ICANN | GNSO

Generic Names Supporting Organization

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

3 de septiembre de 2021

Estado de este documento

El presente documento constituye el Informe Final de Recomendaciones de la Fase 2A 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 Organización de Apoyo para Nombres Genéricos (GNSO).

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 2A 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-2a-updated-final-report-03sep21-en.pdf

Resumen Ejecutivo

1.1 Información de referencia

El 17 de mayo de 2018, la Junta Directiva de la ICANN aprobó la Especificación Temporaria para los Datos de Registración de dominios genéricos de alto nivel (gTLD) a fin de permitir que las partes contratadas cumplan con los requisitos contractuales existentes de la ICANN y, al mismo tiempo, cumplan con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Esta acción de la Junta Directiva impulsó el inicio del PDP del Consejo de la GNSO el 19 de julio de 2018. El PDP se llevó a cabo en dos fases: la Fase 1 se constituyó para confirmar, o no, la Especificación Temporaria para el 25 de mayo de 2019; la Fase 2 se constituyó para debatir, entre otros temas, un modelo de acceso estandarizado a los datos de registración sin carácter público (SSAD).

El Consejo de la GNSO adoptó el Informe Final para la Fase 2 durante la reunión que celebró el 24 de septiembre de 2020; sin embargo, en respuesta a una solicitud de algunos miembros del Equipo responsable del EPDP, el Consejo de la GNSO solicitó a dicho equipo que continuase trabajando en dos temas: 1) la diferenciación de datos de registración de personas jurídicas y físicas y 2) la posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme. Estos dos temas constituyen el enfoque central de la Fase 2A.

De manera más específica, el Equipo responsable del EPDP recibió las instrucciones siguientes:

a) Personas jurídicas vs. físicas: se espera que el equipo responsable del EPDP analice el estudio realizado por la ICANN (tal como lo solicitó el Equipo responsable del EPDP y lo aprobó el Consejo de la GNSO durante la Fase 1), junto con el asesoramiento legal que brindó Bird & Bird, así como los aportes sustanciales proporcionados sobre este tema durante el foro de comentario público sobre el anexo y responda lo siguiente:
i. Si se requieren actualizaciones a la recomendación de la Fase 1 del EPDP sobre este tema (“los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y personas jurídicas, aunque no están obligados a hacerlo”);
ii. Qué pautas, si las hubiese, pueden brindarse a los registradores o registros que realizan la diferenciación entre registraciones de personas físicas y jurídicas.
b) En relación a la posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme, se espera que el equipo responsable del EPDP analice el asesoramiento legal y considere propuestas específicas que proporcionen medidas de protección suficientes para abordar las cuestiones indicadas en el memorando legal. Los grupos que solicitaron más tiempo para considerar este tema, entre los que se incluyen el ALAC, el GAC y el SSAC, tendrán la responsabilidad de presentar propuestas concretas para abordar esta cuestión. Se espera que esta consideración aborde:
i. Si es factible que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme y, de ser así, si debería ser un requisito obligatorio.

ii. Si es factible, pero no es un requisito obligatorio, qué pautas, si las hubiese, pueden brindar las partes contratadas que desean implementar direcciones de correo electrónico anonimizadas uniformes.

1.2 Informe Inicial

El 3 de junio de 2021, el equipo responsable del EPDP publicó su Informe Inicial para comentario público. El Informe Inicial destacó las conclusiones del equipo hasta ese momento y estaba destinado a servir como herramienta para solicitar aportes de la comunidad, en particular, sobre áreas donde aún había divergencias significativas. Si bien las recomendaciones preliminares se incluyeron en el Informe Inicial, el equipo responsable del EPDP solicitó que se consideraran estas recomendaciones junto con un conjunto de preguntas planteadas para ayudar a informar la finalización de su informe.

Tras la publicación del Informe Inicial, el equipo responsable del EPDP: (i) examinó meticulosamente los comentarios públicos recibidos en respuesta a la publicación del Informe Inicial, (ii) continuó con la revisión del trabajo en curso con los grupos comunitarios que los miembros del equipo representan, y (iii) 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 solicitudes de consenso sobre las recomendaciones contenidas en este Informe Final fueron llevadas a cabo por el Presidente del equipo responsable del EPDP, tal como se requiere en las Pautas para los Grupos de Trabajo de la GNSO. En resumen:

1.3 Respuestas y recomendaciones

Declaración del Presidente

Si bien este Informe final y sus recomendaciones tienen el apoyo consensuado del equipo responsable de la Fase 2A del EPDP, resulta importante señalar que algunos grupos consideraron que el trabajo no avanzó lo necesario o no incluyó información detallada suficiente, si bien otros grupos manifestaron que ciertas recomendaciones no eran apropiadas o necesarias. Además, durante la etapa final de nuestro trabajo, algunos grupos hubieran preferido contar con la oportunidad de asignar designaciones de consenso más granulares a partes componentes de las recomendaciones. En este contexto, todos los lectores del Informe Final de la Fase 2A del EPDP también deberían leer las declaraciones minoritarias que presentó cada grupo, las cuales se anexaron e incluyeron en el Informe Final y en el registro histórico de nuestro trabajo.

Más allá del consenso alcanzado sobre las recomendaciones contenidas en el Informe Final, hay varias áreas sobre las que los grupos de la Fase 2A del EPDP no llegaron a un pleno consenso, entre ellas, si la diferenciación entre los datos de registración de personas jurídicas y físicas debería ser obligatoria u opcional, y si el beneficio de la publicaciones de los datos de registración de personas jurídicas estaba adecuadamente equilibrado con el riesgo de la divulgación accidental de datos

personales. Estas diferencias de opinión y perspectiva son, en su gran mayoría, inalterables por las recomendaciones contenidas en el Informe Final.

Este Informe Final constituye una transigencia de que es lo máximo que el grupo pudo lograr en este momento durante el tiempo y el alcance actualmente asignados, y no debería interpretarse como resultados que fueron completamente satisfactorios para todos. Esto resalta la importancia de las declaraciones minoritarias de comprender el contexto completo de las recomendaciones del Informe Final.

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

Consulte la sección 3 para conocer el texto completo de las recomendaciones y respuesta.

Respuesta a la instrucción del Consejo (a)(i).

El equipo responsable del EPDP remitirá la siguiente respuesta a la instrucción del Consejo de si se requieren actualizaciones a la recomendación de la Fase 1 del EPDP sobre este tema ("los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y personas jurídicas, aunque no están obligados a hacerlo"):

El equipo responsable del EPDP no logró consenso sobre recomendar cambios a la recomendación N. °17.1 de la Fase 1 del EPDP ("Los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y jurídicas, aunque no están obligados a hacerlo").

Propuesta al Consejo de la GNSO

El equipo responsable del EPDP reconoce que los desarrollos legislativos actuales y futuros pueden requerir más trabajo sobre políticas respecto de este tema, por ejemplo, abordar posibles conflictos con requisitos de políticas existentes o considerar si existe el riesgo de fragmentación del mercado deba abordarse. Al mismo tiempo, el equipo responsable del EPDP reconoce que, hasta que se adopte la legislación, quizá no sea posible evaluar el impacto con precisión. El equipo responsable del EPDP recomienda al Consejo de la GNSO seguir con estos avances a través de los informes legislativos/normativos que elabora la organización de la ICANN.

Teniendo en cuenta las discusiones actuales y la adopción prevista de la Directiva revisada sobre Seguridad de las Redes y los Sistemas de Información ("NIS2"), el equipo responsable del EPDP recomienda encarecidamente al Consejo de la GNSO seguir los procedimientos existentes para identificar y definir posibles trabajos de políticas futuros con posterioridad a la adopción de la Directiva NIS2 a fin de evaluar si se considera recomendable o necesario más desarrollo de políticas.

Pautas para la diferenciación

Recomendación n.° 1

El equipo responsable del EPDP recomienda que se DEBE crear uno o más campos para facilitar la diferenciación entre los datos de registración de personas jurídicas y físicas, o si esos datos de registración contienen datos personales o no personales. La organización de la ICANN DEBE coordinar con la comunidad técnica, por ejemplo, el Grupo de Trabajo para el Protocolo de Acceso a los Datos de Registración de Nombres de Dominio (RDAP WG), para elaborar los estándares necesarios asociados con el uso de estos campos dentro del EPP y del RDDS.

Estos campos PUEDEN ser utilizados por las partes contratadas que diferencian entre datos de registración de personas jurídicas y físicas, o si esos datos de registración contienen información personal o no personal. Para mayor claridad, las partes contratadas PUEDEN hacer uso de los campos, lo que implica que, si una parte contratada decide no usar los campos, estos pueden dejarse en blanco o pueden no estar presentes. Además, las partes contratadas PUEDEN incluir los campos en una respuesta del RDDS.

