentes de la misión de la ICANN, véase la sección 5.4 del documento SAC101v2.[149]

Un ejemplo similar es el Servicio de Datos de Zona Centralizado (CZDS), que la ICANN creó y mantiene con fondos de la ICANN. La ICANN lo hace porque los archivos de zona son un recurso crítico utilizado con fines legítimos por una variedad de usuarios. Y el CZDS proporciona beneficios no solo a sus usuarios sino también a las partes contratadas, que reciben una forma conveniente de gestionar las suscripciones de archivos de zona. El SSAD presenta la misma situación y está diseñado para proporcionar beneficios tanto a sus solicitantes de datos como a las partes contratadas.

5) Esta frase fue una adición de último momento a la Recomendación 14: "Asimismo, los titulares de los datos NO DEBEN sufragar los costos del procesamiento de las solicitudes de divulgación de datos, que han sido denegadas por las Partes contratadas tras la evaluación de las solicitudes presentadas por los usuarios del SSAD". No está claro por qué esta adición es incluso necesaria, y pone en duda que los costos de la evaluación de solicitudes de datos se puedan trasladar de manera alguna a los registratarios, incluso en el desarrollo normal de las actividades comerciales.

6) La recomendación dice: "La Puerta de enlace central NO DEBE cobrar una tarifa aparte a los titulares de los datos por el hecho de que sus datos sean solicitados por o divulgados a terceros". No vemos cómo la Puerta de enlace central podría cobrar a los registratarios. La Puerta de enlace central no tiene ninguna relación comercial con los registratarios.

7) Las acciones de los *registratarios* son generalmente las que hacen que los terceros presenten solicitudes de datos.

8) El SSAC no sabe si la Recomendación 14 infringirá el GDPR.

La Recomendación 14 (incluida la sección 14.6) prevé que los solicitantes de datos paguen tarifas para realizar las solicitudes de datos. El pago de una tarifa de utilización es la única forma de lograr el modelo de "recuperación de costos" previsto en las Recomendaciones 14.2 y 14.6, o de hacer funcionar el sistema sin trasladar los costos a los titulares de los dominios/titulares de los datos.

Conforme al GDPR, si los titulares de los datos desean recibir, actualizar o solicitar la eliminación de sus datos, no se les puede cobrar por ello.[150] En virtud del GDPR, los

[149] https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf

[150] Véase el GDPR, Artículo 15, Artículo 57(4) y la Oficina del Comisionado de Información: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ El GDPR permite cobrar a los titulares de los datos únicamente cuando sus solicitudes sean "manifiestamente infundadas o

terceros con intereses legítimos pueden recibir los datos cuando su derecho prevalece sobre los intereses del titular de los datos. En el SSAD, los terceros suelen realizar dichas solicitudes porque pueden alegar legítimamente que sus derechos están siendo violados por un titular de datos (registratario). El EPDP no examinó si los cobros por solicitudes de datos de terceros están permitidos en virtud del GDPR, o bajo qué circunstancias. La EPDP no procuró asesoramiento jurídico sobre esta cuestión, incluso después de que el SSAC propusiera que la cuestión se enviara para recibir asesoramiento jurídico externo.

Este problema puede evitarse si la ICANN subsidia el SSAD.

8 Otros comentarios

A continuación se incluyen comentarios sobre otras recomendaciones, a las que el SSAC no se opuso, pero que pueden mejorarse. Encomendamos estos comentarios a la GNSO para su consideración.

Respecto a la Recomendación n.° 14:
La recomendación 14.8 es errónea y probablemente innecesaria. Dice: "Al implementar y poner en funcionamiento el SSAD, se debería evitar una carga desproporcionadamente alta para los operadores de menor tamaño". No creemos que nadie sepa lo que significa "una carga desproporcionadamente alta para los operadores de menor tamaño", ni cuáles sean las implicaciones de esta frase. Es evidente que todos y cada uno de los registradores y operadores de registro, sin importar cuán grande o pequeño sea, tendrán que utilizar el SSAD. Es posible que se requiera un esfuerzo mínimo para que cualquier "operador" lo utilice. Ese será el costo de la actividad comercial en el espacio de gTLD y para mantener la acreditación de la ICANN. Nuestra preocupación es que la sección 14.8 no se utilice como una forma de quitarle al SSAD la funcionalidad necesaria.

También es necesario revisar en consecuencia la sección de la Recomendación 14 relativa a las Pautas para la implementación.

La recomendación 18.2.3 indica lo siguiente: "las recomendaciones sobre las operaciones del SSAD y políticas elaboradas por el Comité Permanente deben lograr el consenso de los miembros del Comité para ser enviadas como recomendaciones formales al Consejo de la GNSO. Para que las recomendaciones logren una designación consensuada, **se requerirá el apoyo de las Partes contratadas**". (énfasis agregado)

El Comité Permanente puede realizar dos tipos de recomendaciones:

excesivas". En el SSAD, las solicitudes de datos que sean infundadas o excesivas no están permitidas y serán rechazadas.

- Un tipo son las recomendaciones para cambios contractuales vinculantes. Cuando se sometan a votación por parte de la GNSO, deben alcanzar con un alto nivel (mayoría calificada) conforme a los Estatutos de la ICANN. Básicamente requieren el apoyo de las Partes contratadas para aprobarse.
- El otro tipo son las recomendaciones de implementación. No serán contractualmente vinculantes para las Partes contratadas.

El problema es que la Recomendación 18 aplica el nivel alto de la mayoría calificada a ambos casos, pero solo debería aplicarse al primero. Tal y como está redactada, la Recomendación 18 otorga a las Partes contratadas un poder de veto sobre las opciones de implementación. Hasta donde sabemos, no es un proceso estándar en la toma de decisiones de la GNSO otorgar a cualquier parte o cámara el poder de veto sobre este nivel de decisión.[151]

También existe un problema práctico: no sabemos si las SO y los AC querrán participar en el Comité Permanente si las cuestiones de implementación pueden ser vetadas por uno o dos participantes.

No vemos cómo las cuestiones de implementación llegarían al nivel del Proceso de Orientación de la GNSO, que requiere una votación por mayoría calificada.

9 Reconocimientos, manifestaciones de interés, discrepancias, opiniones alternativas y abstenciones

En aras de la transparencia, estas secciones proporcionan al lector información sobre los aspectos del proceso del SSAC. La sección Reconocimientos enumera los miembros del SSAC, los expertos externos y el personal de la ICANN que contribuyeron directamente en este documento específico. La sección Manifestaciones de interés apunta a las biografías de todos los miembros del SSAC, que manifiestan intereses que pueden representar un conflicto, ya sea real, presunto o potencial, con la participación de un miembro en la elaboración de este informe. La sección Discrepancias y opiniones alternativas ofrece un lugar para que los miembros individuales describan cualquier desacuerdo, u opinión alternativa, que puedan tener con respecto al contenido de este documento o el proceso para su elaboración. La sección Abstenciones identifica a los miembros individuales que se han abstenido de participar en el debate del tema con el que se relaciona este informe. A excepción de los miembros mencionados en la sección Discrepancias y opiniones alternativas y en la sección Abstenciones, este documento tiene la aprobación consensuada de todos los miembros del SSAC.

9.1 Reconocimientos

[151] No vemos cómo las cuestiones de implementación llegarían al nivel del Proceso de Orientación de la GNSO, que requiere una votación por mayoría calificada.

El Comité desea expresar su agradecimiento a los siguientes miembros del SSAC por su tiempo, aportes y revisión en la elaboración de este informe.

Miembros del SSAC
Greg Aaron
Benedict Addis
Ben Butler
Steve Crocker
James Galvin
John Levine
Rod Rasmussen
Tara Whalen

Personal de la ICANN
Andrew McConachie
Danielle Rutherford
Kathy Schnitt
Steve Sheng (editor)

9.2 Manifestaciones de Interés

La información biográfica de los miembros del SSAC y sus Manifestaciones de Interés se encuentran disponibles en: https://www.icann.org/resources/pages/ssac-biographies-2019-11-20-en

9.3 Discrepancias y opiniones alternativas

No hubo discrepancias ni opiniones alternativas.

9.4 Abstenciones

No hubo ninguna abstención.

Anexo F – Aportes de la comunidad

F.1. Solicitud de aportes de SO/AC/SG/C

De acuerdo con el Manual de PDP de la GNSO, un Equipo responsable del EPDP debería solicitar formalmente declaraciones a cada unidad constitutiva y Grupo de Partes Interesadas de la GNSO en la primera etapa de deliberación. También se alienta al Equipo responsable del EPDP a buscar la opinión de los demás Comités Asesores y Organizaciones de Apoyo de la ICANN que puedan contar con pericia, experiencia o interés en el asunto. Como resultado, el Equipo responsable del EPDP se ha extendido a todas las Organizaciones de Apoyo y Comités Asesores de la ICANN, así como a los Grupos de Partes Interesadas y unidades constitutivas de la GNSO, a través de una solicitud de aportes al inicio de sus deliberaciones sobre la fase 2. En respuesta, se recibieron declaraciones de:

- La Unidad Constitutiva de Negocios (BC) de la GNSO
- El Grupo de Partes Interesadas No Comerciales (NCSG) de la GNSO
- El Grupo de Partes Interesadas de Registros (RySG)
- El Grupo de Partes Interesadas de Registradores (RrSG)
- La Unidad Constitutiva de Proveedores de Servicios de Internet y Servicios de Conectividad (ISPCP)

Aquí pueden verse las declaraciones completas: https://community.icann.org/x/zIWGBg.

Todos los aportes recibidos fueron agregados a la herramienta de revisión de aportes iniciales y considerados por el Equipo responsable del EPDP.

F.2. Foro de Comentario Público sobre el Informe Inicial

El 7 de Febrero de 2020, el Equipo responsable del EPDP publicó su Informe Inicial para comentario público. En el Informe Inicial se esbozaron las cuestiones básicas debatidas en relación con el Sistema Estandarizado de Acceso/Divulgación a datos de registración de gTLD sin carácter público ("SSAD") propuesto y las recomendaciones preliminares adjuntas.

El Equipo responsable del EPDP utilizó un formulario de Google para facilitar la revisión de los comentarios públicos. Se recibieron 45 aportes de los Grupos de Partes Interesadas de la GNSO, Unidades constitutivas, Comités Asesores de la ICANN, empresas y organizaciones, además de dos aportes de personas. Los aportes recibidos se encuentran en:

https://docs.google.com/spreadsheets/d/1EBiFCsWfqQnMxEcCaKQywCccEVdBc9_ktPA3PU8nrQk/edit?usp=sharing.

Para facilitar su revisión de los comentarios públicos, el Equipo responsable del EPDP desarrolló un conjunto de herramientas para la revisión de comentarios públicos (PCRT) y mesas de debate (véase https://community.icann.org/x/Hi6JBw). A través de las sesiones plenarias y las revisiones en línea, el Equipo responsable del EPDP completó su revisión y evaluación de los aportes proporcionados y acordó los cambios realizados a las recomendaciones y/o el informe.

F.3. Comentario público sobre el Anexo

El 26 de marzo de 2020, el Equipo responsable del EPDP publicó un Anexo al Informe Inicial para comentario público. El Anexo se refiere a las recomendaciones y/o conclusiones preliminares del Equipo responsable del EPDP sobre los temas de prioridad 2 enumerados anteriormente.

El Equipo responsable del EPDP utilizó un formulario de Google para facilitar la revisión de los comentarios públicos. Se recibieron 28 aportes de los Grupos de Partes Interesadas de la GNSO, Unidades constitutivas, Comités Asesores de la ICANN, empresas y organizaciones, además de un aporte de una persona. Los aportes recibidos se encuentran en: https://docs.google.com/spreadsheets/d/1jN5ThNtmcVJ8txdAGw0ynl5vrGJOuEv8xeccvzjR9qM/edit#gid=2086811131.

Para facilitar su revisión de los comentarios públicos, el Equipo responsable del EPDP desarrolló un conjunto de herramientas para la revisión de comentarios públicos (PCRT) y mesas de debate (véase https://community.icann.org/x/Hi6JBw). A través de la revisión en línea y las sesiones plenarias, el Equipo responsable del EPDP completó su revisión y evaluación de los aportes proporcionados y acordó qué recomendaciones y/o conclusiones de prioridad 2 estaban listas para ser incluidas en este Informe Final.

Anexo G – Comité de Asuntos Jurídicos

Preguntas de la Fase 2 presentadas a Bird & Bird

1. Si consideramos un Sistema Estandarizado de Acceso/Divulgación donde:

    - las partes contratadas "CP" están obligadas contractualmente por la ICANN a revelar los datos de registración, incluidos los datos personales,
    - los datos deben ser divulgados a través del RDAP a los Solicitantes, ya sea directamente o a través de un organismo intermediario de acreditación/autorización de solicitudes,
    - la acreditación la lleva a cabo un tercero encargado por la ICANN sin la participación de las Partes contratadas,
    - la divulgación se realiza de forma automatizada sin ninguna intervención manual,
    - se informa debidamente a los titulares de los datos, de conformidad con los requisitos contractuales de la ICANN, sobre los fines para los que se pueden procesar los datos personales y los tipos de entidades que pueden hacerlo. El contrato de las Partes contratadas con la ICANN también exige que las mismas notifiquen al titular de los datos sobre esta posible divulgación y procesamiento de terceros antes de que el titular de los datos firme el acuerdo de registro con las Partes contratadas, y nuevamente cada año a través del recordatorio de exactitud de los datos de registración que exige la ICANN. Las Partes contratadas lo han hecho.