El SSAD, en consonancia con las recomendaciones de la Fase 2 del EPDP, DEBE ser compatible con los campos a fin de facilitar la integración entre el SSAD y los sistemas de las partes contratadas. Estos campos deben tener la capacidad de ajustarse a los valores siguientes:

Estado legal

- No se realizó la distinción del estado legal (valor predeterminado)
- No especificado – indica que el titular del nombre registrado o el registrador no especificó
- El titular del nombre registrado es una persona física
- El titular del nombre registrado es una persona jurídica

Datos Personales

- No se determinó la presencia de datos personales (valor predeterminado)
- No especificado – indica que el titular del nombre registrado o el registrador no especificó
- Los datos de registración contienen información personal
- Los datos de registración NO contienen información personal

Respuesta a la instrucción del Consejo (a)(ii).

Recomendación n.° 2

El equipo responsable del EPDP recomienda que las partes contratadas que opten por diferenciar en función del tipo de persona DEBERÍAN seguir las pautas[1] mencionadas más abajo y documentar claramente todos los pasos del tratamiento de datos. No obstante, no es el rol ni la responsabilidad del equipo responsable del EPDP realizar una determinación final con respecto a los riesgos jurídicos, ya que dicha responsabilidad, en última instancia, recae sobre el responsable del tratamiento de datos.

El Reglamento General de Protección de Datos (GDPR) protege a las personas físicas en relación al tratamiento de sus datos personales. El GDPR no abarca el tratamiento 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 detalles de contacto de la persona jurídica. [Cláusula 14, GDPR] Por lo general, esto permite la divulgación de datos de personas jurídicas porque está fuera de la competencia del GDPR; sin embargo, al tratar datos de personas jurídicas, las partes contratadas deberían implementar medidas de protección a fin de asegurar que la identificación de datos personales sobre una persona física no se divulgue dentro de los datos marcados como persona jurídica, ya que esto es un ejemplo de la información que *está* dentro del alcance del GDPR. Para obtener más información sobre esta distinción, consulte la carta del Comité Europeo de Protección de Datos, a partir de la pág. 4.

1. Los registratarios deberían poder autoidentificarse como personas físicas o jurídicas. Los registradores deberían brindar esta opción para que los registratarios se autoidentifiquen como personas físicas o jurídicas (i) al momento de la registración, o sin demora indebida después de la registración,[2] y (ii) en el momento en que el registratario actualice su información de contacto o sin demora indebida después de actualizar la información de contacto.
2. Todo proceso de diferenciación debe garantizar que los datos de personas físicas sean omitidos en el RDDS público, a menos que el titular de los datos haya prestado su consentimiento para publicarlos o puedan ser publicados debido a otro fundamento jurídico en virtud del GDPR, en consonancia con el enfoque de "protección de datos desde el diseño y por defecto" estipulado en el artículo 25 del GDPR.
3. Como parte de la implementación, los registradores deberían considerar usar los campos descriptos en la recomendación n.° 1 del RDDS, el SSAD o sus propios juegos de datos que indicarían el tipo de persona pertinente (física o jurídica) y, si fuese jurídica, también el tipo de datos pertinente (datos personales o no personales). Este marcado podría facilitar la revisión de solicitudes de divulgación y requisitos de automatización mediante el SSAD y el retorno de datos no

[1] Tenga en cuenta que los coordinadores de enlace de la organización de la ICANN proporcionaron al equipo responsable del EPDP los siguientes aportes sobre cómo implementar estas pautas una vez adoptadas: https://mm.icann.org/pipermail/gnso-epdp-team/2021-May/003904.html.

[2] Para mayor claridad, los registradores deberían asegurarse de que, si no se le brinda al registratario la opción de autoidentificarse en el momento de la registración, se debería brindar esta opción en un período no mayor a los 15 días posteriores a la fecha de registración.

personales de personas jurídicas por sistemas distintos del SSAD (por ejemplo, el WHOIS o el RDAP). Un mecanismo de marcado también puede ayudar a indicar cambios al tipo de datos en los campos de datos de registración.

4. Los registradores deberían asegurarse de comunicar claramente la naturaleza y las consecuencias de que un registratario se identifique como persona jurídica. Estas comunicaciones deberían incluir:

a. Una explicación de qué es una persona jurídica en lenguaje simple que sea fácil de comprender.

b. Pautas para el registratario (titular de los datos)[3] por parte del registrador respecto de las posibles consecuencias de:

i. Identificar los datos de registración de su nombre de dominio como persona jurídica;
ii. Confirmar la presencia de datos personales o datos no personales, y;
iii. Prestar consentimiento.[4] Esto también está en consonancia con la sección 3.7.7.4 del Acuerdo de Acreditación de Registradores (RAA).

5. Si los registratarios se identifican como personas jurídicas y confirman que sus datos de registración no contienen datos personales, entonces los registradores deberían publicar los datos de registración en el Servicio de Directorio de Datos de Registración de Nombres de Dominio de acceso público.

6. Los registratarios (titulares de los datos) deben tener un medio sencillo para corregir posibles errores.

7. La distinción entre personas jurídicas y físicas registratarias por sí sola puede no ser determinante de la forma en que se debería tratar la información (hacerla pública o estar enmascarada), ya que los datos suministrados por personas jurídicas pueden incluir datos personales que están protegidos por leyes de protección de datos, como el GDPR.

Recomendación n.° 3

El equipo responsable del EPDP recomienda, conforme a los requisitos del artículo 40 del GDPR para códigos de conducta, que las pautas elaboradas anteriormente respecto de la diferenciación entre personas jurídicas y físicas deberían ser consideradas en todo posible trabajo futuro dentro de la ICANN por los encargados y responsables del tratamiento de datos pertinentes en relación con la elaboración de un código de conducta del GDPR. A los efectos de evitar dudas, este código de conducta es independiente y distinto del código de conducta al que se hace referencia en el RAA o los Acuerdos de Registro. En consonancia con la cláusula 99 del GDPR, “Al redactar un código de conducta, o al enmendar o ampliar dicho código, las asociaciones y otros organismos que representan categorías de encargados y responsables del tratamiento de datos deberían consultar con las partes interesadas, incluidos los titulares de los datos cuando sea factible, y considerar las presentaciones recibidas y visiones expresadas en respuesta a dichas consultas”.

Respuesta a la instrucción del Consejo (b)(i).

[3] Tenga en cuenta que no siempre el registratario es el titular de los datos, pero, en todos los casos, se debe proporcionar notificación adecuada/consentimiento a todas las partes y por todas las partes, en virtud de la ley aplicable relacionada con la protección de datos.

[4] Consulte también https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

El equipo responsable del EPDP reconoce que puede ser técnicamente factible tener un contacto de correo electrónico basado en el registratario o un contacto de correo electrónico basado en la registración.[5] Ciertas partes interesadas ven riesgos y otras inquietudes[6] que impiden que el equipo responsable del EPDP realice una recomendación de exigir que las partes contratadas hagan que una dirección de correo electrónico basada en el registratario o en la registración esté públicamente disponible en este momento. El equipo responsable del EPDP sí señala que ciertos grupos de partes interesadas han manifestado los beneficios de 1) un contacto de correo electrónico basado en la registración con el fin de garantizar la posibilidad de ponerse en contacto, ya que se han manifestado preocupaciones con la facilidad de uso de los formularios web y 2) un contacto de correo electrónico basado en el registratario para garantizar la correlación con la registración.[7]

Respuesta a la instrucción del Consejo (b)(ii).

Recomendación n.° 4

El equipo responsable del EPDP recomienda que las partes contratadas que optan por publicar una dirección de correo electrónico basada en el registratario o en la registración con la intención de que sea seudonimizada en el RDDS de acceso público deberían evaluar el asesoramiento legal obtenido por el equipo responsable del EPDP sobre este tema (consulte Anexo F), así como cualquier otro asesoramiento relevante suministrado por las autoridades de protección de datos pertinentes.

Al evaluar los riesgos, beneficios y medidas de protección asociados con la publicación de una dirección de correo electrónico basada en el registratario o en la registración con la intención de que sea seudonimizada en el RDDS de acceso público, las partes contratadas deberían, al menos, considerar los siguientes aspectos:

- Es probable que tanto las direcciones de correo electrónico basadas en el registratario como aquellas basadas en la registración de personas tengan datos personales (es decir, ningún enfoque crea datos anónimos como se definen en el GDPR). Es probable que estos datos sean datos personales tanto desde la perspectiva del responsable del tratamiento de datos como para terceros.
- Sin embargo, incluso si se consideraran datos personales, el enmascaramiento de las direcciones de correo electrónico brinda beneficios en comparación con la publicación de las direcciones de correo electrónico de registratarios reales, entre ellos: (i) demostrar una técnica para mejorar la privacidad/medida de protección de datos desde el diseño y por defecto (artículo 25 del GDPR); y (ii) una reducción de riesgos relevante al llevar a cabo un análisis de equilibrio de interés legítimo para la divulgación de la dirección de correo electrónico enmascarada a terceros.