    Además, suponer que se han establecido las siguientes medidas de protección

    - La ICANN, o quien esta designe, ha validado/verificado la identidad del Solicitante, y ha requerido en cada caso que el Solicitante:
        - demuestre que tiene un fundamento jurídico para solicitar y procesar los datos,
        - proporcione su fundamento jurídico,
        - demuestre que está solicitando únicamente los datos necesarios para su propósito,
        - acuerde procesar los datos de conformidad con el GDPR, y
        - acepte las cláusulas contractuales estándar de la UE para la transferencia de datos.

    - La ICANN, o quien esta designe, registra las solicitudes de datos de registración sin carácter público, audita estos registros de forma periódica, toma medidas de cumplimiento contra los presuntos usos indebidos y pone estos registros a disposición del titular de los datos cuando así lo solicite.

1. ¿Qué riesgo o responsabilidad, si los hubiere, enfrentarían las Partes contratadas por la actividad de procesamiento de la divulgación en este contexto, incluido el riesgo de que un tercero haga un uso indebido o eluda las medidas de protección?

2. ¿Considerarían que los criterios y medidas de protección descritos anteriormente son suficientes para lograr que la divulgación de los datos de registración cumpla con los requisitos? Si existe algún riesgo, ¿qué medidas de protección mejoradas o adicionales eliminarían[1] este riesgo?

3. En este escenario, ¿la Parte contratada se consideraría responsable del tratamiento de datos o encargada del tratamiento[2], y hasta qué punto, en caso de que así sea, se ve afectada la responsabilidad de la Parte contratada por esta distinción entre responsable y encargada del tratamiento?

4. Responder únicamente si aún existe un riesgo para la Parte contratada: Si todavía existe un riesgo para las Partes contratadas, ¿qué medidas de protección adicionales podrían ser necesarias para eliminar la responsabilidad de las Partes contratadas en función de la naturaleza de la solicitud de divulgación, es decir, en función de si los datos son solicitados, por ejemplo, por agentes privados que interponen demandas civiles o por autoridades encargadas del cumplimiento de la ley en función de su jurisdicción o de la naturaleza del delito (falta o delito grave) o de las sanciones asociadas (multa, prisión o pena capital)?

Nota a pie 1: "En este sentido, cabe destacar el rol especial que pueden desempeñar las medidas de protección en la reducción de las repercusiones indebidas en los titulares de los datos y, por consiguiente, en la modificación del equilibrio de derechos e intereses en la medida en que no se invaliden los intereses legítimos del responsable del tratamiento de datos." (https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf)

Nota a pie 2: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

2. En qué medida, si procede, son responsables las partes contratadas cuando un tercero, que accede a datos de WHOIS sin carácter público en el marco de un plan de acreditación mediante el cual el acceso está acreditado para el propósito declarado, se compromete a respetar ciertas medidas de protección razonables similares a un código de conducta en relación con el uso de los datos, pero tergiversa sus propósitos previstos para el procesamiento de esos datos y posteriormente los procesa de manera incongruente con el propósito declarado. En dichas circunstancias, si existe la posibilidad de responsabilidad para las partes contratadas, ¿existen medidas que puedan adoptarse para mitigar o reducir el riesgo de responsabilidad para las partes contratadas?

3. Suponiendo que exista una política que permita a las partes acreditadas acceder a los datos de WHOIS sin carácter público a través de un SSAD (y que requiera que la parte acreditada se comprometa a ciertas medidas de protección razonables similares a un código de conducta), ¿está legalmente permitido, en virtud del Artículo 6.1.(f), realizar lo siguiente?

   · Definir categorías específicas de solicitudes de partes acreditadas (por ejemplo, respuesta rápida a un ataque de malware o contactar a un infractor de propiedad intelectual que no responda), para las cuales pueda haber presentaciones automáticas de datos de WHOIS sin carácter público, sin tener que verificar manualmente las calificaciones de las partes acreditadas para cada solicitud de divulgación individual.
   · Permitir divulgaciones automatizadas de dichos datos, sin que sea necesaria una revisión manual por parte del responsable o encargado del tratamiento de datos de cada solicitud de divulgación individual.

Además, si no es posible automatizar ninguno de estos pasos, por favor proporcionar cualquier orientación sobre cómo realizar la prueba de equilibrio en virtud del Artículo 6.1.(f).

A modo de referencia, consulte las siguientes medidas de protección posibles:

· La divulgación es requerida en virtud del contrato de las Partes contratadas con la ICANN (como resultado de la política de la Fase 2 del EPDP).
· El contrato de las Partes contratadas con la ICANN exige que la Parte contratada notifique al titular de los datos los fines para los que se pueden procesar los datos personales y los tipos de entidades que pueden hacerlo. La Parte contratada debe notificar al titular de los datos sobre esta oportunidad de optar por no hacerlo antes de que el titular de los datos firme el acuerdo de registro con la Parte contratada, y nuevamente cada año a través del recordatorio de exactitud de los datos de registración que exige la ICANN. Las Partes contratadas lo han hecho.
· La ICANN, o quien esta designe, ha validado la identidad del Solicitante, y ha requerido que el Solicitante:
  o demuestre que tiene un fundamento jurídico para solicitar y procesar los datos,
  o proporcione su fundamento jurídico,
  o demuestre que está solicitando únicamente los datos necesarios para su propósito,
  o acuerde procesar los datos de conformidad con el GDPR, y
  o acepte las cláusulas contractuales estándar para la transferencia de datos.
· La ICANN, o quien esta designe, registra las solicitudes de datos de registración sin carácter público, audita estos registros de forma periódica, toma medidas de

cumplimiento contra los presuntos usos indebidos y pone estos registros a disposición del titular de los datos cuando así lo solicite.

4. En virtud del GDPR, el responsable del tratamiento de datos puede divulgar datos personales a las autoridades competentes encargadas del cumplimiento de la ley en virtud del Art. 6.1.(c) del GDPR siempre y cuando la autoridad encargada del cumplimiento de la ley tenga la autoridad legal para crear una obligación jurídica en virtud de la ley aplicable. Algunos comentaristas han interpretado que la "obligación jurídica" se aplica únicamente a las obligaciones jurídicas basadas en la legislación de la Unión Europea o de los Estados miembros.

En cuanto al responsable del tratamiento de datos:

a. En consecuencia, ¿se deduce que el responsable del tratamiento de datos no puede ampararse en el Art. 6.1.(c) del GDPR para divulgar datos personales a las autoridades encargadas del cumplimiento de la ley fuera de la jurisdicción del responsable del tratamiento de datos? De forma alternativa, ¿existe alguna circunstancia en la que los responsables del tratamiento de datos puedan ampararse en el Art. 6.1.(c) del GDPR para divulgar datos personales a las autoridades encargadas del cumplimiento de la ley fuera de la jurisdicción del responsable del tratamiento de datos?

b. ¿Puede el responsable del tratamiento de datos ampararse en cualquier otro fundamento jurídico, además del Art. 6.1.(f) del GDPR, para divulgar datos personales a las autoridades encargadas del cumplimiento de la ley fuera de la jurisdicción del responsable del tratamiento de datos?

En cuanto a la autoridad encargada del cumplimiento de la ley:

Dado que el Art. 6.1 del GDPR establece que las autoridades públicas europeas no pueden utilizar el Art. 6.1.(f) del GDPR como fundamento jurídico para el procesamiento realizado en el desempeño de sus tareas, estas autoridades públicas necesitan tener otra base jurídica para que la divulgación pueda tener lugar (por ejemplo, el Art. 6.1.(c) del GDPR).

c. Ante esta situación, ¿es posible para las autoridades de cumplimiento de la ley no pertenecientes a la UE ampararse en el Art. 6.1.(f) del GDPR como fundamento jurídico para su procesamiento? En este contexto, ¿puede el responsable del tratamiento de datos ampararse en el Art. 6.1.(f) del GDPR para divulgar los datos personales? Si las autoridades encargadas del cumplimiento de la ley no pertenecientes a la UE no pueden ampararse en el Art. 6.1.(f) del GDPR como base legal para su procesamiento, ¿en qué fundamento jurídico pueden ampararse las autoridades encargadas del cumplimiento de la ley no pertenecientes a la UE?

- Resúmenes ejecutivos[152]

Preguntas 1 y 2

Resumen Ejecutivo:
El equipo responsable de la Fase 2 del EPDP envió su primer grupo de preguntas a Bird & Bird el 29 de agosto de 2019. Bird & Bird respondió a este grupo de preguntas en una serie de tres memorandos. El Memorando 1 se entregó el 9 de septiembre de 2019. En el Memorando 1 se analizó la función jurídica de las partes contratadas en el Sistema Estandarizado de Acceso/Divulgación (SSAD) propuesto, la suficiencia de las medidas de protección propuestas y el riesgo de responsabilidad de las partes contratadas por la divulgación a través del SSAD. Las preguntas enviadas a Bird & Bird se proporcionan en el Anexo a este documento e incluyen una serie de supuestos en las Secciones 1.1 y 1.2 que forman parte de la base fáctica de las respuestas que figuran a continuación.

En respuesta a estas preguntas, Bird & Bird señaló lo siguiente con respecto a la responsabilidad del tratamiento:

1. Es probable que las partes contratadas sean los responsables del tratamiento de datos en el SSAD, dado que los registratarios tradicionalmente han previsto razonablemente que las partes contratadas sean los responsables del tratamiento para la divulgación de sus datos a terceros. Es difícil demostrar que las partes contratadas solo sirven a los intereses de la organización de la ICANN, en particular, ante las decisiones judiciales pertinentes que sugieren un bajo umbral para la responsabilidad del tratamiento.
2. Si el Equipo responsable del EPDP quisiera recomendar una política en virtud de la cual las partes contratadas sean encargados del tratamiento en un SSAD, se podrían tomar medidas para apoyar este objetivo de política. Las partes contratadas no tendrían que tener una influencia sustancial en los aspectos fundamentales del procesamiento de los datos del SSAD, como por ejemplo: (i) qué datos se procesarán; (ii) durante cuánto tiempo se procesarán; y (iii) quién tendrá acceso a los datos. También sería necesaria una supervisión "constante y cuidadosa" por parte de la organización de la ICANN "para asegurar el cumplimiento cabal del encargado del tratamiento con las instrucciones y términos del contrato", y esfuerzos para instruir a los registratarios sobre que las partes contratadas solo actúan en representación de la organización de la ICANN (por ejemplo, materiales del sitio web de la organización de la ICANN, avisos de privacidad, información en el proceso de registración de nombres de dominio).
3. Sin embargo, el resultado más probable y la posición de partida de las autoridades de supervisión sería que las partes contratadas sean responsables del tratamiento y

[152] Se actualizará cuando el Comité jurídico apruebe los resúmenes ejecutivos

probablemente responsables conjuntos del tratamiento con la organización de la ICANN en lo que respecta a la divulgación de los datos de registración a través del SSAD.

Bird & Bird señaló lo siguiente con respecto a las medidas de protección y la responsabilidad del SSAD:

4. Dada la cantidad de jurisdicciones involucradas y la probable variedad de solicitudes que podría atender el SSAD, Bird & Bird no pudo confirmar que las medidas de protección y los criterios descritos en los supuestos lograrían que la divulgación de datos en un SSAD totalmente automatizado cumpliera con los requisitos.
5. Bird & Bird sugirió medidas de protección adicionales que el EPDP debería considerar relacionadas con (i) la base legal, la proporcionalidad y la minimización de datos; (ii) los derechos individuales; (iii) la transferencia internacional de datos; y (iv) la seguridad.
6. En virtud del GDPR, las partes que intervienen en el mismo proceso están sujetas a la responsabilidad tanto de las personas como de las autoridades de supervisión. La responsabilidad individual es conjunta y solidaria, lo que significa que cada parte implicada en el procesamiento es potencialmente responsable de todos los daños y perjuicios del titular de los datos, con algunas normas diferentes para los responsables frente a los encargados del tratamiento. Las autoridades de supervisión pueden proceder contra los responsables o encargados del tratamiento y, actualmente, no está claro si la responsabilidad conjunta y solidaria se aplica cuando varias partes participan en el mismo procesamiento (es decir, la acción coercitiva no es apropiada si otros son responsables).

---

1. ¿Las Partes contratadas son responsables o encargados del tratamiento?

Responsables del tratamiento de datos

- La responsabilidad se ve considerablemente afectada por el hecho de que las Partes contratadas sean responsables o encargados del tratamiento. (1.4)

- Un responsable del tratamiento de datos es "la persona física o jurídica, autoridad pública, agencia u otro organismo que, de forma individual o conjuntamente con otros, determina los propósitos y los medios del procesamiento de los datos personales". (2.2)

- El hecho de que una entidad sea responsable del tratamiento es una determinación fáctica basada en el "control sobre las decisiones clave de procesamiento de datos". El rol de responsable del tratamiento no se puede asignar ni rechazar. (2.3)

- El Grupo de Trabajo del Artículo 29 proporcionó una orientación previa al GDPR sobre los roles de responsable y encargado del tratamiento. En la actualidad, el EDPB está revisando esta orientación y prevé una actualización en los próximos seis meses. (2,4; 2,19)

- El predecesor del EDPB, el Grupo de Trabajo del Artículo 29 (WP29), determinó que "la primera y principal función del concepto de responsable del tratamiento es determinar quién será responsable del cumplimiento de las normas de protección de datos y cómo los titulares de los datos pueden ejercer los derechos en la práctica. En otras palabras: asignar la responsabilidad". Si se lee de forma literal, esto refleja que el responsable del tratamiento tiene la responsabilidad de la mayoría de las obligaciones en virtud del GDPR; pero la frase también indica un grado de conveniencia regulatoria: muestra la necesidad subyacente de hacer responsable a alguien. Esto puede influir en el enfoque de un tribunal o de una autoridad supervisora, afirma B&B. (2.4)

- Una entidad que toma decisiones clave (sola o conjuntamente con otras) sobre (i) qué datos se procesan; (ii) la duración del procesamiento; y (iii) quién tiene acceso a los datos, está actuando como responsable del tratamiento, no como encargado del tratamiento. Estos aspectos en ocasiones se denominan "elementos esenciales" del procesamiento. (2.6)

- Una entidad puede ser tanto responsable como encargada del tratamiento. Este será el caso cuando una entidad que actúe como encargada del tratamiento también utilice los datos personales para sus propios fines. (2.7)

Encargados del tratamiento de datos

- Un encargado del tratamiento de datos es "una persona física o jurídica, autoridad pública, agencia o cualquier otro organismo que procesa datos personales en representación del responsable del tratamiento de datos". (2.5)

- En las pautas del Grupo de Trabajo del Artículo 29 se destaca la importancia de examinar "el grado de control real que ejerce una parte, la imagen que se da a los titulares de los datos y las expectativas razonables de los titulares de los datos en base a esta visibilidad" para determinar si una entidad es responsable o encargada del tratamiento. (2.5)
- Según el WP29, un encargado del tratamiento sirve "al interés de otra persona" al "implementar las instrucciones indicadas por el responsable del tratamiento al menos en lo que respecta a la finalidad del procesamiento y los elementos esenciales de los medios". (2.5)

- Un encargado del tratamiento solo puede procesar datos personales de acuerdo con las instrucciones del responsable del tratamiento o según lo requerido por la legislación del EEE o de los Estados miembros. (2.7)

Solicitud para el SSAD

Presunción de responsabilidad del tratamiento

- En algunos casos, "los roles tradicionales existentes que normalmente implican una cierta responsabilidad ayudarán a identificar al responsable del tratamiento: por ejemplo, el empleador en relación con los datos sobre sus empleados, el editor en relación con los datos sobre los suscriptores, la asociación en relación con los datos sobre sus miembros o colaboradores". La relación entre una Parte contratada y el registratario (o el contacto del registratario) podría considerarse de manera similar. (2.8) Del mismo modo, la "imagen que se da a los titulares de los datos y las expectativas razonables de los mismos" es una consideración importante para determinar la responsabilidad del tratamiento. Normalmente, un registratario esperará que las Partes contratadas sean los responsables del tratamiento para la divulgación de sus datos a terceros. (2.9)

- Dado que actualmente se considera que las Partes contratadas son los responsables del tratamiento para la divulgación de datos a terceros, esto dará lugar a la presunción de que las Partes contratadas siguen siendo los responsables del tratamiento, incluso una vez que se implemente un SSAD. (2.9)

- Sin embargo, dicha presunción no siempre puede hacerse, dependiendo del análisis de las actividades técnicas de procesamiento. El WP169 señala que, cuando se supone que una persona es un responsable del tratamiento (lo que en el WP169 se denomina "control derivado de la competencia implícita"), solo debería ser así "a menos que otros elementos indiquen lo contrario". Casos recientes del TJUE, en particular su reciente fallo sobre el caso Fashion ID, también han apoyado un análisis más detallado y específico de los hechos. (2.11)

Dificultad para presentar a las Partes contratadas como si actuaran "en representación de" otra persona

- El elemento más importante del rol de un encargado del tratamiento es que solo actúa en representación del responsable del tratamiento. Será difícil demostrar que las Partes contratadas solo sirven a los intereses de la ICANN y procesan los datos en nombre de la ICANN. (2.10)

- Es probable que la divulgación de datos se considere una consecuencia inevitable de ser una Parte contratada, y no algo que las Partes contratadas acuerden hacer en nombre de la ICANN. (2.10)

Análisis fáctico detallado de las actividades de procesamiento técnico

- El umbral fáctico para convertirse en responsable del tratamiento (determinar los propósitos o medios de procesamiento) es bajo. La prueba, según el TJUE, es simplemente si alguien "ejerce influencia sobre el procesamiento de los datos personales, para sus propios fines, y (...) participa, en consecuencia, en la determinación de los fines y medios de ese procesamiento". (2.12)

- En el fallo del caso Jehovan Todistajat del Tribunal de Justicia de la Unión Europea (TJUE), se declaró que la organización comunitaria nacional de los Testigos de Jehová tenía "conocimientos generales" y había fomentado y coordinado la recopilación de datos por parte de los miembros de la comunidad (predicadores puerta a puerta) a un nivel muy general, pero, no obstante, se consideró que había superado la prueba de responsabilidad conjunta del tratamiento con esos miembros de la comunidad. En el fallo del caso Fashion ID del TJUE, bastó con que el operador del sitio web se integrara con el código de la plataforma de Facebook, de modo que el operador participaba así en la determinación de los "medios" para la recopilación de datos de Facebook, y era un responsable conjunto del tratamiento con Facebook. (2.14)

- Por consiguiente, es probable que los tribunales y las autoridades de supervisión consideren que una Parte contratada participa en la determinación de los medios de procesamiento, posiblemente solo mediante la implementación/interacción con el SSAD. (2.14)

Factores que podrían apoyar el estatus de encargado del tratamiento

- La clave para evitar el estatus de responsable del tratamiento es poder demostrar que no está involucrado en la determinación de los "elementos esenciales" del procesamiento (2.6).

- Asimismo, la vigilancia por parte de la ICANN del cumplimiento de un requisito contractual de divulgación de datos podría ser una prueba de la relación entre el responsable y el encargado del tratamiento, dado que "la supervisión constante y cuidadosa por parte del responsable del tratamiento para garantizar el cumplimiento cabal del encargado del tratamiento con las instrucciones y los términos del contrato proporciona una indicación de que el responsable del tratamiento sigue teniendo el control total y exclusivo de las operaciones de procesamiento". (2.16)

- La adopción de medidas para informar claramente a los titulares de los datos que los datos se recopilan únicamente en nombre de la ICANN (por ejemplo, las divulgaciones en el proceso de registración de nombres de dominio, el recordatorio anual de la exactitud de los datos, los avisos de privacidad, los materiales del sitio web de la organización de la ICANN) y otras presentaciones que describan claramente que esta acción la realizan las Partes contratadas únicamente en nombre de la ICANN podrían dar lugar a que las personas tomen más conciencia de la función de la ICANN como

responsable del tratamiento y de la función de las Partes contratadas como encargados del tratamiento. (2.17)

Resumen: las Partes contratadas probablemente sean responsables conjuntos del tratamiento con la ICANN

- El resultado más probable y el punto de partida para las autoridades de supervisión es que las Partes contratadas sean responsables del tratamiento de datos. (2.18)
- El rol de la ICANN en la determinación del propósito y los medios de procesamiento sugiere que son responsables conjuntos del tratamiento con las Partes contratadas para la divulgación de datos a terceros. (2.18)

2. ¿Son suficientes las medidas de protección propuestas para lograr que la divulgación de los datos de registración cumpla con los requisitos?

Medidas de protección del SSAD

- Dada la cantidad de jurisdicciones involucradas y la probable variedad de solicitudes que podría atender el SSAD, esta opinión no pudo confirmar que las medidas de protección y los criterios descritos en los supuestos lograrían que la divulgación de datos en un sistema totalmente automatizado cumpliera con los requisitos. (3.8)
- B&B afirma que hay que tener cuidado en el procesamiento de los datos personales: un responsable del tratamiento (ya sea en incumplimiento de su contrato con el responsable del tratamiento o que se comporte de manera incompatible con las instrucciones del responsable del tratamiento) puede convertirse en un responsable del tratamiento en sí mismo y, por lo tanto, enfrentarse a sanciones (como se indica en la tabla de la pág. 7 del memorando). (3.6)
- Las medidas de protección descritas son útiles, pero deberán incluir las medidas adicionales que se describen a continuación. (3.8)
    - Fundamento jurídico: las medidas de protección tienen que: (i) considerar si las Partes contratadas, y no solo el Solicitante, tienen un fundamento jurídico para el procesamiento; (ii) tener en cuenta el marco jurídico particular aplicable a una Parte contratada; (iii) garantizar que se realice una prueba de equilibrio adecuada de los intereses legítimos, si es un fundamento jurídico apropiado en un caso determinado[153] (y puede que no sea seguro suponer que para una categoría de solicitudes el equilibrio de intereses esté siempre a favor de la divulgación; en determinados casos, como las investigaciones o los enjuiciamientos que podrían dar lugar a la pena capital, podrían ser

[153] Si la divulgación es una obligación legal conforme a las leyes de la UE o de los Estados miembros de la UE/EEE (incluidos los tratados en los que sea parte la UE o un Estado miembro pertinente), no es necesario considerar la prueba de intereses legítimos.

especialmente problemáticos); y (iv) garantizar que no se divulgarán tipos o volúmenes de datos indebidos a los solicitantes (por ejemplo, vigilancia basada en normas o bloqueo de solicitudes de tamaños inusuales, sistemas de permisos). (3.9 – 3.12)

- Derechos individuales: abordar la forma en que se tramitan las solicitudes de los titular de los datos, incluidos: (i) los derechos de acceso a los registros de solicitudes (que a su vez pueden ser datos personales de alto riesgo o incluso de "categoría especial"); (ii) el período de tiempo apropiado para la retención de esos registros; (iii) la forma en que se proporciona la información a los titular de los datos; (iv) la forma de abordar las situaciones en que el Solicitante insiste en no proporcionar información al titular de los datos (por ejemplo, confidencialidad del cumplimiento de la ley); y (v) las solicitudes para restringir o bloquear el procesamiento. (3.13 – 3.16)
- Transferencia de datos: para las transferencias internacionales de datos, el EPDP prevé recurrir al mecanismo de protección jurídica de las Cláusulas Contractuales Estándar (CCE) de la UE; sin embargo: (i) algunos Solicitantes, incluidas las autoridades públicas, no aceptarán sus condiciones; (ii) no es fácil cumplir las condiciones de las CCE, especialmente a gran escala; (iii) si las Partes contratadas del EEE son encargados del tratamiento, no pueden ampararse directamente en las CCE para transferir datos a la organización de la ICANN o a los Solicitantes fuera del EEE, por lo que habría que encontrar una solución alternativa. (3.17)
- Seguridad: las medidas de protección deberían ser proporcionales al riesgo para los titulares de los datos en caso de que sus datos se vean comprometidos. (3.18)

3. ¿Cuál es el riesgo de responsabilidad de las Partes contratadas por la divulgación?

- Si las medidas de protección son inadecuadas o son objeto de uso indebido/elusión por parte de los Solicitantes (o se contravienen otros aspectos del GDPR, por ejemplo, una notificación inadecuada o la falta de un fundamento jurídico para el procesamiento), las Partes contratadas podrían enfrentarse a investigaciones, órdenes de cumplimiento (por ejemplo, prohibiciones de procesamiento), y (financieramente) tanto a la responsabilidad ante las personas (civil) como a la responsabilidad ante las autoridades supervisoras (multas).
- A grandes rasgos, B&B expresa en las partes pertinentes que: (1) si las partes son responsables conjuntos del tratamiento, esto no significa que cada una de ellas tenga que asumir todos los elementos de cumplimiento, (2) si las Partes contratadas son encargados del tratamiento, solo serán responsables ante las personas (responsabilidad civil) en virtud del artículo 82 si han incumplido las obligaciones impuestas a los encargados del procesamiento en virtud del Reglamento, o han actuado por fuera o de

forma contraria a las instrucciones lícitas del responsable del tratamiento, (3) incluso cuando las partes son consideradas responsables conjuntos del tratamiento, en recientes decisiones judiciales (relativas al cumplimiento por parte de las autoridades supervisoras) se ha hecho hincapié en que la responsabilidad conjunta no implica una responsabilidad igual por las infracciones del GDPR, y (4) las Partes contratadas, como responsables conjuntos del tratamiento con la organización de la ICANN, se beneficiarían de una clara asignación de responsabilidades en virtud de los términos del "acuerdo" de responsabilidad conjunta que deben firmar conforme al Art. 26 del GDPR.