[5] Algunos miembros del equipo responsable del EPDP señalaron que, incluso si fuera técnicamente posible, se deberían considerar otros factores relacionados a los esfuerzos necesarios para implementar dicha función a fin de determinar la factibilidad general.
[6] Por ejemplo, 1) no queda claro que el trabajo que implica implementar dicho concepto se justifique por el beneficio potencial. 2) Además, no queda claro que los objetivos, tal como se presentan, se cumplen de forma eficaz o incluso de la mejor manera al requerir las direcciones de correo electrónico basadas en el registratario o en la registración.
[7] La capacidad de identificar los dominios que registró un registratario en particular es importante para el cumplimiento de la ley y las investigaciones de ciberseguridad de actores maliciosos que frecuentemente registran muchos dominios con fines maliciosos.

- Es probable que, en general, la publicación de una dirección de correo electrónico basada en la registración implique un riesgo menor que la publicación de direcciones de correo electrónico basadas en el registratario debido a la cantidad de información que una parte puede potencialmente vincular a un titular de los datos en función de un contacto de correo electrónico basado en el registratario.
- Tanto para la publicación de direcciones de correo electrónico basadas en el registratario como para la publicación de aquellas basadas en la registración, las partes contratadas deberían adoptar medidas eficaces para mitigar la disponibilidad de detalles de contacto a spammers.

1.4 Conclusiones y próximos pasos

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

1.5 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 las instrucciones adoptadas por el Consejo de la GNSO; y
- 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 manifestación de la totalidad de las iniciativas y deliberaciones de dicho equipo.

2.1 Metodología de trabajo

El equipo responsable del EPDP comenzó sus deliberaciones para la Fase 2A el 17 de diciembre de 2020. El equipo llevó a cabo su trabajo a través de teleconferencias programadas una o más veces por semana, además de intercambios de correo electrónico en su lista de correo. 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 como parte del paquete de proyectos para la Fase 2A del EPDP, el cual fue analizado y actualizado en forma periódica, y compartido con el Consejo de la GNSO.

2.2 Resumen informativo y enfoque

Con el fin de garantizar un entendimiento común de los temas que se abordarán como parte de sus deliberaciones sobre la Fase 2A, el equipo de apoyo al personal elaboró resúmenes informativos para cada uno de los temas. Los resúmenes informativos incluyeron: 1) instrucciones del Consejo al equipo responsable del EPDP, 2) recomendaciones relevantes de la Fase 1 y Fase 2 del EPDP, 3) estudios o asesoramiento legal relevantes obtenidos con anterioridad, 4) requisitos procesales, 5) instrucciones sobre plazos y 6) el enfoque propuesto. Estos resúmenes informativos se distribuyeron al equipo responsable del EPDP antes de la primera reunión y, junto con la lectura asignada, formaron la base de la primera asignación del equipo responsable del EPDP. En particular, se le solicitó al equipo responsable del EPDP analizar exhaustivamente los estudios asignados y el asesoramiento legal anterior, e identificar todas las preguntas aclaratorias.

2.3 Comité de Asuntos Jurídicos

De manera similar a la Fase 1 y a la Fase 2, el equipo responsable del EPDP contó con su Comité de Asuntos Jurídicos para analizar y perfeccionar las preguntas que identificó dicho equipo. El Comité de Asuntos Jurídicos está compuesto por un miembro de cada grupo de partes interesadas/unidad constitutiva/comité asesor representado en el equipo responsable del EPDP.

El Comité de Asuntos Jurídicos de la Fase 2A 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 formulasen de manera neutral, de forma tal que evitasen tanto los resultados supuestos como la posición 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 utilizase de manera responsable.

El Comité de Asuntos Jurídicos distribuyó todas las preguntas acordadas al equipo responsable del EPDP antes de enviarlas a Bird & Bird.

A la fecha, el equipo responsable del EPDP acordó enviar cuatro preguntas sobre la Fase 2A a Bird & Bird. El texto completo de las preguntas y el asesoramiento legal recibido en respuesta a las preguntas se encuentran en el Anexo F.

2.4 Preguntas del Consejo

Al abordar las preguntas asignadas por el Consejo de la GNSO, el equipo responsable del EPDP consideró lo siguiente: (1) los aportes recibidos de cada grupo como parte de las deliberaciones; (2) los aportes relevantes de las fases 1 y 2; (3) los aportes brindados sobre estos temas por cada grupo en respuesta a la solicitud de aportes iniciales durante las fases anteriores, así como los comentarios relevantes recibidos durante el foro de comentario público sobre el anexo de la Fase 2 del EPDP;[8] (4) la lectura requerida identificada para cada tema de los resúmenes informativos, incluido el estudio de la organización de la ICANN sobre "Diferenciación entre personas jurídicas y físicas en Servicios de Directorio de Datos de Registración de Nombres de Dominio (RDDS)", y (5) los aportes realizados por Bird & Bird.

[8] Consulte https://community.icann.org/x/Ag9pBQ, https://community.icann.org/x/Ag9pBQ, https://www.icann.org/public-comments/epdp-phase-2-addendum-2020-03-26-en y también la Herramienta de revisión de comentarios públicos sobre anexos.

3 Respuestas del equipo responsable del EPDP a las preguntas del Consejo y recomendaciones

Tras analizar los comentarios públicos sobre el Informe Inicial, el equipo responsable del EPDP presenta sus respuestas y 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:

Declaración del Presidente

Si bien este Informe final y sus recomendaciones tienen el apoyo consensuado del equipo responsable de la Fase 2A del EPDP, resulta importante señalar que algunos grupos consideraron que el trabajo no avanzó lo necesario o no incluyó información detallada suficiente, si bien otros grupos manifestaron que ciertas recomendaciones no eran apropiadas o necesarias. Además, durante la etapa final de nuestro trabajo, algunos grupos hubieran preferido contar con la oportunidad de asignar designaciones de consenso más granulares a partes componentes de las recomendaciones. En este contexto, todos los lectores del Informe Final de la Fase 2A del EPDP también deberían leer las declaraciones minoritarias que presentó cada grupo, las cuales se anexaron e incluyeron en el Informe Final y en el registro histórico de nuestro trabajo.

Más allá del consenso alcanzado sobre las recomendaciones contenidas en el Informe Final, hay varias áreas sobre las que los grupos de la Fase 2A del EPDP no llegaron a un pleno consenso, entre ellas, si la diferenciación entre los datos de registración de personas jurídicas y físicas debería ser obligatoria u opcional, y si el beneficio de la publicaciones de los datos de registración de personas jurídicas estaba adecuadamente equilibrado con el riesgo de la divulgación accidental de datos personales. Estas diferencias de opinión y perspectiva son, en su gran mayoría, inalterables por las recomendaciones contenidas en el Informe Final.

Este Informe Final constituye una transigencia de que es lo máximo que el grupo pudo lograr en este momento durante el tiempo y el alcance actualmente asignados, y no debería interpretarse como resultados que fueron completamente satisfactorios para todos. Esto resalta la importancia de las declaraciones minoritarias de comprender el contexto completo de las recomendaciones del Informe Final.

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

3.1 Personas jurídicas vs. físicas

El Consejo de la GNSO le encargó al equipo responsable del EPDP la tarea de abordar las dos preguntas siguientes:

i. Si se requieren actualizaciones a la recomendación de la Fase 1 del EPDP sobre este tema ("los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y personas jurídicas, aunque no están obligados a hacerlo");
ii. Qué pautas, si las hubiese, pueden brindarse a los registradores o registros que realizan la diferenciación entre registraciones de personas físicas y jurídicas.

Para abordar estas preguntas, el equipo responsable del EPDP comenzó a analizar toda la información relevante, por ejemplo, (1) el estudio realizado por la organización de la ICANN,[9] (2) el asesoramiento legal brindado por Bird & Bird, y (3) los aportes sustanciales proporcionados sobre este tema durante el foro de comentario público. Tras el análisis de esta información, el equipo responsable del EPDP identificó varias preguntas aclaratorias, las cuales, después de la revisión realizada por el Comité de Asuntos Jurídicos del equipo responsable del EPDP, fueron presentadas a Bird & Bird (consulte https://community.icann.org/x/xQhACQ). El equipo responsable del EPDP analizó las respuestas de Bird & Bird y aplicó el asesoramiento recibido en sus recomendaciones mencionadas más adelante en este documento.

• Respuesta del equipo responsable del EPDP a la pregunta i.

El equipo responsable del EPDP debatió esta pregunta de manera exhaustiva. Como punto de partida, el equipo responsable del EPDP señala que el GDPR y muchas otras leyes de protecciones de datos establecen requisitos para proteger los datos personales de las personas físicas. No protegen los datos no personales de las personas jurídicas.[10] Al mismo tiempo, el equipo responsable del EPDP reconoce que el Comité Europeo de Protección de Datos ("EDPB") ha asesorado a la ICANN en una carta de julio de 2018 en la que manifestó que "el simple hecho de que un registratario sea una persona jurídica no necesariamente justifica la publicación ilimitada de datos personales relacionados con las personas físicas que trabajan para esa organización o que la representan", y que "los datos personales que identifican a los empleados individuales (o a terceros) que actúan en nombre del registratario no deberían estar disponibles públicamente por defecto en el contexto del WHOIS".[11] Para obtener más visiones sobre las diversas perspectivas acerca de esta pregunta, se recomienda a los lectores consultar el Informe Inicial del equipo responsable del EPDP, así como las declaraciones minoritarias anexadas a dicho informe.

[9] Como parte de la recomendación de política n.°17 de su Fase 1, el equipo responsable del EPDP recomendó que, "a la brevedad posible", la organización de la ICANN lleve a cabo un estudio, para el cual se elaboren términos de referencia en consulta con la comunidad, que considere lo siguiente:

- La viabilidad y los costos, incluidos los costos de implementación y de posible responsabilidad para diferenciar entre personas físicas y jurídicas;
- Ejemplos de industrias u otras organizaciones que han diferenciado entre personas físicas y jurídicas exitosamente;
- Riesgos de privacidad para los titulares del nombre registrado ante la diferenciación entre personas físicas y jurídicas; y
- Otros posibles riesgos (si los hubiese) para los registradores y registros resultantes de la falta de diferenciación".

La organización de la ICANN entregó el estudio al equipo responsable del EPDP en julio de 2020.

[10] " Esta reglamentación no abarca el tratamiento 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".

[11] Andrea Jelinek, Comité Europeo de Protección de Datos, carta a Göran Marby con fecha del 5 de julio de 2018, disponible en https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

El equipo responsable del EPDP remitirá la siguiente respuesta a la instrucción del Consejo de si se requieren actualizaciones a la recomendación de la Fase 1 del EPDP sobre este tema ("los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y personas jurídicas, aunque no están obligados a hacerlo"):

El equipo responsable del EPDP no logró consenso sobre recomendar cambios a la recomendación N. °17.1 de la Fase 1 del EPDP ("Los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y jurídicas, aunque no están obligados a hacerlo").

Propuesta al Consejo de la GNSO

El equipo responsable del EPDP reconoce que los desarrollos legislativos actuales y futuros pueden requerir más trabajo sobre políticas respecto de este tema, por ejemplo, abordar posibles conflictos con requisitos de políticas existentes o considerar si existe el riesgo de fragmentación del mercado deba abordarse. Al mismo tiempo, el equipo responsable del EPDP reconoce que, hasta que se adopte la legislación, quizá no sea posible evaluar el impacto con precisión. El equipo responsable del EPDP recomienda al Consejo de la GNSO seguir con estos avances a través de los informes legislativos/normativos que elabora la organización de la ICANN.

Teniendo en cuenta las discusiones actuales y la adopción prevista de la Directiva revisada sobre Seguridad de las Redes y los Sistemas de Información ("NIS2"), el equipo responsable del EPDP recomienda encarecidamente al Consejo de la GNSO seguir los procedimientos existentes para identificar y definir posibles trabajos de políticas futuros con posterioridad a la adopción de la Directiva NIS2 a fin de evaluar si se considera recomendable o necesario más desarrollo de políticas.

Pautas para la diferenciación

El equipo responsable del EPDP reconoce que puede ser necesario facilitar y armonizar las prácticas para las partes contratadas que deciden hacer la diferenciación entre personas físicas y jurídicas.

Para facilitar la diferenciación, el equipo responsable del EPDP ha elaborado las pautas que están disponibles en la sección contenida más adelante en este documento. En estas pautas, el equipo responsable del EPDP sugiere que los registradores consideren el uso de un campo que indicaría el tipo de registratario implicado (persona jurídica/física) y el tipo de datos de los registratarios jurídicos implicados (personales/no personales). Este concepto de identificar el tipo de datos de registración de nombres de dominio implicados también se menciona en la recomendación n.° 9.4.4 de la Fase 2 del EPDP (respuesta automatizada a solicitudes de divulgación).

En la recomendación siguiente, el equipo responsable del EPDP describe cómo una parte contratada que desea realizar la diferenciación puede hacerlo mediante uno o varios campos nuevos para capturar los resultados de dicha diferenciación.

Recomendación n.° 1

El equipo responsable del EPDP recomienda que se DEBE crear uno o más campos para facilitar la diferenciación entre los datos de registración de personas jurídicas y físicas, o si esos datos de registración contienen datos personales o no personales. La organización de la ICANN DEBE coordinar con la comunidad técnica, por ejemplo, el Grupo de Trabajo para el Protocolo de Acceso a los Datos de Registración de Nombres de Dominio (RDAP WG), para elaborar los estándares necesarios asociados con el uso de estos campos dentro del EPP y del RDDS.

Estos campos PUEDEN ser utilizados por las partes contratadas que diferencian entre datos de registración de personas jurídicas y físicas, o si esos datos de registración contienen información personal o no personal. Para mayor claridad, las partes contratadas PUEDEN hacer uso de los campos, lo que implica que, si una parte contratada decide no usar los campos, estos pueden dejarse en blanco o pueden no estar presentes. Además, las partes contratadas PUEDEN incluir los campos en una respuesta del RDDS.

El SSAD, en consonancia con las recomendaciones de la Fase 2 del EPDP, DEBE ser compatible con los campos a fin de facilitar la integración entre el SSAD y los sistemas de las partes contratadas. Estos campos deben tener la capacidad de ajustarse a los valores siguientes:

Estado legal

- No se realizó la distinción del estado legal (valor predeterminado)
- No especificado – indica que el titular del nombre registrado o el registrador no especificó
- El titular del nombre registrado es una persona física
- El titular del nombre registrado es una persona jurídica

Datos Personales

- No se determinó la presencia de datos personales (valor predeterminado)
- No especificado – indica que el titular del nombre registrado o el registrador no especificó
- Los datos de registración contienen información personal
- Los datos de registración NO contienen información personal

Respuesta del equipo responsable del EPDP a la pregunta ii.

El equipo responsable del EPDP centró su tarea primero en considerar las pautas que resultarían útiles para los registradores y operadores de registro que opten por hacer la diferenciación entre registraciones de personas físicas y jurídicas.
Definiciones (tenga en cuenta que estas son obtenidas de trabajos anteriores relacionados con el EPDP, como se indica más abajo):

- EPDP-p1-IRT:[12] “Publicación”, “Publicar” y “Publicados” significa proporcionar datos de registración en servicios de directorio de datos de registración de acceso público.
- EPDP-p1-IRT:[13] “Datos de registración” significa los valores de elementos de datos recopilados de una persona física o jurídica, o generados por el registrador u operador de registro, en cualquier caso en relación con un nombre registrado de conformidad con la sección 7 de esta política.
- Informe Final de la Fase 1 del EPDP:[14] “Divulgación” significa la acción de tratamiento mediante la cual el responsable del tratamiento de datos acepta la responsabilidad de divulgar la información personal a terceros, según la solicitud de divulgación correspondiente.

Información de referencia y observaciones del equipo responsable del EPDP
En la elaboración de las pautas mencionadas más adelante en el presente, el equipo responsable del EPDP desea recordar al Consejo y a la comunidad en general los siguientes aspectos:

Alcance del GDPR y otras leyes de protección de datos
A. El GDPR y otras leyes de protección de datos establecen requisitos para proteger los datos personales de personas físicas. No protegen los datos personales de personas jurídicas ni los datos no personales.
B. El GDPR no abarca el tratamiento 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. Sin embargo, cuando se usa la información de una persona física en relación con una persona jurídica, por ejemplo, como representante de una empresa, los datos de la persona física permanecen protegidos como datos personales en virtud del GDPR.
C. La distinción entre registratarios que son personas jurídicas y físicas puede no ser determinante de la forma en que se debería tratar la información (hacerla pública o estar enmascarada), ya que los datos suministrados por personas jurídicas pueden incluir datos personales que están protegidos por leyes de protección de datos, como el GDPR.
D. Si bien el GDPR no abarca el tratamiento de datos personales que se relacionan con personas jurídicas, los Principios del GDPR, algunos de los cuales se describen más adelante en el presente, aun pueden ser aplicados si los datos personales de una persona física son tratados como parte del proceso de diferenciación y deberían ser ponderados según corresponda por las partes contratadas. En consonancia con los Principios estipulados en el artículo 5 del GDPR:
a. Legalidad, equidad y transparencia: “Cualquier tratamiento de datos personales debe ser legal, equitativo y transparente. Debe ser claro y transparente para los individuos a quienes conciernen los datos personales que se recopilan, usan, consultan o de algún otro modo se tratan, y en la medida en que los datos personales son, o serán, tratados”. El principio de transparencia “concierne, en particular, información a los titulares de datos sobre la identidad del responsable del tratamiento de datos y los fines del tratamiento [.][15] [. . .]