Responsabilidad ante las personas

- El Artículo 82 del GDPR establece las normas sobre la responsabilidad ante las personas. (4.2)
- Los responsables del tratamiento son susceptibles de responsabilidad por los daños y perjuicios causados por el procesamiento que infrinja el GDPR. Los encargados del tratamiento son susceptibles de responsabilidad por los daños y perjuicios causados por el procesamiento cuando no hayan cumplido con los requisitos específicos del encargado del procesamiento o cuando hayan actuado por fuera o de forma contraria a las instrucciones del responsable del tratamiento. (4.2)
- Un responsable o encargado del tratamiento no es susceptible de responsabilidad si demuestra que no fue en absoluto responsable del evento que provocó los daños. (4.2)
- Cuando varios responsables o encargados del tratamiento participan en el mismo proceso, cada entidad es susceptible de responsabilidad por la totalidad de los daños y perjuicios (responsabilidad conjunta y solidaria) ante las personas (4.2, 4.3)
- Si las Partes contratadas son encargadas del tratamiento, solo serán susceptibles de responsabilidad si no cumplen las obligaciones específicas de los encargados del tratamiento conforme al GDPR, o si actúan por fuera o de forma contraria a las instrucciones del responsable del tratamiento. En ese caso, es poco probable que las Partes contratadas infrinjan las instrucciones del responsable del tratamiento porque el SSAD está automatizado; por consiguiente, la fuente más probable de responsabilidad para ellas, por lo tanto, sería por tener medidas de seguridad inadecuadas o por no cumplir las normas del GDPR sobre las transferencias internacionales de datos. Las Partes contratadas podrían recurrir a la organización de la ICANN para que prescriba acuerdos de seguridad y de transferencia internacional que permitan a las Partes contratadas argumentar que "no tienen responsabilidad alguna por el hecho que provoca los daños". (4.4)
- Si las Partes contratadas son responsables del tratamiento, y si la divulgación infringe el GDPR, es poco probable que eviten la responsabilidad ante las personas si no pueden demostrar que "no tienen responsabilidad alguna por el hecho que provoca los daños",

si participan activamente en el evento de divulgación.

- Cualquier responsabilidad genera la posibilidad de que las Partes contratadas sean susceptibles de responsabilidad por todos los daños y perjuicios causados al titular de los datos. Este riesgo es mayor en un escenario de responsables conjuntos del tratamiento. (4.5, 4.6).
- Las Partes contratadas que se consideren responsables de la totalidad de los daños y perjuicios causados a un titular de los datos pueden solicitar contribuciones apropiadas de otras partes responsables. (4.7)
- En su calidad de responsables del tratamiento de datos, las Partes contratadas y la ICANN tendrían la obligación positiva de hacer frente al riesgo de que los Solicitantes procuren un acceso indebido a los datos personales. Las medidas de protección deben ser adecuadas al nivel de riesgo. Si un Solicitante elude las medidas de protección del SSAD, los tribunales podrían aceptar que las medidas de protección eran adecuadas, lo que limitaría la responsabilidad primaria de las Partes contratadas. (4,9; 4,10)
- Incluso en el caso de un incumplimiento del GDPR causado por un Solicitante, las Partes contratadas, la ICANN y el Solicitante pueden considerarse "involucrados en el mismo procesamiento", siendo cada parte responsable conjunta y solidariamente de los daños y perjuicios derivados de ese incumplimiento. Las Partes contratadas y la ICANN pueden argumentar que "no tienen responsabilidad alguna por el hecho que provoca los daños", pero que, de otro modo, tendrían que procurar la indemnización por parte del Solicitante o unirse al Solicitante en el procedimiento inicial para repartir los daños y perjuicios. (4.11)

Responsabilidad ante las autoridades de supervisión

- Las autoridades de supervisión pueden proceder contra los responsables y encargados del tratamiento de datos. (4.12)
- No está claro si la responsabilidad conjunta y solidaria se aplica cuando intervienen varias partes en el procesamiento (es decir, podría decirse que la acción coercitiva no es apropiada si otros son responsables). (4.13)
- Es necesario que haya una redacción clara en una ley para imponer la responsabilidad conjunta y solidaria, lo que refuerza el argumento de que esto se habría declarado expresamente si se hubiera previsto con respecto a las multas de las autoridades de supervisión. El Art. 83(2)(d) deja claro que la responsabilidad conjunta/solidaria no se aplica a las autoridades de supervisión. (4.13.2)
- Incluso cuando las partes son responsables conjuntos del tratamiento, las recientes decisiones judiciales (relativas al cumplimiento por parte de las autoridades supervisoras) hacen hincapié en que la responsabilidad conjunta no implica una responsabilidad igual en las infracciones del GDPR. (4.13.4)

- Por lo tanto, las partes contratadas y la ICANN se beneficiarían de responsabilidades claramente asignadas en virtud de un acuerdo de responsabilidad conjunta del tratamiento (y dicho acuerdo, en cualquier caso, es obligatorio en todas las situaciones de responsabilidad conjunta del tratamiento, conforme al Art. 26 del GDPR). (4.14)
- Tal vez sea posible aprovechar las disposiciones de la "autoridad principal" (también conocida como "ventanilla única" o "consistencia") del GDPR para garantizar que toda medida coercitiva se lleve a cabo a través del establecimiento en Bruselas de la organización de la ICANN, en lugar de contra las Partes contratadas. Este mecanismo solo está disponible cuando hay un procesamiento transfronterizo de datos personales (entidades en múltiples Estados miembros del EEE, o efectos sobre titulares de los datos en múltiples Estados miembros del EEE). (4.15 – 4.17)
- Las disposiciones de la "autoridad principal" en el GDPR no se refieren específicamente a la responsabilidad conjunta del tratamiento, pero las pautas sugieren que si la organización de la ICANN y las Partes contratadas designaran el establecimiento de Bélgica de la ICANN como establecimiento principal para el procesamiento (es decir, donde se adoptan las decisiones relativas al procesamiento), se podría reducir al mínimo el riesgo de las medidas coercitivas directamente contra las Partes contratadas. Este es un enfoque novedoso y no probado. (4.15 – 4.20)

Anexo:
Preguntas legales 1 y 2: Responsabilidad, medidas de protección, responsable y encargado del tratamiento

Mientras el Equipo responsable del EPDP deliberaba sobre la arquitectura de un SSAD, surgieron varias preguntas con respecto a la responsabilidad y las medidas de protección. En respuesta, el Comité Jurídico de la Fase 2 formuló las siguientes preguntas a los asesores jurídicos externos:

1. Si consideramos un Sistema Estandarizado de Acceso/Divulgación donde:
   - o las partes contratadas "CP" están obligadas contractualmente por la ICANN a revelar los datos de registración, incluidos los datos personales,
   - o los datos deben ser divulgados a través del RDAP a los Solicitantes, ya sea directamente o a través de un organismo intermediario de acreditación/autorización de solicitudes,
   - o la acreditación la lleva a cabo un tercero encargado por la ICANN sin la participación de las Partes contratadas,
   - o la divulgación se realiza de forma automatizada sin ninguna intervención manual,

- se informa debidamente a los titulares de los datos, de conformidad con los requisitos contractuales de la ICANN, sobre los fines para los que se pueden procesar los datos personales y los tipos de entidades que pueden hacerlo. El contrato de las Partes contratadas con la ICANN también exige que las mismas notifiquen al titular de los datos sobre esta posible divulgación y procesamiento de terceros antes de que el titular de los datos firme el acuerdo de registro con las Partes contratadas, y nuevamente cada año a través del recordatorio de exactitud de los datos de registración que exige la ICANN. Las Partes contratadas lo han hecho.

Además, suponer que se han establecido las siguientes medidas de protección

- La ICANN, o quien esta designe, ha validado/verificado la identidad del Solicitante, y ha requerido en cada caso que el Solicitante:
  - demuestre que tiene un fundamento jurídico para solicitar y procesar los datos,
  - proporcione su fundamento jurídico,
  - demuestre que está solicitando únicamente los datos necesarios para su propósito,
  - acuerde procesar los datos de conformidad con el GDPR, y
  - acepte las cláusulas contractuales estándar de la UE para la transferencia de datos.
- La ICANN, o quien esta designe, registra las solicitudes de datos de registración sin carácter público, audita estos registros de forma periódica, toma medidas de cumplimiento contra los presuntos usos indebidos y pone estos registros a disposición del titular de los datos cuando así lo solicite.

a. ¿Qué riesgo o responsabilidad, si los hubiere, enfrentarían las Partes contratadas por la actividad de procesamiento de la divulgación en este contexto, incluido el riesgo de que un tercero haga un uso indebido o eluda las medidas de protección?

b. ¿Considerarían que los criterios y medidas de protección descritos anteriormente son suficientes para lograr que la divulgación de los datos de registración cumpla con los requisitos? Si existe algún riesgo, ¿qué medidas de protección mejoradas o adicionales eliminarían1541 este riesgo?

[154] "En este sentido, cabe destacar el rol especial que pueden desempeñar las medidas de protección en la reducción de las repercusiones indebidas en los titulares de los datos y, por consiguiente, en la modificación del equilibrio de derechos e intereses en la medida en que no se invaliden los intereses legítimos del responsable del tratamiento de datos." https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf

c. En este escenario, ¿la Parte contratada se consideraría responsable del tratamiento de datos o encargada del tratamiento1552, y hasta qué punto, en caso de que así sea, se ve afectada la responsabilidad de la Parte contratada por esta distinción entre responsable y encargada del tratamiento?

d. Responder únicamente si aún existe un riesgo para la Parte contratada: Si todavía existe un riesgo para las Partes contratadas, ¿qué medidas de protección adicionales podrían ser necesarias para eliminar la responsabilidad de las Partes contratadas en función de la naturaleza de la solicitud de divulgación, es decir, en función de si los datos son solicitados, por ejemplo, por agentes privados que interponen demandas civiles o por autoridades encargadas del cumplimiento de la ley en función de su jurisdicción o de la naturaleza del delito (falta o delito grave) o de las sanciones asociadas (multa, prisión o pena capital)?

2. En qué medida, si procede, son responsables las partes contratadas cuando un tercero, que accede a datos de WHOIS sin carácter público en el marco de un plan de acreditación mediante el cual el acceso está acreditado para el propósito declarado, se compromete a respetar ciertas medidas de protección razonables similares a un código de conducta en relación con el uso de los datos, pero tergiversa sus propósitos previstos para el procesamiento de esos datos y posteriormente los procesa de manera incongruente con el propósito declarado. En dichas circunstancias, si existe la posibilidad de responsabilidad para las partes contratadas, ¿existen medidas que puedan adoptarse para mitigar o reducir el riesgo de responsabilidad para las partes contratadas?

[155] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

Pregunta 3

Resumen Ejecutivo:

El equipo responsable de la Fase 2 del EPDP envió su primer grupo de preguntas a Bird & Bird el 29 de agosto de 2019. Bird & Bird respondió a este grupo de preguntas en una serie de tres memorandos. El Memorando 2 se entregó el 10 de septiembre de 2019 y en él se analizaron preguntas relacionadas con la forma en que la "prueba de equilibrio" de intereses legítimos que se exige conforme al Artículo 6.1.(f) del GDPR podría aplicarse en un SSAD, ya sea de forma muy automatizada (Pregunta A) o, si no es posible automatizar esa decisión, la forma en que debería realizarse la prueba de equilibrio (Pregunta B). Las preguntas completas se proporcionan en el Anexo A de este resumen e incluyen una serie de supuestos que forman parte de la base fáctica de las respuestas que figuran a continuación.