[12] Consulte https://docs.google.com/document/d/1SVFkoI6RmrVVz--RrVLSOj1bmz1qLb7_JTuvt7At4Uo/edit.
[13] Ibidem.
[14] Consulte https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-2-20feb19-en.pdf.
[15] Consulte: Pautas del Comité Irlandés de Protección de datos sobre el derecho a ser informado. (https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-1 4-gdpr) y las Pautas

Si el fundamento legal es consentimiento, entonces "brindar información a los titular de los datos antes de obtener su consentimiento es esencial a fin de permitirles tomar decisiones informadas, comprender qué están acordando y, por ejemplo, ejercer su derecho a retirar su consentimiento".[16]

b. Limitación de propósito: "Los datos personales deberán [. . .] recopilarse con fines específicos, explícitos y legítimos, y no pueden tener ningún tratamiento que sea incompatible con esos propósitos".[17].

c. Minimización de datos: "Limitar la cantidad de datos personales recopilados a aquella que sea necesaria para el propósito".[18]

d. Responsabilidad: El principio de responsabilidad del GDPR "requiere que las organizaciones demuestren (y, en la mayoría de los casos, documenten) las formas en que cumplen con los principios de protección de datos al realizar transacciones".[19]

Recomendaciones relevantes de la Fase 1 del EPDP[20]

E. En virtud de la recomendación n.° 6 de la Fase 1 del EPDP[21], "tan pronto como sea comercialmente razonable, el registrador debe ofrecer al titular del nombre registrado la oportunidad de prestar su consentimiento para publicar información de contacto editada, así como la dirección de correo electrónico, en el RDS (sistema de Servicios de Directorio de Registración) del registrador patrocinador".

F. En virtud de la recomendación n.° 17 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".

Recomendaciones relevantes de la Fase 2 del EPDP

G. En virtud de la recomendación 9.4.4 del Informe Final de la Fase 2[22], que aborda la automatización del procesamiento del SSAD: "el Equipo responsable del EPDP recomienda que los siguientes tipos de solicitudes de divulgación, para los cuales se ha indicado la autorización legal en

para los Grupos de Trabajo sobre el Artículo 29 sobre la transparencia en virtud del Reglamento 2016/679, secciones 6 y 7 (según fue adoptado por el EDPB) (https://ec.europa.eu/newsroom/article29/items/622227).

[16] Consulte las Pautas del EDPB, 05/2020, Pautas 05/2020 sobre consentimiento en virtud del reglamento 2016/679, sección 3.3.

[17] Consulte el artículo 5(1)(b) del GDPR; consulte también las pautas sobre limitación de propósito de la Oficina del Comisario de Información del Reino Unido, (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/).

[18] Consulte las Pautas del EDPB, 04/2019, Protección de datos desde el diseño y por defecto, sección 3.5 (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf) y el artículo 5.1 (c) del GDPR.

[19] Consulte: Pautas sobre responsabilidad del Comité Irlandés de Protección de Datos (https://www.dataprotection.ie/en/organisations/know-your-obligations/accountability-obligation); consulte también las Pautas del EDPB, 04/2019, Protección de datos desde el diseño y por defecto, sección 3.9 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[20] Nota: la recomendación n.°°12 de la Fase 1 del EPDP respecto del campo Organización, una vez implementado, puede también ayudar a las partes contratadas a diferenciar entre personas jurídicas y físicas, si optan por hacerlo.

[21] Para más información sobre el estado de la implementación de las recomendaciones de la Fase 1 del EPDP, consulte https://www.icann.org/resources/pages/registration-data-policy-gtlds-epdp-1-2019-07-30-en.

[22] Tenga en cuenta que las recomendaciones de la Fase 2 del EPDP están en poder de la Junta directiva de la ICANN para su consideración/aprobación.

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[.] [. . .] Ningún dato personal en el acta de la registración que haya sido divulgado previamente por la Parte contratada". Esta recomendación 9.4.4 se centra principalmente en la automatización de la divulgación de las actas de registración que no incluyen datos personales.[23]

H. En virtud de la recomendación 8.7.1 del Informe Final de la Fase 2, si la parte contratada recibe una solicitud del administrador del punto de acceso centralizado de SSAD y la parte contratada determinó que es una solicitud válida, "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 en virtud de la ley aplicable".

Modelos empresariales de los registradores

I. Los registradores operan diferentes modelos empresariales (minorista, mayorista, protección de marcas, otros) y la pauta de un modelo demasiado prescriptivo o que se adapte a todos puede no considerar adecuadamente el rango de modelos empresariales de los registradores y los diversos flujos de proceso que los diferentes modelos empresariales pueden requerir. En cambio, cualquier pauta debería brindar a los registradores la flexibilidad de implementar la diferenciación de la manera en que mejor se adapte a su modelo empresarial y reduzca los riesgos asociados con la diferenciación a un nivel aceptable para dicho registrador en particular. Por ejemplo, la diferenciación en el momento de la registración puede no ser factible en todas las circunstancias, incluso para ciertos modelos empresariales de registradores.

Pauta propuesta

Recomendación n.° 2

El equipo responsable del EPDP recomienda que las partes contratadas que opten por diferenciar en función del tipo de persona DEBERÍAN seguir las pautas[24] mencionadas más abajo y documentar claramente todos los pasos del tratamiento de datos. No obstante, no es el rol ni la responsabilidad del equipo responsable del EPDP realizar una determinación final con respecto a los riesgos jurídicos, ya que dicha responsabilidad, en última instancia, recae sobre el responsable del tratamiento de datos.

El Reglamento General de Protección de Datos (GDPR) protege a las personas físicas en relación al tratamiento de sus datos personales. El GDPR no abarca el tratamiento 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 detalles de contacto de la persona jurídica. [Cláusula 14, GDPR] Por lo general, esto permite la divulgación de datos de personas

[23] Tenga en cuenta que los detalles exactos de cómo se implementará esta recomendación serán determinados por la organización de la ICANN junto con el Equipo para la Revisión de la Implementación, una vez que la Junta de la ICANN haya aprobado las recomendaciones.

[24] Tenga en cuenta que los coordinadores de enlace de la organización de la ICANN proporcionaron al equipo responsable del EPDP los siguientes aportes sobre cómo implementar estas pautas una vez adoptadas: https://mm.icann.org/pipermail/gnso-epdp-team/2021-May/003904.html.

jurídicas porque está fuera de la competencia del GDPR; sin embargo, al tratar datos de personas jurídicas, las partes contratadas deberían implementar medidas de protección a fin de asegurar que la identificación de datos personales sobre una persona física no se divulgue dentro de los datos marcados como persona jurídica, ya que esto es un ejemplo de la información que *está* dentro del alcance del GDPR. Para obtener más información sobre esta distinción, consulte la carta del Comité Europeo de Protección de Datos, a partir de la pág. 4.

1. Los registratarios deberían poder autoidentificarse como personas físicas o jurídicas. Los registradores deberían brindar esta opción para que los registratarios se autoidentifiquen como personas físicas o jurídicas (i) al momento de la registración, o sin demora indebida después de la registración,[25] y (ii) en el momento en que el registratario actualice su información de contacto o sin demora indebida después de actualizar la información de contacto.
2. Todo proceso de diferenciación debe garantizar que los datos de personas físicas sean omitidos en el RDDS público, a menos que el titular de los datos haya prestado su consentimiento para publicarlos o puedan ser publicados debido a otro fundamento jurídico en virtud del GDPR, en consonancia con el enfoque de "protección de datos desde el diseño y por defecto" estipulado en el artículo 25 del GDPR.
3. Como parte de la implementación, los registradores deberían considerar usar los campos descriptos en la recomendación n.° 1 del RDDS, el SSAD o sus propios juegos de datos que indicarían el tipo de persona pertinente (física o jurídica) y, si fuese jurídica, también el tipo de datos pertinente (datos personales o no personales). Este marcado podría facilitar la revisión de solicitudes de divulgación y requisitos de automatización mediante el SSAD y el retorno de datos no personales de personas jurídicas por sistemas distintos del SSAD (por ejemplo, el WHOIS o el RDAP). Un mecanismo de marcado también puede ayudar a indicar cambios al tipo de datos en los campos de datos de registración.
4. Los registradores deberían asegurarse de comunicar claramente la naturaleza y las consecuencias de que un registratario se identifique como persona jurídica. Estas comunicaciones deberían incluir:

c. Una explicación de qué es una persona jurídica en lenguaje simple que sea fácil de comprender.

d. Pautas para el registratario (titular de los datos)[26] por parte del registrador respecto de las posibles consecuencias de:

i. Identificar los datos de registración de su nombre de dominio como persona jurídica;
ii. Confirmar la presencia de datos personales o datos no personales, y;
iii. Prestar consentimiento.[27] Esto también está en consonancia con la sección 3.7.7.4 del Acuerdo de Acreditación de Registradores (RAA).