En respuesta a la Pregunta A, Bird & Bird señaló lo siguiente con respecto a la automatización:

1. El proceso altamente automatizado descrito por el Equipo responsable del EPDP podría equivaler a una toma de decisiones exclusivamente automatizada que tuviera un efecto jurídico o similarmente significativo en los titulares de los datos (los "titulares de los datos" serían aquí los destinatarios de las solicitudes de datos de gTLD sin carácter público).
2. En general, esto no está permitido a menos que una de los fundamentos jurídicos limitados/exenciones en virtud del Art. 22(1) justifique la divulgación. Esto es mucho más acotado que el Art. 6.1.(f) del GDPR. Sería difícil para el SSAD, tal como se ha propuesto, cumplir con el Art. 22(1) del GDPR; por lo tanto, el SSAD debe estructurarse de manera que no entre en el ámbito del Artículo 22 en primer lugar.
3. Para lograrlo, sería necesario limitar el acceso/divulgación automática a situaciones en que no se produzcan "efectos jurídicos o de importancia similar" para el titular de los datos. Entre los ejemplos proporcionados en el memorando cabe citar la divulgación de los datos de contacto de los administradores de los registratarios que sean personas no físicas en respuesta a los ataques de malware o a la infracción de la propiedad intelectual. El proceso de tramitación de las solicitudes de mayor riesgo no debería estar totalmente automatizado; debería haber alguna participación humana significativa (por lo menos, supervisión).
4. De forma alternativa, el SSAD podría estructurarse de manera que no tome una decisión basada en su procesamiento automático de datos personales relativos a los destinatarios de una solicitud. Por ejemplo, el SSAD podría publicar las categorías de solicitudes que serán aceptadas y pedir a los solicitantes que confirmen que cumplen los criterios pertinentes. En cambio, si se exige al *Solicitante* que realice el análisis necesario y que luego certifique el resultado ante el SSAD, se podría argumentar que el SSAD no tomaría una decisión (de revelar datos) basada en su propio procesamiento automatizado de datos personales, por lo tanto, el Art. 22 del GDPR no se aplicaría. Sin

embargo, confiar en la autocertificación de los Solicitantes tal vez genere un margen para el uso indebido del sistema por parte de los Solicitantes, lo cual (como se ha explicado en respuestas anteriores) podría significar la responsabilidad para la ICANN y las Partes contratadas.

5. En lo que respecta a la autenticación del Solicitante (como paso distinto de la evaluación de los motivos u otros parámetros de una solicitud), Bird & Bird cree que ciertamente sería posible automatizar el proceso para autenticar a la persona que realiza la solicitud. También puede ser posible automatizar otros aspectos del proceso de solicitud.

En respuesta a la Pregunta B, Bird & Bird:

1. Estableció la guía oficial de la UE (WP29) sobre cómo debería llevarse a cabo la prueba de equilibrio de intereses legítimos del el Art. 6.1.(f).
2. Señaló que si la ICANN y las Partes contratadas son responsables conjuntos del tratamiento, ambos deben establecer un interés legítimo en el procesamiento. En lo que respecta a las Partes contratadas, es probable que el interés pertinente sea el del tercero, el Solicitante. La ICANN, en cambio, puede establecer su interés en la seguridad, estabilidad y resiliencia del sistema de nombres de dominio, *así como* el interés del tercero solicitante; y
3. Proporcionó un debate de alto nivel sobre las medidas de protección que podrían desplegarse para inclinar aún más la balanza a favor del procesamiento previsto como parte del SSAD.

1. Pregunta A

En la pregunta A, se pregunta si el Art. 6.1.(f) del GDPR (el fundamento jurídico de los "intereses legítimos" para el procesamiento) permitiría al SSAD procesar automáticamente las solicitudes (al menos en determinadas categorías predefinidas), sin requerir la (i) verificación manual, solicitud por solicitud de que la solicitud cumple los criterios pertinentes para su divulgación; y (ii) la divulgación de los datos de registración pertinentes.

El SSAD podría entrar dentro el ámbito del Art. 22 del GDPR, en lugar de estar exclusivamente relacionado con el Art. 6.1.(f) del GDPR

- El Art. 6.1.(f) del GDPR permite el procesamiento automatizado a menos que ello equivalga a una "toma de decisiones individual automatizada" que tenga efectos jurídicos o de importancia similar para el titular de los datos ("toma de decisiones únicamente automatizada"), lo cual generalmente no se permite a menos que uno de los fundamentos jurídicos/exenciones más limitados previstos en el Art. 22.1 del GDPR justificara la divulgación.

- Si bien el Articulo 22 del GDPR establece que el titular de los datos tiene "derecho a no estar sujeto a" dicha decisión, en la práctica, el Artículo 22 ha sido interpretado por los

reguladores como una prohibición general (es decir, no es necesario que el titular de los datos se oponga a dicha decisión).

- El proceso descrito por el Equipo responsable del EPDP podría equivaler a esa toma de decisiones automatizada que afecta al destinatario de una solicitud (por ejemplo, cuando los organismos encargados de la aplicación de la ley quieren entablar un proceso contra personas que dirigen sitios web ilícitos).

- Si el Art. 22 se aplica al procesamiento descrito por el EPDP, es decir, **si el procesamiento del SSAD equivale a una decisión individual automatizada con efectos jurídicos o de importancia similar, no se permitiría en virtud del Art. 6.1.(f) del GDPR (base de los "intereses legítimos" para el procesamiento).** El Art. 22(1) establece su propio conjunto, más limitado, de motivos en los que se puede basar la toma de decisiones del Art. 22.

- B&B informa que **será difícil para el SSAD cumplir con las exenciones en el Art. 22(1); por lo tanto, el EPDP debería garantizar que el procesamiento del SSAD no entre en el ámbito de aplicación del Art. 22.**

Estrategia de mitigación 1: evitar decisiones si pueden tener "efectos jurídicos o de importancia similar" para personas cuyos datos se divulgan.

- Una forma de lograrlo podría ser limitando el acceso y la divulgación automáticos a situaciones en las que no se produzcan "efectos jurídicos o de importancia similar" para el titular de los datos.

- Una decisión de divulgar datos a través del SSAD no tendría en sí misma un "efecto jurídico" sobre el titular de los datos. La prueba más relevante para el SSAD son los "efectos de importancia similar". Esto significa algo similar a tener un efecto jurídico, algo digno de atención (por ejemplo, afectar significativamente las circunstancias, el comportamiento o las elecciones de las personas afectadas).[156]

- Tal vez sea posible determinar categorías de solicitudes que no tengan un efecto "jurídico o de importancia similar" en la persona, como la divulgación de los datos de contacto de los administradores para los registratarios no físicos (empresa/organización/institución). Es mucho más probable que otras divulgaciones relacionadas con los datos de registración de una persona física tengan un "efecto significativo similar". Habría que tener mucho cuidado con ese análisis.

- Para las decisiones que tienen más probabilidades de tener un "efecto significativo", serían necesarias una revisión o supervisión humanas. La participación humana "simbólica" no sería suficiente. Para que el elemento de revisión humana cuente, el

[156] Según las directrices oficiales, los siguientes son ejemplos clásicos de decisiones que podrían ser suficientemente significativas: (i) decisiones que afectan la situación financiera de una persona; (ii) decisiones que afectan el acceso a los servicios de salud; (iii) decisiones que deniegan oportunidades de empleo o ponen a alguien en grave desventaja; iv) decisiones que afectan el acceso de una persona a la educación.

responsable del tratamiento debe asegurar una supervisión significativa por parte de alguien que tenga la autoridad y la competencia para cambiar la decisión.

Estrategia de mitigación 2: Evitar los diseños del SSAD que impliquen el procesamiento de datos personales sobre el destinatario de una solicitud a fin de decidir si se cumple la solicitud

- También puede ser posible estructurar el SSAD de manera que no implique "una decisión basada únicamente en el procesamiento automatizado". El artículo 22 del GDPR exige que la decisión se base en el procesamiento *de datos personales*. Si las decisiones se basan en algo que no sean datos personales, no se aplica el Artículo 22 del GDPR.

- Por consiguiente, en lugar de que el SSAD solicite detalles a los solicitantes (por ejemplo, información sobre el destinatario de la solicitud, por ejemplo, el registratario, y por qué se requieren sus datos), y luego analice esa información (automáticamente) a fin de evaluar si se cumplen los criterios pertinentes para la divulgación de datos de registración sin carácter público, el SSAD podría en cambio publicar las categorías de solicitudes que se aceptarán y pedir a los solicitantes que confirmen que cumplen los criterios pertinentes. En este caso, el SSAD no procesaría *datos personales* sobre el objetivo de la solicitud, a fin de adoptar una decisión sobre la divulgación de los datos, por lo tanto, no se aplicaría el Artículo 22.

- Como se ha señalado en relación con preguntas anteriores, las partes que participan en el SSAD tienen la responsabilidad de adoptar "medidas técnicas y organizativas apropiadas" para protegerse contra el riesgo de que los Solicitantes hagan un uso indebido del sistema SSAD.

- Por lo tanto, toda decisión de basarse en la autocertificación, en lugar de evaluar las solicitudes, tendría que equilibrarse cuidadosamente con estas obligaciones de mitigación de riesgos; esto probablemente reduciría las ocasiones en que podría utilizarse este enfoque de autodeclaración. Bird & Bird señala que, conforme a dicho plan, el SSAD podría seguir pidiendo a los Solicitantes que proporcionen información adicional sobre la naturaleza de su solicitud *con fines de auditoría*, pero no se utilizaría para evaluar la solicitud en sí (es decir, no se utilizaría para la adopción de decisiones automatizadas).

2. Pregunta B

En esta pregunta, **el Equipo responsable del EPDP solicita orientación sobre cómo realizar la prueba de equilibrio en virtud del Artículo 6.1.(f) (suponiendo que no sea posible automatizar los pasos descritos).**

- La orientación oficial es que la prueba de equilibrio debería dividirse en cuatro pasos:

    1. Evaluar el interés que se cumple con el procesamiento

2. Considerar el impacto en el titular de los datos
3. Realizar una prueba de equilibrio provisional
4. Considerar el impacto de cualquier medida de protección adicional desplegada para prevenir cualquier impacto indebido en el titular de los datos.

1. Evaluación del interés legítimo del responsable del tratamiento

- El Artículo 6.1.(f) indica que puede procesarse lícitamente si es "necesario a los efectos de los intereses legítimos perseguidos por el responsable del tratamiento o un tercero".
- Existen tres subelementos para esto: i) la legitimidad; ii) la existencia de un interés; y iii) la necesidad.

Legitimidad

- Parece que la "legitimidad" no es una prueba alta. El WP29 indicó que "un interés puede ser considerado como legítimo siempre y cuando el responsable del tratamiento pueda perseguir este interés de una manera que esté de acuerdo con la protección de datos y otras leyes".

Establecimiento del "interés" en el procesamiento

- B&B señala que si la ICANN y las Partes contratadas son responsables conjuntos del tratamiento, ambos deben establecer un interés legítimo en el procesamiento. En lo que respecta a las Partes contratadas, es probable que el interés pertinente sea el del tercero, el solicitante. La ICANN, en cambio, puede establecer su interés en la seguridad, estabilidad y resiliencia del sistema de nombres de dominio, así como el interés del tercero solicitante.
- "Interés" no es lo mismo que "propósito".
    - "Propósito" es la razón específica por la que se procesan los datos
    - "Interés" es el interés más amplio que un responsable del tratamiento puede tener en el procesamiento, o el beneficio que el responsable del tratamiento obtiene, o que la sociedad puede derivar del procesamiento. (Esto significa también que los intereses podrían ser públicos o privados; por ejemplo, en el caso de las acciones para impedir la infracción en materia de marcas comerciales, podría haber un interés privado para la persona cuya marca se ha infringido y un interés público más amplio en impedir el riesgo de confusión por parte del público. Este factor podría ser útil en la documentación de la prueba de equilibrio).
- El interés debe ser "real y específico", no "vago y especulativo".

- En la página 25, el WP217 ofrece una lista no exhaustiva de contextos en los que pueden surgir intereses legítimos, entre otros:
    - "Ejercicio del derecho a la libertad de expresión o de información, incluso en los medios de comunicación y las artes"
    - Ejecución de demandas judiciales
    - Prevención del fraude, usos indebidos de los servicios
    - Seguridad física, TI y seguridad de la red
    - Procesamiento para fines de investigación
- El EPDP sugiere que las posibles medidas de protección del SSAD podrían incluir el requisito de que el solicitante declare que tiene un fundamento jurídico para realizar la solicitud y que puede "proporcionar su fundamento jurídico". Sin embargo, cuando los datos se divulguen conforme al Art. 6.1.(f), sería más útil que el solicitante confirmara su *interés* en recibir los datos personales.

Necesidad

- Con respecto a la necesidad, B&B aconseja que el procesamiento (divulgación) propuesto debe ser "necesario" para este interés.
    - El caso Oesterreichischer Rundfunk del TJUE define esto como: *"...el adjetivo 'necesario'... implica que se trata de una 'necesidad social apremiante' y que la medida empleada es 'proporcional al objetivo legítimo que se persigue'."*
    - Un Tribunal de Apelaciones del Reino Unido también sugiere que el término "necesario" significa "más que deseable pero menos que indispensable o absolutamente necesario".
- B&B sugiere que un factor relevante a considerar para la necesidad podría ser si un solicitante ha tratado de ponerse en contacto con la persona de alguna otra manera (aunque esto puede ser inapropiado en el caso de las solicitudes de los organismos de cumplimiento de la ley).
- B&B señala que el SSAD propone pedir a los solicitantes que confirmen que solicitan únicamente los datos necesarios para su propósito.