5. Si los registratarios se identifican como personas jurídicas y confirman que sus datos de registración no contienen datos personales, entonces los registradores deberían publicar los datos

[25] Para mayor claridad, los registradores deberían asegurarse de que, si no se le brinda al registratario la opción de autoidentificarse en el momento de la registración, se debería brindar esta opción en un período no mayor a los 15 días posteriores a la fecha de registración.
[26] Tenga en cuenta que no siempre el registratario es el titular de los datos, pero, en todos los casos, se debe proporcionar notificación adecuada/consentimiento a todas las partes y por todas las partes, en virtud de la ley aplicable relacionada con la protección de datos.
[27] Consulte también https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

de registración en el Servicio de Directorio de Datos de Registración de Nombres de Dominio de acceso público.

6. Los registratarios (titulares de los datos) deben tener un medio sencillo para corregir posibles errores.

7. La distinción entre personas jurídicas y físicas registratarias por sí sola puede no ser determinante de la forma en que se debería tratar la información (hacerla pública o estar enmascarada), ya que los datos suministrados por personas jurídicas pueden incluir datos personales que están protegidos por leyes de protección de datos, como el GDPR.

Recomendación n.° 3

El equipo responsable del EPDP recomienda, conforme a los requisitos del artículo 40 del GDPR para códigos de conducta, que las pautas elaboradas anteriormente respecto de la diferenciación entre personas jurídicas y físicas deberían ser consideradas en todo posible trabajo futuro dentro de la ICANN por los encargados y responsables del tratamiento de datos pertinentes en relación con la elaboración de un código de conducta del GDPR. A los efectos de evitar dudas, este código de conducta es independiente y distinto del código de conducta al que se hace referencia en el RAA o los Acuerdos de Registro. En consonancia con la cláusula 99 del GDPR, “Al redactar un código de conducta, o al enmendar o ampliar dicho código, las asociaciones y otros organismos que representan categorías de encargados y responsables del tratamiento de datos deberían consultar con las partes interesadas, incluidos los titulares de los datos cuando sea factible, y considerar las presentaciones recibidas y visiones expresadas en respuesta a dichas consultas”.

Tres escenarios de ejemplo

(Nota: estos escenarios son meramente ilustraciones de la forma en que un registrador podría aplicar las pautas mencionadas anteriormente. NO deben ser considerados pautas en sí).

El equipo responsable del EPDP identificó tres diferentes escenarios generales respecto de cómo la diferenciación podría llevarse a cabo en función de quién es responsable y el momento de dicha diferenciación. Se debería señalar que pueden ser posibles otros enfoques o una combinación de ellos.

1. Autoidentificación del titular de los datos en el momento de la registración/recopilación de los datos

a. El registrador informa al registratario (en virtud de la pauta n.° 3 mencionada anteriormente) y solicita al registratario (titular de los datos) en el momento de recopilación de datos de registración que designe el tipo de persona jurídica o física. El registrador también debe solicitar al registratario que confirme si sólo se proporcionan datos personales para el tipo de persona jurídica.[28]

b. Si el registratario (titular de los datos) se identificó como persona jurídica y brindó la confirmación de que los datos de registración no incluyen datos personales, el registrador debería

[28] Tenga en cuenta que la confirmación de que sólo se suministran datos personales también podría suceder en un momento posterior. Sin embargo, hasta que el registratario confirme que no hay datos personales en los datos de registración, el registrador no configura los datos de registración en divulgación automatizada.

(i) acceder a los detalles de contacto suministrados para verificar la declaración del registratario;[29] (ii) configurar el juego de datos de registración en divulgación automatizada en respuesta a las consultas del SSAD; y (iii) publicar los datos (para brindar los datos de registración en los Servicios de Directorio de Datos de Registración de Nombres de Dominio de acceso público).

c. Si el registratario (titular de los datos) se identificó como persona física o confirmó que existen datos personales, el registrador no configura dichos datos de registración en divulgación y publicación automatizadas, a menos que el titular de los datos preste consentimiento para su publicación.[30]

2. Autoidentificación del titular de los datos al momento de actualizar la registración[31]

a. El registrador recopila los datos de registración y los edita de manera provisoria.

b. El registrador informa al registratario (en virtud de la pauta n.° 3 mencionada anteriormente) y solicita al registratario (titular de los datos) que se identifique como persona jurídica o física. El registrador también debería solicitar al registratario que se identifica como persona jurídica que confirme que no se proporcionan datos personales.[32]

c. El registratario (titular de los datos) se identifica como persona jurídica o física, y confirma que no se suministraron datos personales una vez finalizada la actualización. Por ejemplo, el registratario puede confirmar el tipo de persona al momento de la verificación inicial de los datos, en respuesta a su recepción del correo electrónico de recordatorio de datos del WHOIS para las registraciones existentes o mediante una notificación separada en la que se solicita la autoidentificación.[33]

d. Si el titular de los datos se identificó como persona jurídica y confirma que los datos de registración no incluyen datos personales, el registrador debería (i) acceder a los detalles de contacto suministrados para verificar la declaración del registratario;[34] (ii) configurar el juego de

[29] En virtud del asesoramiento brindado por Bird & Bird, "se recomienda este método de verificación, ya que ayudará a reducir los riesgos. Esa reducción de los riesgos sería mayor si existiese un período de gracia razonable dentro del cual se pueda presentar la objeción, antes de que los datos en cuestión se publiquen en los datos de registración" y "el requisito de una respuesta afirmativa a los correos de verificación parece ser excesivamente cauteloso, a menos que estudios muestren que las medidas adoptadas no pueden mantener cantidades realmente sustanciales de datos personales al margen de los datos de registración publicados. Sin embargo, si un correo electrónico de verificación "rebota" (es decir, una parte contratada sabe que no fue entregado), entonces sería mejor que no se procediera con la publicación".

[30] Tenga en cuenta que el titular de los datos puede no ser la parte que ejecuta el proceso, pero puede haberle solicitado a un tercero que lo hiciera. En dicho caso, quizá no sea posible documentar el consentimiento.

[31] La expectativa para este escenario es que se siga un cronograma similar al que actualmente se aplica en la Especificación sobre Exactitud del WHOIS del Acuerdo de Acreditación de Registradores (consulte https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy).

[32] Tenga en cuenta que la confirmación de que sólo se suministran datos personales también podría suceder en un momento posterior. Sin embargo, hasta que el registratario confirme que no hay datos personales en los datos de registración, el registrador no configura los datos de registración en divulgación automatizada.

[33] Nota: la implementación de la recomendación 12 de la Fase 1 del EPDP (campo de organización) puede facilitar el proceso de autoidentificación.

[34] En virtud del asesoramiento brindado por Bird & Bird, "se recomienda este método de verificación, ya que ayudará a reducir los riesgos. Esa reducción de los riesgos sería mayor si existiese un período de gracia razonable dentro del cual se pueda presentar la objeción, antes de que los datos en cuestión se publiquen en los datos de registración" y "el requisito de una respuesta afirmativa a los correos de verificación parece ser excesivamente cauteloso, a menos que estudios muestren que las medidas adoptadas no pueden mantener cantidades realmente sustanciales de datos personales al margen de los datos de registración publicados. Sin embargo, si un correo electrónico de verificación "rebota" (es decir, una parte contratada sabe que no fue entregado), entonces sería mejor que no se procediera con la publicación".

datos de registración en divulgación automatizada en respuesta a las consultas del SSAD; y (iii) publicar los datos.

3. El registrador determina el tipo de registratario en función de los datos suministrados

a. El registrador recopila los datos de registración y los edita de manera provisoria.

b. El registrador usa los datos recopilados para inferir el tipo de persona jurídica o física.[35]

c. Si el registrador infiere que se trata de una persona jurídica y, luego, se le informa al registratario (titular de los datos) (según la pauta n.° 3 anteriormente mencionada) y este confirma que no hay datos personales presentes, el registrador debería (i) acceder a los detalles de contacto suministrados para verificar la declaración del registratario;[36] (ii) configurar el juego de datos de registración en divulgación automatizada en respuesta a las consultas del SSAD; y (iii) publicar los datos.

d. Si el registrador infirió que el registratario es una persona física y detectó datos personales, el registrador no debería divulgar los datos de registración, a menos que el registratario preste su consentimiento para su publicación o el registrador divulga los datos en respuesta a una solicitud de divulgación legítima.

El equipo responsable del EPDP reconoce que, en todos los escenarios presentados anteriormente, existe la posibilidad de una identificación errónea, lo que puede ocasionar la divulgación accidental de datos personales. En este respecto, el equipo responsable del EPDP recomienda revisar el memorando de Bird & Bird, el cual también está disponible en el Anexo F, en particular, las secciones 11.1-2, 13, 14.3 y 18.