2. Evaluación del impacto en las personas

- B&B afirma que el EDPB sugiere una serie de factores a considerar cuando se evalúa el impacto en las personas:

- ***Evaluación del impacto.*** Considerar el impacto directo en los titulares de los datos así como las posibles consecuencias más amplias del procesamiento de datos (por ejemplo, accionando procedimientos legales).
- ***Naturaleza de los datos.*** Considerar el nivel de sensibilidad de los datos así como si los datos ya están disponibles de forma pública.
- ***Estatus del titular de los datos***. Considerar si el estatus del titular de los datos aumenta su vulnerabilidad (por ejemplo, niños, otras clases protegidas)
- ***Alcance del procesamiento.*** Considerar si los datos se mantendrán estrictamente cerrados (riesgo menor) o si se divulgarán públicamente, si se pondrán a disposición de una gran cantidad de personas, o si se combinarán con otros datos (riesgo mayor).
- ***Expectativas razonables del titular de los datos***. Considerar si el titular de los datos esperaría razonablemente que su datos se procesen/divulguen de esta manera.
- ***Estatus del responsable del tratamiento y del titular de los datos.*** Considerar el poder de negociación y cualquier desequilibrio de autoridad entre el responsable del tratamiento y el titular de los datos.

- Tal vez sea posible que el SSAD tenga en cuenta estos factores, mediante la identificación de las solicitudes que supondrían un alto riesgo para las personas, a fin de que esas solicitudes reciban una atención adicional.
- Para evaluar el riesgo se puede utilizar una metodología de riesgo clásica (que considere la gravedad y la probabilidad).
- No se trata de un ejercicio puramente cuantitativo; si bien la métrica de una solicitud (por ejemplo, el número de personas afectadas) es pertinente, no es determinante: se debe seguir considerando un impacto potencialmente significativo en un solo titular de los datos.

3. Balance provisional

- Una vez que se hayan considerado los intereses legítimos del responsable del tratamiento o de un tercero y los de la persona, se puede hacer un balance de los mismos. Asegurar el cumplimiento de otras obligaciones de protección de datos ayuda con el balance, pero no es determinante (por ejemplo, el hecho de que el SSAD asegure la existencia de cláusulas contractuales estándar con los solicitantes en relación con la protección adecuada de los datos es útil, porque tal vez reduce el riesgo para las personas, pero no es determinante).

4. Medidas de protección adicionales

- B&B informa que si no está claro cómo debe lograrse el equilibrio, el responsable del tratamiento puede considerar la posibilidad de adoptar medidas de protección adicionales para reducir el impacto del procesamiento en los titulares de los datos.
- Entre ellas figuran, por ejemplo:
    - Transparencia
    - Fortalecimiento de los derechos de los titulares al acceso o portabilidad de los datos
    - Derecho incondicional a no participar
- En el documento WP217, págs. 41 y 42, se proporcionan más detalles sobre las medidas de protección que pueden contribuir a "inclinar la balanza" a favor del procesamiento (en este caso, a favor de las divulgaciones), en la prueba de equilibrio de los intereses legítimos.

Anexo: Pregunta legal 3: intereses legítimos y presentaciones y/o divulgaciones automatizadas

a) Suponiendo que exista una política que permita a las partes acreditadas acceder a los datos de WHOIS sin carácter público a través de un Sistema Estandarizado de Acceso/Divulgación de datos de registración de dominios sin carácter público para terceros ("SSAD") (y que requiera que la parte acreditada se comprometa a ciertas medidas de protección razonables similares a un código de conducta), ¿está legalmente permitido, en virtud del Artículo 6.1.(f), realizar lo siguiente?:

- Definir categorías específicas de solicitudes de partes acreditadas (por ejemplo, respuesta rápida a un ataque de malware o contactar a un infractor de propiedad intelectual que no responda), para las cuales pueda haber presentaciones automáticas de datos de WHOIS sin carácter público, sin tener que verificar manualmente las calificaciones de las partes acreditadas para cada solicitud de divulgación individual.

- Permitir divulgaciones automatizadas de dichos datos, sin que sea necesaria una revisión manual por parte del responsable o encargado del tratamiento de datos de cada solicitud de divulgación individual.

b) Además, si no es posible automatizar ninguno de estos pasos, por favor proporcionar cualquier orientación sobre cómo realizar la prueba de equilibrio en virtud del Artículo 6.1.(f).

A modo de referencia, consulte las siguientes medidas de protección posibles:

- La divulgación es requerida en virtud del contrato de las Partes contratadas con la ICANN (como resultado de la política de la Fase 2 del EPDP).
- El contrato de las Partes contratadas con la ICANN exige que la Parte contratada notifique al titular de los datos los fines para los que se pueden procesar los datos personales y los tipos de entidades que pueden hacerlo. La Parte contratada debe notificar al titular de los datos sobre esta oportunidad de optar por no hacerlo antes de que el titular de los datos firme el acuerdo de registro con la Parte contratada, y nuevamente cada año a través del recordatorio de exactitud de los datos de registración que exige la ICANN. Las Partes contratadas lo han hecho.
- La ICANN, o quien esta designe, ha validado la identidad del Solicitante, y ha requerido que el Solicitante:
  - demuestre que tiene un fundamento jurídico para solicitar y procesar los datos,
  - proporcione su fundamento jurídico,
  - demuestre que está solicitando únicamente los datos necesarios para su propósito,

  - acuerde procesar los datos de conformidad con el GDPR, y
  - acepte las cláusulas contractuales estándar para la transferencia de datos.
- La ICANN, o quien esta designe, registra las solicitudes de datos de registración sin carácter público, audita estos registros de forma periódica, toma medidas de cumplimiento contra los presuntos usos indebidos y pone estos registros a disposición del titular de los datos cuando así lo solicite.

Pregunta 4

Resumen Ejecutivo:

El equipo responsable de la Fase 2 del EPDP envió su primer grupo de preguntas a Bird & Bird el 29 de agosto de 2019. Bird & Bird respondió a este grupo de preguntas en una serie de tres memorandos. El Memorando 3 se entregó el 9 de septiembre de 2019 y en el mismo se analizan las cuestiones relativas a los fundamentos jurídicos en virtud de los cuales los datos personales contenidos en los datos de registración de los gTLD podían divulgarse a las autoridades encargadas del cumplimiento de la ley fuera de la jurisdicción del responsable del tratamiento de datos.

Específicamente, el memorando responde a las siguientes preguntas:

- ¿Puede un responsable del tratamiento de datos ampararse en el Artículo 6.1.(c) del GDPR para divulgar datos personales a las autoridades encargadas del cumplimiento de la ley fuera de la jurisdicción del responsable del tratamiento de datos?
- Si no es así, puede el responsable del tratamiento de datos ampararse en cualquier otro fundamento jurídico, además del Art. 6.1.(f) para divulgar datos personales a las autoridades encargadas del cumplimiento de la ley fuera de la jurisdicción del responsable del tratamiento de datos?
- ¿Es posible para las autoridades de cumplimiento de la ley no pertenecientes a la UE ampararse en el Art. 6.1.(f) del GDPR como fundamento jurídico para su procesamiento? En este contexto, ¿puede el responsable del tratamiento de datos ampararse en el Art. 6.1.(f) del GDPR para divulgar los datos personales? Si las autoridades encargadas del cumplimiento de la ley no pertenecientes a la UE no pueden ampararse en el Art. 6.1.(f) del GDPR como base legal para su procesamiento, ¿en qué fundamento jurídico pueden ampararse las autoridades encargadas del cumplimiento de la ley no pertenecientes a la UE?

En general, Bird & Bird recomendó lo siguiente:

1. Para aplicar el Art. 6.1.(c) debe existir "el derecho de la Unión o el derecho de un Estado miembro al que esté sujeto el responsable del tratamiento" y, por lo tanto, este fundamento tiene una aplicación limitada cuando el organismo de cumplimiento de la ley se encuentra fuera de la jurisdicción del responsable del tratamiento.
2. Conforme a los seis fundamentos jurídicos para el procesamiento de datos personales, Artículos: 6.1.(a) - Consentimiento, 6.1.(b) - Contrato, 6.1.(d) - Intereses vitales de una persona, y 6.1.(e) - Interés público o autoridad oficial, probablemente no sean aplicables a las solicitudes de organismos de cumplimiento de la ley.
3. Art. 6.1.(f) - Interés legítimo, puede ser una base aplicable para el responsable del tratamiento cuando una autoridad encargada del cumplimiento de la ley no perteneciente a la UE solicite obtener datos personales de un responsable del tratamiento en la UE.
4. Si un organismo de cumplimiento de la ley se encuentra fuera del EEE, su fundamento jurídico para el procesamiento en virtud del GDPR no es relevante dado que no está sujeto al GDPR. Las organizaciones que divulguen a los organismos de cumplimiento de la ley fuera del EEE seguirán necesitando un fundamento válido para hacerlo, lo que normalmente será un interés legítimo en el caso de la ICANN.
5. Si la Parte contratada está sujeta al GDPR pero está ubicada fuera del EEE, también estará sujeta a la ley local. Esto significa que los responsables del tratamiento pueden enfrentarse a un conflicto de leyes.

1. ¿Puede un responsable del tratamiento de datos ampararse en el Artículo 6.1.(c) del GDPR para divulgar datos personales a las autoridades encargadas del cumplimiento de la ley fuera de la jurisdicción del responsable del tratamiento de datos?

- El procesamiento necesario para el cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento solo está disponible cuando la obligación legal está establecida en la legislación de la UE o del Estado miembro.

- Cuando el responsable del tratamiento está sujeto a obligaciones de divulgación que se derivan de leyes de jurisdicciones fuera de la UE, el responsable del tratamiento no puede ampararse en el Art. 6.1.(c).

- El responsable del tratamiento puede estar sujeto a la obligación legal en virtud de la legislación de la UE o de los Estados miembros para divulgar datos personales a una autoridad encargada del cumplimiento de la ley que no pertenezca a la UE.

- Los Tratados de Asistencia Legal Mutua (MLAT) pueden cubrir, pero cuando llega una solicitud donde exista un MLAT, el responsable del tratamiento debe denegar la solicitud y remitirse al MLAT. Cuando no exista un MLAT u otro acuerdo, el responsable del tratamiento debe asegurarse de que la divulgación a un tercer país no infrinja la legislación local.

2. ¿Puede el responsable del tratamiento de datos ampararse en cualquier otro fundamento jurídico, además del Artículo 6.1.(f) del GDPR, para divulgar datos personales a las autoridades encargadas del cumplimiento de la ley fuera de la jurisdicción del responsable del tratamiento de datos?

- Los Artículos 6.1.(f) y 6.1.(c) pueden aplicarse, pero es probable que los otros cinco fundamentos jurídicos para el procesamiento de datos personales no lo hagan.

- Cuando una autoridad encargada del cumplimiento de la ley de un país no perteneciente a la UE solicita obtener datos personales de un responsable del tratamiento en la Unión Europea, el responsable del tratamiento puede demostrar un interés legítimo (6.1.(f)) en la divulgación de los datos. El EDPB también ha sugerido este enfoque en su correspondencia con la ICANN (por ejemplo, EDPB-85-2018).

3. ¿Es posible para las autoridades de cumplimiento de la ley no pertenecientes a la UE ampararse en el Artículo 6.1.(f) del GDPR como fundamento jurídico para su procesamiento? En este contexto, ¿puede el responsable del tratamiento de datos ampararse en el Artículo 6.1.(f) del GDPR para divulgar los datos personales? Si las autoridades encargadas del cumplimiento de la ley no pertenecientes a la UE no pueden ampararse en el Artículo 6.1.(f) del GDPR como base legal para su procesamiento, ¿en qué fundamento jurídico pueden ampararse las autoridades encargadas del cumplimiento de la ley no pertenecientes a la UE?

- En su calidad de entidades de un país, las autoridades encargadas del cumplimiento de la ley están amparadas por la inmunidad del Estado y, por lo tanto, las autoridades encargadas del cumplimiento de la ley que no pertenezcan a la UE no están sujetas al GDPR.

- Incluso suponiendo que el GDPR pudiera aplicarse a las autoridades encargadas del cumplimiento de la ley no pertenecientes a la UE, parece poco probable que las autoridades encargadas del cumplimiento de la ley de fuera de la UE consideren la posibilidad de justificar su procesamiento en el marco del GDPR.

- Por lo tanto, las autoridades encargadas del cumplimiento de la ley no pertenecientes a la UE no necesitan evaluar en qué fundamento jurídico del GDPR ampararse para procesar los datos.

- No obstante, el responsable del tratamiento que transfiera datos a un organismo de cumplimiento de la ley que esté fuera de la UE tendrá que estudiar la forma de cumplir las obligaciones del Capítulo V (transferencias de datos personales a terceros países u organizaciones internacionales).

Pregunta 5 (Direcciones electrónicas seudonimizadas)

El grupo ha analizado la opción de sustituir la dirección de correo electrónico proporcionada por el interesado por una dirección de correo electrónico alternativa que de por sí no identificaría al interesado (Ejemplo: 'sfjgsdfsafgkas@pseudo.nym'). Con este enfoque, surgieron dos opciones en el debate, en las cuales: (a) se utilizaría la misma cadena de caracteres única para múltiples registraciones del titular de los datos ("seudonimización"), o (b) la cadena de caracteres sería única para cada registración ("anonimización"). Conforme a la opción (a), la identidad del interesado puede, aunque no necesariamente, ser identificable mediante la referencia cruzada del contenido de todas las registraciones de nombres de dominio para los que se utilice la cadena de caracteres.

De estas opciones, surgió la siguiente pregunta: En las opciones (a) y/o (b), ¿debería considerarse que la dirección alternativa es un dato personal del titular de los datos en el marco del GDPR y cuáles serían las consecuencias y riesgos jurídicos de esta determinación con respecto a la publicación propuesta de esta cadena de caracteres en la parte de acceso público del servicio de datos de registración (RDS)?

Respuesta resumida de Bird & Bird

Creemos que cualquiera de las dos opciones ((a) o (b)) seguiría siendo tratada como la publicación de datos personales en la web. Este parecería ser un caso cubierto por una declaración hecha en la Opinión de 2014 del Grupo de Trabajo del Artículo 29 sobre técnicas de anonimización [ec.europa.eu]: "cuando un responsable del tratamiento de datos no elimina los datos originales (identificables) a nivel de evento, y el responsable del tratamiento de datos entrega parte de este conjunto de datos (por ejemplo, después de eliminar o enmascarar los datos identificables), el conjunto de datos resultante sigue siendo datos personales". El propósito de poner a disposición esta dirección de correo electrónico, aunque esté enmascarada, es presumiblemente permitir que terceros se pongan en contacto directamente con el titular de los datos (por ejemplo, para entregarle citaciones judiciales, retiros por demandas, etc.), por lo que está claramente vinculada a ese titular de los datos en particular, al menos en lo que respecta a la ICANN/Partes contratadas. Sin embargo, cualquiera de las dos opciones sería vista como una valiosa tecnología de mejora de la privacidad (OPET) / medida de privacidad por diseño.

Pregunta 6 (Consentimiento)

Los datos de registración presentados por los registratarios que son personas jurídicas pueden contener los datos de personas físicas. En un memorando de la Fase 1 se estableció que los registradores pueden basarse en la autoidentificación de un registratario como persona jurídica o física si se mitiga el riesgo adoptando medidas adicionales para garantizar la exactitud de la designación del registratario. Como seguimiento de ese memorando: ¿cuáles son las opciones de consentimiento y los requisitos relacionados con dichas designaciones? Concretamente: ¿tienen derecho los responsables del tratamiento de datos a basarse en una declaración que obligue a los registratarios que son personas jurídicas a obtener el consentimiento de una persona física que actúe como contacto y cuya información pueda mostrarse públicamente en el RDS? En caso afirmativo, ¿qué declaraciones, de haberlas, serían útiles para que el responsable del tratamiento las obtenga del registratario que es una persona jurídica en este caso?

Como parte de su análisis, sírvase consultar las políticas y prácticas del GDPR del registro del protocolo de Internet (dirección IP) RIPE-NCC (el registro para Europa, con sede en los Países Bajos). Los clientes (registratarios) de RIPE-NCC son personas jurídicas que se exhiben públicamente en WHOIS. RIPE-NCC asigna la responsabilidad a sus registratario que son personas jurídicas de obtener el permiso de esas personas físicas, y establece procedimientos y medidas de protección para ello. RIPE-NCC establece justificaciones de la misión y propósitos de recolección de datos similares a los de la Especificación Temporaria de la ICANN. ¿Podrían utilizarse políticas y procedimientos similares en la ICANN?

Ver también las políticas de ARIN, el registro de direcciones IP para América del Norte. ARIN tiene algunos clientes ubicados en la UE. ARIN también publica los datos de las personas físicas en sus resultados de WHOIS. Los clientes de ARIN son personas físicas, que presentan los datos de los contactos de personas físicas.

Respuesta resumida de Bird & Bird

Este documento analiza los requisitos de consentimiento establecidos en el GDPR y examina las opciones de consentimientos a los efectos de la publicación en el RDS de los datos personales proporcionados en el contexto de la registración de registratarios que son personas jurídicas.

Requisitos de consentimiento

Conforme al GDPR, el consentimiento debe ser libre, específico, informado e inequívoco. Además, es necesario obtenerlo antes de que se lleve a cabo el procesamiento. Los responsables del tratamiento deben ser capaces de demostrar que se ha dado un consentimiento válido y las personas tienen derecho a retirarlo en cualquier momento. En virtud del GDPR, la obligación de obtener el consentimiento recae en el responsable del tratamiento. El responsable del tratamiento puede instruir a un tercero para que obtenga el

consentimiento de las personas en su nombre; sin embargo, el hecho de hacerlo no exime al responsable del tratamiento de sus obligaciones en virtud del GDPR.

Opciones de consentimiento

Sobre la base de los requisitos mencionados, en este documento se examinan las siguientes opciones de obtención del consentimiento para hacer públicos los datos personales en el RDS y se exponen las consideraciones de cumplimiento de cada una de ellas:

1. Los responsables del tratamiento solicitan el consentimiento válido directamente a las personas
    - Hacer públicos los datos personales en el RDS es opcional.
    - Antes de hacer públicos los datos personales, el responsable del tratamiento se pone en contacto directamente con las personas para solicitar el consentimiento de acuerdo con el GDPR.
    - En caso de denegación del consentimiento o falta de respuesta, los datos personales no se harán públicos.

2. El registratario obtiene un consentimiento válido y proporciona pruebas al responsable del tratamiento
    - Hacer públicos los datos personales en el RDS es opcional.
    - Antes de hacer públicos los datos personales, el responsable del tratamiento le exige al registratario que: (a) obtenga el consentimiento de las personas; y (b) proporcione pruebas al responsable del tratamiento que indiquen que se ha obtenido el consentimiento.
    - En caso de denegación del consentimiento o de no recibir pruebas, los datos personales no se harán públicos.

3. El registratario obtiene un consentimiento válido y el responsable del tratamiento lo confirma con la persona
    - Antes de hacer públicos los datos personales, el responsable del tratamiento le exige al registratario que: (a) obtenga el consentimiento de las personas; y (b) proporcione pruebas al responsable del tratamiento que indiquen que se ha obtenido el consentimiento.
    - El responsable del tratamiento hace un seguimiento de las personas directamente: les informa que el registratario ha confirmado que han otorgado su consentimiento.

4. El registratario asume la obligación de obtener el consentimiento
    - Los registratarios pueden proporcionar datos de contacto no personales.
    - Los datos de registración se hacen públicos de forma predeterminada (independientemente de que se incluyan o no datos personales).
    - Mediante una declaración, los registratarios se comprometen a asegurarse de que han obtenido el consentimiento de las personas si deciden proporcionar datos personales.

Pregunta 7 (Exactitud)

Pregunta 1a

¿Quién tiene derecho a invocar el Principio de exactitud? Entendemos que uno de los propósitos del Principio de exactitud es proteger al titular de los datos de los daños y perjuicios generados a raíz del procesamiento de información inexacta. ¿Tienen otros actores, como las partes contratadas y la ICANN (como responsables del tratamiento), los organismos de cumplimiento de la ley, los titulares de derechos de propiedad intelectual, etc., legitimación para invocar el Principio de exactitud en el marco del GDPR? Al responder a esta pregunta, ¿podrían por favor aclarar las partes/intereses que debemos considerar en general y, específicamente, al interpretar los siguientes pasajes de los memorandos anteriores?, a saber:

- En ambos memorandos se hace referencia a las "partes relevantes" en varias secciones. ¿Las "partes relevantes" se limitan al responsable (o responsables) del tratamiento de datos o deberíamos tener en cuenta también a los intereses de terceros?
    - "Puede haber dudas sobre si es suficiente que el RNH o el titular de la cuenta confirmen la exactitud de la información relativa a los contactos técnicos y administrativos, en lugar de solicitar información a dichos contactos directamente. El GDPR no requiere necesariamente que, en los casos en que los datos personales deban ser validados, lo haga el propio titular de los datos. La ICANN y las partes relevantes pueden recurrir a terceros para confirmar la exactitud de los datos personales si es razonable hacerlo. Por lo tanto, no vemos ningún motivo inmediato para concluir que los procedimientos actuales son insuficientes". (énfasis agregado) (Párrafo 19 - Exactitud)
    - “En resumen, debido a que el cumplimiento del Principio de Exactitud se basa en un estándar de razonabilidad, la ICANN y las partes relevantes estarán mejor situadas para evaluar si estos procedimientos son suficientes. Desde nuestro punto de vista, como los procedimientos requieren pasos afirmativos que ayudarán a confirmar la exactitud, a menos que haya razones para creer que son insuficientes, no vemos un requisito claro para revisarlos." (énfasis agregado) (Párrafo 21 - Exactitud)
    - "Si las partes relevantes no tuvieran motivos para dudar de la confiabilidad de la autoidentificación de un registratario, es probable que pudieran basarse únicamente en la autoidentificación, sin confirmación independiente. Sin embargo, comprendemos que las partes estén preocupadas por el hecho de que algunos registratarios no entiendan la pregunta y se identifiquen a sí mismos erróneamente. Por lo tanto, existiría un riesgo de responsabilidad si las partes relevantes no adoptaran nuevas medidas para garantizar la exactitud de la designación del registratario". (énfasis agregado) (Párrafo 17 - Personas jurídicas vs. físicas)

1.b Del mismo modo, el memorando sobre Personas jurídicas vs físicas se refiere a la "importancia" de los datos para determinar el nivel de esfuerzo necesario para garantizar la exactitud. ¿La evaluación de la "importancia" de los datos se limita a considerar la importancia para el titular de los datos y el o los responsables del tratamiento, o incluye también la importancia de los datos para terceros (en este caso, las autoridades encargadas del cumplimiento de la ley, los titulares de derechos de propiedad intelectual y otros que solicitarían los datos al responsable del tratamiento para sus propios fines)?

- "Como se explica en las Directrices de la Oficina del Comisionado de Información (ICO): 'Cuanto más importante sea que los datos personales sean exactos, mayor será el esfuerzo que se debe hacer para asegurar su exactitud'. Por lo tanto, si se utilizan los datos para tomar decisiones que puedan afectar significativamente a la persona en cuestión o a otros, es necesario poner más esfuerzo en garantizar la exactitud". (Párrafo 14 - Personas jurídicas vs. físicas)

Resumen ejecutivo de Bird & Bird

Este documento examina otras consideraciones en relación con el Principio de exactitud (las partes que tienen la obligación de cumplir este principio, las personas que tienen capacidad para invocarlo y la base sobre la cual se evaluará la exactitud de los datos). Establece los factores que deben tenerse en cuenta al evaluar la exactitud de los datos y se formulan recomendaciones sobre medidas para aumentar la exactitud de los datos de registración en poder de las partes contratadas.

Partes sujetas al principio de exactitud y "partes relevantes".

La obligación de cumplir con el Principio de exactitud del GDPR recae en el responsable (o responsables) del tratamiento. Las referencias a "partes relevantes" en los memorandos de Exactitud y Personas jurídicas vs. físicas eran hacia los responsables del tratamiento relevantes de datos de WHOIS.

Partes que tienen derecho a invocar el Principio de exactitud

El GDPR prevé una serie de recursos: reclamos ante las autoridades de supervisión, recursos judiciales y derecho a indemnización de un responsable o encargado del tratamiento. Los titulares de los datos (y cuando lo permita la legislación nacional, sus representantes) tienen derecho a ejercer todos los recursos establecidos en el GDPR. En algunos casos, estos derechos también pueden ser ejercidos por otras personas (físicas o jurídicas), por ejemplo, las afectadas por la decisión de una autoridad de supervisión o las que sufrieron daños y perjuicios como resultado de una infracción del GDPR.

Intereses de diversas partes al considerar la exactitud

El propósito para el cual se procesan los datos personales es pertinente para determinar las medidas necesarias para garantizar la exactitud de los datos. Los intereses del titular de los datos deben tenerse en cuenta al evaluar la exactitud de los datos. En algunas circunstancias, los intereses del responsable del tratamiento también serán relevantes. Aunque hay algunas referencias a los derechos de "otros" en las directrices de la ICO sobre la exactitud, este punto no se aclara más en nuestra revisión de las directrices, la jurisprudencia o la doctrina. Ante la falta de orientación, no recomendamos poner demasiado énfasis en este punto.

Medidas razonables para la exactitud de los datos

El Principio de exactitud no se ha examinado ampliamente en la doctrina ni la jurisprudencia y las referencias a dicho principio son limitadas. El carácter razonable y apropiado de las medidas de exactitud debe considerarse según el enfoque basado en el riesgo del GDPR, teniendo en cuenta, entre otras cosas, el propósito y el impacto del procesamiento. En este documento figura una lista de las medidas de exactitud sugeridas.

Pregunta 8 (Casos de uso de automatización)

Información de referencia

1. En el primer escenario, la automatización se llevaría a cabo dentro de una Puerta de enlace central encargada de recibir las solicitudes de los usuarios acreditados. La Puerta de enlace central haría una recomendación automatizada sobre si los datos solicitados deberían ser divulgados o no, mientras que la decisión final de divulgar los datos recaería en las Partes contratadas, que podrían seguir la recomendación o no (Escenario 1.a.). Las Partes contratadas con suficiente confianza en la Puerta de enlace pueden optar por automatizar la decisión de divulgar los datos (Escenario 1.b.).