3.2 Factibilidad de contactos únicos

El Consejo de la GNSO le encargó al equipo responsable del EPDP la tarea de abordar las dos preguntas siguientes:

i. Si es factible que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme y, de ser así, si debería ser un requisito obligatorio.
ii. Si es factible, pero no es un requisito obligatorio, qué pautas, si las hubiese, pueden brindar las partes contratadas que desean implementar direcciones de correo electrónico anonimizadas uniformes.

[35] Algunos miembros del equipo responsable del EPDP señalaron que pueden existir riesgos en el caso de que el registrador infiera una diferenciación sin la participación del registratario (titular de los datos).

[36] En virtud del asesoramiento brindado por Bird & Bird, "se recomienda este método de verificación, ya que ayudará a reducir los riesgos. Esa reducción de los riesgos sería mayor si existiese un período de gracia razonable dentro del cual se pueda presentar la objeción, antes de que los datos en cuestión se publiquen en los datos de registración" y "el requisito de una respuesta afirmativa a los correos de verificación parece ser excesivamente cauteloso, a menos que estudios muestren que las medidas adoptadas no pueden mantener cantidades realmente sustanciales de datos personales al margen de los datos de registración publicados. Sin embargo, si un correo electrónico de verificación "rebota" (es decir, una parte contratada sabe que no fue entregado), entonces sería mejor que no se procediera con la publicación".

El Consejo también indicó que "Los grupos que solicitaron más tiempo para considerar este tema, entre los que se incluyen el ALAC, el GAC y el SSAC, tendrán la responsabilidad de presentar propuestas concretas para abordar esta cuestión".[37]

Al abordar estas preguntas, el equipo responsable del EPDP comenzó con una revisión del asesoramiento legal recibidas durante la Fase 1 y consideró las posibles propuestas que podrían brindar suficientes medidas de protección para abordar las cuestiones indicadas en el memorando legal.

El equipo responsable del EPDP señaló cómo una dirección de correo electrónico anonimizada utilizada tuvo impacto en las medidas de protección necesarias y los posibles impactos sobre los titulares de los datos y, por ende, la factibilidad. El equipo consideró los efectos y beneficios de dos usos de dicho contacto, de acuerdo con los dos objetivos distintos establecidos por aquellos que defienden el uso de contactos únicos, a saber 1) la posibilidad de ponerse en contacto con el registratario de manera rápida y eficaz, y 2) correlación entre las registraciones registradas por el mismo registratario.

El equipo responsable del EPDP también observó que la terminología utilizada en el contexto de este debate podría mejorarse para que sea más precisa. El equipo responsable del EPDP le encargó al Comité de Asuntos Jurídicos la tarea de proponer terminología actualizada y revisar las preguntas aclaratorias que se enviarán a Bird & Bird. El Comité de Asuntos Jurídicos propuso un conjunto de definiciones de trabajo, que se envió al equipo responsable del EPDP el 23 de febrero de 2021 (consulte aquí). Además, el Comité de Asuntos Jurídicos elaboró un conjunto de preguntas de seguimiento que se presentó a Bird & Bird, y Bird & Bird brindó una respuesta el 9 de abril de 2021. El equipo responsable del EPDP consideró este asesoramiento legal en la elaboración de su respuesta a las preguntas del Consejo.

Definiciones

Después de la revisión inicial de la primera pregunta de la carta orgánica, el equipo responsable del EPDP señaló que el término anónimo estaba aplicado erróneamente en esta pregunta. El equipo responsable del EPDP señaló que, para que los datos sean verdaderamente anonimizados en virtud del GDPR, el titular de los datos podría no ser identificable "por el responsable del tratamiento de datos o por cualquier otra persona", ya sea directa o indirectamente. (Consulte el artículo 26 del GDPR) Con este entendimiento, el equipo responsable del EPDP optó por centrar su pregunta en la seudonimización de los datos y, posteriormente, perfeccionó las definiciones en sus preguntas de seguimiento a Bird & Bird.

"Contacto de correo electrónico basado en el registratario" significa "un correo electrónico para todos los dominios registrados por un único registratario [patrocinado por un registrador específico]

[37] https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-2-priority-2-items-10sep20-en.pdf

O [entre registratarios],[38] que tiene el propósito de ser datos seudónimos[39] al ser tratados por partes no contratadas.[40]"[41]

"Contacto de correo electrónico basado en la registración" significa "un correo electrónico de uso único separado para cada nombre de dominio registrado por un único registratario, que tiene el propósito de ser datos anónimos al ser tratados por partes no contratadas". [42]

Tenga en cuenta, sin embargo, que aun cuando se adoptasen estas definiciones, Bird & Bird informó que tanto los contactos de correo electrónico basados en el registratario como aquellos basados en la registración crean "una alta probabilidad de que la publicación o divulgación automatizada de dichas direcciones de correo electrónico sean consideradas como el tratamiento de datos personales".

Información de referencia y observaciones del equipo responsable del EPDP

Al elaborar su respuesta a las preguntas del Consejo, el equipo responsable del EPDP desea recordar al Consejo y a la comunidad en general lo siguiente:

Anexo a la Especificación Temporaria ("Cuestiones importantes para consideración de la comunidad")

- La Especificación Temporaria para los Datos de Registración de los gTLD, según la adoptó la Junta Directiva de la ICANN el 17 de mayo de 2018, incluyó el siguiente texto en el Anexo titulado "Cuestiones importantes para consideración de la comunidad":

[38] El Comité de Asuntos Jurídicos asumió la tarea de revisar las pautas jurídicas recibidas durante la Fase 2 y determinar si se requería más asesoramiento legal. Como asunto inicial, el Comité de Asuntos Jurídicos optó por perfeccionar la terminología utilizada en su pregunta de la Fase 2; en particular, en vez de referirse a "anonimización" y "seudonimización", el Comité de Asuntos Jurídicos acordó usar los términos "contacto de correo electrónico basado en la registración" y "contacto de correo electrónico basado en el registratario" porque el equipo responsable del EPDP señaló que el uso anterior de "anonimización" no estaba en consonancia con la definición de anónimo contenida en el GDPR. En la formación de nuevas definiciones, el Comité de Asuntos Jurídicos señaló que podría existir un contacto basado en el registratario dentro del registrador patrocinador O entre todos los registradores. El Comité de Asuntos Jurídicos determinó, no obstante, que la pregunta respecto de si el contacto basado en el registratario debería existir dentro del registrador patrocinador o entre los registradores era una pregunta sobre política para el equipo responsable del EPDP, no una pregunta sobre asuntos jurídicos para el Comité de Asuntos Jurídicos o para Bird & Bird. En consecuencia, el Comité de Asuntos Jurídicos optó por dejar ambas opciones entre paréntesis y Bird & Bird opinó sobre la legalidad y los riesgos asociados de ambas opciones dentro del memorando de la Fase 2A.

[39] Algunos miembros del equipo responsable del EPDP creen que se debería cambiar seudónimo por anónimo. Sin embargo, debería señalarse que la definición anteriormente suministrada fue incluida en la pregunta a Bird & Bird y en el asesoramiento de dicha firma.

[40] Algunos miembros del equipo responsable del EPDP consideran que se debería cambiar "por partes no contratadas" a por partes que no sean los responsables del tratamiento de datos". Sin embargo, debería señalarse que la definición anteriormente suministrada fue incluida en la pregunta a Bird & Bird y en el asesoramiento de dicha firma.

[41] Algunos miembros del equipo responsable del EPDP sugirieron ampliar la definición para incluir "O [entre los TLD operados por el mismo proveedor de servicios de registro]". Sin embargo, debería señalarse que la definición anteriormente suministrada fue incluida en la pregunta a Bird & Bird y en el asesoramiento de dicha firma.

[42] Algunos miembros del equipo responsable del EPDP consideran que se debería cambiar "por partes no contratadas" a por partes que no sean los responsables del tratamiento de datos". Sin embargo, debería señalarse que la definición anteriormente suministrada fue incluida en la pregunta a Bird & Bird y en el asesoramiento de dicha firma.

"Abordar la factibilidad de exigir 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 cumplan con los requisitos de la sección 2.5.1 del Apéndice A".
A modo de referencia, el Apéndice A, sección 2.5.1 estipula que: "El registrador DEBE proporcionar una dirección de correo electrónico o un formulario web para facilitar la comunicación por correo electrónico con el contacto relevante, pero NO DEBE identificar la dirección de correo electrónico de contacto o al contacto en sí".

Recomendaciones relevantes de la Fase 1 del EPDP

Recomendación 6 de la Fase 1 del EPDP
El equipo responsable del EPDP recomienda que, tan pronto como sea comercialmente razonable, el registrador debe ofrecer al titular del nombre registrado la oportunidad de proporcionar su consentimiento para publicar información de contacto editada, así como la dirección de correo electrónico, en el RDS del registrador patrocinador.