2. En el segundo escenario, la decisión de divulgar los datos del registratario sería adoptada por la Puerta de enlace central sin que la Parte contratada pudiera revisar la solicitud. La puerta de enlace central tomaría esta decisión ya sea (i) después de obtener los datos pertinentes de la Parte contratada y de evaluarlos como parte de su proceso de toma de decisiones (Escenario 2.a.), o (ii) sin obtener los datos del registratario (en cuyo caso, la decisión se basaría únicamente en la información sobre el Solicitante y las declaraciones realizadas en la solicitud) (Escenario 2.b.). Un ejemplo que se da de este último escenario sería la divulgación automatizada de los datos de registración de microsoft-login.com al propietario verificado de la marca MICROSOFT, en respuesta a una solicitud en la que se alegue una infracción en materia de marcas comerciales y se declare la intención de procesar los datos para el establecimiento, el ejercicio o la defensa de demandas judiciales. Nos han solicitado que asumamos que cada escenario estaría sujeto a un conjunto de medidas de protección que se incluyen en este memorando como Apéndice 1.

A. Casos de uso del Escenario 1:

En base al asesoramiento proporcionado anteriormente en los memorandos sobre las Preguntas 1 y 2 (Responsabilidad) y la Pregunta 3 (Automatización), por favor, proporcione el siguiente análisis para cada caso de uso en el Anexo 1:

1. Sírvase describir el riesgo de responsabilidad para la Puerta de enlace central y las Partes contratadas (CP) en relación con la automatización de esta recomendación, y con la automatización de la decisión de divulgar información personal a un tercero. Si se requiere información adicional para evaluar el riesgo, sírvase indicar la información adicional necesaria.

2. ¿La decisión de divulgar información personal a un tercero es una decisión "que produce efectos jurídicos en relación con [el titular de los datos] o que lo afecta de forma similar y significativa" dentro del ámbito del artículo 22?

3. ¿Existen disposiciones o medidas de protección adicionales que mitiguen el riesgo de responsabilidad?

4. ¿Influye la toma de decisiones automatizada realizada de esta manera en su análisis de las funciones/responsabilidad de las partes descritas en el memorando de las Preguntas 1 y 2 (por ejemplo, las Partes contratadas siguen siendo responsables del tratamiento con responsabilidad cuando "la divulgación tenga lugar de forma automatizada, sin ninguna intervención manual"? 1.1.4).

B. Casos de uso del Escenario 2:

En el segundo escenario (alternativo), en el que la Puerta de enlace central tiene la capacidad contractual de exigir a las Partes contratadas que proporcionen los datos a la Puerta de enlace central:

1. ¿Cómo influyen los escenarios alternativos en el análisis proporcionado en las preguntas 1 a 4 anteriores?

2. ¿Qué escenario implica el menor riesgo de responsabilidad para las Partes contratadas? Al responder a esto, por favor indique sus suposiciones con respecto a las respectivas funciones de la ICANN y las partes contratadas, incluido un escenario en el que la Puerta de enlace central haya tercerizado la toma de decisiones a un proveedor de servicios legales independiente.

C. Aclaraciones adicionales sobre la automatización

1. Si la decisión de divulgar datos personales a un tercero es automatizada, ¿de qué manera el o los responsables del tratamiento deben proporcionar al registratario información relativa a la posibilidad de adoptar decisiones automatizadas en el procesamiento de su información personal? ¿Cómo debería comunicarse esta información al registratario y qué información relativa a la toma de decisiones automatizada debe comunicarse al registratario a fin de garantizar un procesamiento justo y transparente de conformidad con el Artículo 13?

2. ¿El suministro de la información de la respuesta a la pregunta C.1 anterior por parte del o los Responsables del tratamiento afecta al derecho del registratario a obtener confirmación de si se ha producido o no una decisión automatizada de divulgar su información personal a un tercero? ¿Afecta al derecho del registratario a obtener información significativa asociada conforme al Artículo 15.1.(h)?

3. ¿La manera en que se tome la decisión mencionada anteriormente influye en la forma en que debe proporcionarse esta información?

4. ¿Qué función desempeña la causa inmediata para determinar si la decisión de la divulgación produce un efecto jurídico o de importancia similar? Es decir, ¿en qué medida debe estar relacionada la decisión de divulgar los datos personales de un registratario con el efecto jurídico o de importancia similar del procesamiento de datos personales en última instancia? Sírvase

describir el riesgo de responsabilidad para la Puerta de enlace central o la Parte contratada si, tras recibir los datos personales, el Solicitante lleva a cabo su propio procesamiento que tenga un efecto jurídico o de importancia similar.

5. En la sección 1.12 del anterior memorándum sobre Automatización, Bird & Bird señaló lo siguiente: También puede ser posible estructurar el SSAD de manera que no implique "una decisión basada únicamente en el procesamiento automatizado". Para ampliar el concepto, en lugar de que el SSAD solicite información a los solicitantes y evalúe si se cumplen los criterios pertinentes para la divulgación de datos de registración sin carácter público, el SSAD podría publicar las categorías de solicitudes que se aceptarán y pedir a los Solicitantes que confirmen que cumplen los criterios pertinentes. En este caso, no habría un procesamiento automatizado que llevara a la decisión de divulgar los datos. El SSAD podría pedir a los solicitantes que proporcionen información adicional sobre la naturaleza de su solicitud con fines de auditoría, pero no se utilizaría para evaluar la solicitud en sí. ¿Podría explicar en detalle cómo se lograría que la decisión de divulgar "no sea automatizada" mediante (i) la publicación de las categorías de solicitudes que se aprobarán y (ii) el requisito de que un Solicitante seleccione manualmente la categoría aplicable y confirme que cumple los criterios de esa categoría de solicitudes?

Resumen ejecutivo de Bird & Bird

Este documento examina los escenarios y los casos de uso presentados por el Equipo responsable del EPDP en relación con las decisiones automatizadas para la divulgación de datos de registración sin carácter público. Identifica los casos de decisiones totalmente automatizadas que entrarían en el ámbito de aplicación del Art. 22 del GDPR, los desafíos asociados con el Art. 22 y las alternativas disponibles. En el documento se sugieren además medidas de protección para la protección de datos y se examinan consideraciones en materia de transparencia en el contexto del SSAD. Por último, examina el estatus de las partes en cada escenario y el riesgo de responsabilidad asociado.

Decisiones y alternativas del Artículo 22

El Artículo 22 del GDPR se aplica a las decisiones totalmente automatizadas que producen efectos jurídicos o de importancia similar. Las decisiones del Art. 22 solo se permiten en casos limitados, que no es probable que se apliquen en el contexto del SSAD. Las decisiones totalmente automatizadas solo se permitirán si: (a) no incluyen el procesamiento de datos personales; (b) no producen efectos jurídicos o de importancia similar; (c) están autorizados por la legislación aplicable de la UE o de los Estados miembros que establezca medidas adecuadas para proteger a las personas; o (d) están cubiertos por una derogación nacional del Art. 22 (por ejemplo, a los efectos de la detección de delitos penales). En todos los demás casos, es necesario que haya una participación humana significativa en el proceso de toma de decisiones.

¿Los criterios del Art. 22 se aplican al SSAD?

(a) Procesamiento exclusivamente automatizado: Para que se aplique el Art. 22, es necesario que haya algún tipo de tratamiento de datos personales, pero no hay ningún requisito que indique que solo se procesen datos personales para la decisión. La decisión que aquí se examina implicará, en la mayoría de los casos, el procesamiento de datos personales, independientemente de que la Puerta de enlace central tenga o no acceso a los datos solicitados y los tenga en cuenta en la toma de decisiones. Aparte del Escenario 1.a, en el que el SSAD solo emitiría una recomendación automatizada, todos los demás escenarios incluirían una decisión (de divulgar datos de registratarios a terceros) basada únicamente en el procesamiento automatizado.

(b) Efecto jurídico o de importancia similar: el término no está definido en el GDPR; sin embargo, indica un umbral elevado. El hecho de que la divulgación de los datos del registratario tenga o no ese efecto dependerá de las circunstancias de la solicitud: en el documento se evalúa la naturaleza de los efectos de la divulgación en cada caso de uso. Hemos dado respuestas claras de "sí" y "no" cuando ha sido posible: algunos casos de uso podrían mejorarse a partir de nuevas instancias de debate. El rol de la causa inmediata en la determinación de los efectos de una decisión no ha sido examinado por los tribunales o las autoridades de supervisión. En la doctrina alemana se han producido algunos debates; sin embargo, ante la falta de un debate más amplio, las opiniones de las autoridades de supervisión sobre este tema podrían ser útiles, dado que podrían permitir la automatización del SSAD sobre la base de que la Puerta de enlace central/Parte contratada solo está tomando una decisión preliminar.

Medidas de protección

En el Apéndice 2 de este documento, figura una lista de las medidas de protección sugeridas para la protección de datos. Esto incluye, entre otras cosas: la colaboración con las autoridades de supervisión, la definición clara del alcance de cada caso de uso y el establecimiento de un fundamento jurídico, la imposición de condiciones adecuadas de divulgación al Solicitante, la implementación de medidas de seguridad apropiadas, la adopción de medidas para cumplir el principio de responsabilidad, el establecimiento de políticas para respetar los derechos de las personas y la concertación de cláusulas adecuadas de protección de datos con los encargado del tratamiento.

Transparencia

La forma de proporcionar la información no se ve afectada por la existencia de la toma de decisiones automatizada; pero el contenido de la información sí.

- La información se facilitará normalmente a través del aviso de privacidad; dada la importancia del SSAD en el sistema de nombres de dominio, sería conveniente presentarla de manera destacada.
- Lo más eficiente sería que los registradores proporcionaran la información pertinente (dada su relación directa con los registratarios), independientemente de que se les

considere responsables del tratamiento en el contexto del SSAD. Si no son responsables del tratamiento, pero proporcionan la información en nombre del responsable del tratamiento, esto debería especificarse claramente a los registratarios.
- En cuanto al contenido, para decisiones del el Art. 22 únicamente, la notificación debe incluir también información sobre: la existencia de la decisión automatizada, la lógica implicada y el significado y las consecuencias previstas del procesamiento.
- Los elementos del Art. 15 del GDPR (derecho de acceso) deben facilitarse previa solicitud, aunque ya se hayan incluido en la notificación.
- El derecho de acceso exige que los responsables del tratamiento proporcionen información sobre los destinatarios a los que "se han divulgado o se divulgarán los datos": esto indica que, a falta de exenciones aplicables, los registratarios que ejerzan su derecho de acceso deben ser informados sobre las instancias de divulgación de sus datos a terceros.

Estatus de las partes

(a) En el Escenario 1, la decisión final de divulgar los datos de los registratarios corresponde a las Partes contratadas. El análisis realizado en el memorando sobre Responsabilidad también se aplicaría aquí y lo más probable es que las Partes contratadas sean consideradas por las autoridades de supervisión como responsables conjuntos del tratamiento junto con la ICANN.

(b) En el Escenario 2, la situación es menos clara. En función de si se adopta un enfoque de macronivel o micronivel, las Partes contratadas pueden consideradas responsables (conjuntos) del tratamiento para la toma automatizada de decisiones y la divulgación de datos a los Solicitantes o simplemente para la divulgación de datos a la Puerta de enlace central. Creemos que la segunda opción (responsables del tratamiento solo para la divulgación de datos a la Puerta de enlace central) es el mejor análisis, pero el punto no está claro. Es poco probable que la tercerización de la toma de decisiones a un proveedor independiente de servicios jurídicos altere la posición anterior.

En ambos escenarios, no sería plausible argumentar que las Partes contratadas son encargados del tratamiento.

La responsabilidad de las Partes contratadas se examina con respecto a:

(a) el estatus de las partes contratadas: cuando las partes contratadas sean responsables conjuntos del tratamiento, es importante asignar claramente las tareas y responsabilidades mediante un acuerdo;
(b) el tipo de responsabilidad:
- Responsabilidad frente a las personas: la norma es la responsabilidad conjunta y solidaria y las Partes contratadas pueden ser susceptibles de responsabilidad por la totalidad de los daños y perjuicios causados por el procesamiento en el que están

involucrados, independientemente de su estatus. Solo pueden evitarlo si demuestran que no estuvieron de ninguna manera involucrados en el hecho que provocó los daños y perjuicios. En caso contrario, tienen derecho a reclamar a los demás responsables del tratamiento la parte de la indemnización correspondiente a su responsabilidad.

- Responsabilidad ante las autoridades de supervisión: la responsabilidad conjunta y solidaria está menos clara aquí y hay margen para argumentar que las acciones coercitivas deberían imponerse en función del "grado de responsabilidad" de la parte.

En lo que respecta al riesgo, el Escenario 2 parece presentar un menor riesgo de responsabilidad tanto en lo que respecta a la indemnización de las personas como a las acciones coercitivas de las autoridades de supervisión.