Recomendación 13 de la Fase 1 del EPDP
1) El Equipo responsable del EPDP recomienda que el registrador DEBE proporcionar una dirección de correo electrónico o un formulario web para facilitar la comunicación por correo electrónico con el contacto relevante, pero NO DEBE identificar la dirección de correo electrónico del contacto o el contacto mismo, a menos que, en virtud de la Recomendación n.° 6, el titular del nombre registrado haya dado su consentimiento para la publicación de su dirección de correo electrónico.
2) El equipo responsable del EPDP recomienda que los registradores DEBEN mantener archivos de registro, los cuales no deben contener ninguna información personal y que sí contendrán la confirmación de que se ha producido una transmisión de la comunicación entre el solicitante de divulgación y el titular del nombre registrado, sin incluir el origen, el destinatario o el contenido del mensaje. Dichos registros estarán a disposición de la ICANN para fines de cumplimiento, según sea solicitado. Nada en esta recomendación debe interpretarse para impedir que el registrador tome medidas razonables y apropiadas para evitar el uso indebido del proceso de contacto del registrador.[43]

*Nota: durante las deliberaciones en la Fase 2A, algunos miembros del equipo responsable del EPDP plantearon la cuestión de los formularios web y posibles problemas con el uso de dichos formularios. Se señaló que, si bien la opción de un formulario web es parte de la recomendación 13 de la Fase 1 del EPDP, este requisito es idéntico al contenido en la Especificación Temporaria que está en vigencia desde el 25 de mayo de 2018. Las consultas con la organización de la ICANN indicaron que los formularios web no han sido una fuente significativa de reclamos ni se ha planteado este tema como un problema en el contexto del Equipo para la Revisión de la Implementación que está a cargo de implementar la recomendación de la Fase 1.[44] Algunos miembros consideran que , incluso si se presentan problemas, estos no se encuentran dentro del

[43] Algunos ejemplos de uso indebido podrían incluir, entre otros, a solicitantes que inundan el sistema del registrador con solicitudes de contacto voluminosas e inválidas. Esta recomendación no pretende impedir solicitudes legítimas.
[44] Consulte https://community.icann.org/x/I4GBCQ.

alcance del equipo responsable del EPDP, teniendo en cuenta su competencia limitada. El equipo responsable del EPDP no pudo llegar a un acuerdo sobre cómo proceder respecto de este tema.

Recomendación 14 de la Fase 1 del EPDP
Ante el caso de la registración de un nombre de dominio donde se usa un servicio de privacidad/representación (proxy) "afiliado" (por ejemplo, cuando se enmascaran datos asociados con una persona física), el registrador (y, cuando corresponda, el registro) DEBE incluir los datos completos del servicio de privacidad/representación (proxy) no personales del RDDS como respuesta a cualquier consulta, que también PUEDEN incluir el correo electrónico seudonimizado del servicio de privacidad/representación (proxy) existente.
Consideración de este tema por la Fase 2 del EPDP

El Informe Final de la Fase 2 del EPDP señaló lo siguiente:

"Posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme: El equipo del EPDP recibió asesoramiento legal 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 ahora factible en el marco del GDPR. El Consejo de la GNSO está estudiando la posibilidad de continuar con el trabajo sobre este tema".

Respuestas propuestas por el equipo responsable del EPDP a las preguntas del Consejo

i. Si es factible que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme y, de ser así, si debería ser un requisito obligatorio.
ii. Si es factible, pero no es un requisito obligatorio, qué pautas, si las hubiese, pueden brindar las partes contratadas que desean implementar direcciones de correo electrónico anonimizadas uniformes.

• Respuesta del equipo responsable del EPDP a la pregunta i.

El equipo responsable del EPDP reconoce que puede ser técnicamente factible tener un contacto de correo electrónico basado en el registratario o un contacto de correo electrónico basado en la registración.[45] Ciertas partes interesadas ven riesgos y otras inquietudes[46] que impiden que el equipo responsable del EPDP realice una recomendación de exigir que las partes contratadas hagan que una dirección de correo electrónico basada en el registratario o en la registración esté públicamente disponible en este momento. El equipo responsable del EPDP sí señala que ciertos grupos de partes interesadas han manifestado los beneficios de 1) un contacto de correo

[45] Algunos miembros del equipo responsable del EPDP señalaron que, incluso si fuera técnicamente posible, se deberían considerar otros factores relacionados a los esfuerzos necesarios para implementar dicha función a fin de determinar la factibilidad general.
[46] Por ejemplo, 1) no queda claro que el trabajo que implica implementar dicho concepto se justifique por el beneficio potencial. 2) Además, no queda claro que los objetivos, tal como se presentan, se cumplen de forma eficaz o incluso de la mejor manera al requerir las direcciones de correo electrónico basadas en el registratario o en la registración.

electrónico basado en la registración con el fin de garantizar la posibilidad de ponerse en contacto, ya que se han manifestado preocupaciones con la facilidad de uso de los formularios web y 2) un contacto de correo electrónico basado en el registratario para garantizar la correlación con la registración.[47]

• Respuesta del equipo responsable del EPDP a la pregunta ii.

Recomendación n.° 4

El equipo responsable del EPDP recomienda que las partes contratadas que optan por publicar una dirección de correo electrónico basada en el registratario o en la registración con la intención de que sea seudonimizada en el RDDS de acceso público deberían evaluar el asesoramiento legal obtenido por el equipo responsable del EPDP sobre este tema (consulte Anexo F), así como cualquier otro asesoramiento relevante suministrado por las autoridades de protección de datos pertinentes.

Al evaluar los riesgos, beneficios y medidas de protección asociados con la publicación de una dirección de correo electrónico basada en el registratario o en la registración con la intención de que sea seudonimizada en el RDDS de acceso público, las partes contratadas deberían, al menos, considerar los siguientes aspectos:

- Es probable que tanto las direcciones de correo electrónico basadas en el registratario como aquellas basadas en la registración de personas tengan datos personales (es decir, ningún enfoque crea datos anónimos como se definen en el GDPR). Es probable que estos datos sean datos personales tanto desde la perspectiva del responsable del tratamiento de datos como para terceros.
- Sin embargo, incluso si se consideraran datos personales, el enmascaramiento de las direcciones de correo electrónico brinda beneficios en comparación con la publicación de las direcciones de correo electrónico de registratarios reales, entre ellos: (i) demostrar una técnica para mejorar la privacidad/medida de protección de datos desde el diseño y por defecto (artículo 25 del GDPR); y (ii) una reducción de riesgos relevante al llevar a cabo un análisis de equilibrio de interés legítimo para la divulgación de la dirección de correo electrónico enmascarada a terceros.
- Es probable que, en general, la publicación de una dirección de correo electrónico basada en la registración implique un riesgo menor que la publicación de direcciones de correo electrónico basadas en el registratario debido a la cantidad de información que una parte puede potencialmente vincular a un titular de los datos en función de un contacto de correo electrónico basado en el registratario.
- Tanto para la publicación de direcciones de correo electrónico basadas en el registratario como para la publicación de aquellas basadas en la registración, las partes contratadas deberían adoptar medidas eficaces para mitigar la disponibilidad de detalles de contacto a spammers.

[47] La capacidad de identificar los dominios que registró un registratario en particular es importante para el cumplimiento de la ley y las investigaciones de ciberseguridad de actores maliciosos que frecuentemente registran muchos dominios con fines maliciosos.

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, posiblemente, su aprobación.

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) que tiene 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 a 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 vigente. Para los Dominios de Alto Nivel con Código de País (ccTLD), los operadores de estos TLD establecen sus propias políticas, 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 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", por sus siglas en inglés). 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 gubernamentales multinacionales, organizaciones que se rigen por tratados, y economías diferenciadas. Su función consiste en 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 el EEE.

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

13. Dominios genéricos de alto nivel (gTLD)
"gTLD" se refiere a los dominios de alto nivel del DNS delegados por la ICANN en virtud de un acuerdo de registro que se encuentra en plena vigencia, que no sean 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 tienen un 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 regirse por las políticas de consenso en dicho contrato; y (iii) que eligen, en forma voluntaria, ser miembros del RySG. El RySG puede incluir Grupos de Interés, de conformidad con lo establecido en el Artículo IV. El RySG representa las opiniones del RySG ante el Consejo de la GNSO y 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 de servidores raíz. Al principio, 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. En la actualidad, la ICANN desempeña las funciones de la IANA. Como asociación pública-privada, 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 procesos ascendentes y basados 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 a nivel mundial en la ICANN, 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. Su objetivo 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 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: organizaciones sin fines de lucro que sirven a intereses no comerciales; 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; empresas 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 alternativa 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. Nombre registrado

"Nombre registrado" se refiere a un nombre de dominio dentro del dominio de un gTLD que consiste en dos (2) o más niveles (por ejemplo, john.smith.name) sobre los cuales un operador de registro de gTLD (o una filial o subcontratista de éste que presta servicios de registro) mantiene datos en la base de datos del registro, se encarga de su mantenimiento u obtiene ingresos a partir de dicho mantenimiento. Un nombre en una base de datos de 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 sobre 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 eficaz. Lo 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 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 Organizaciones de Apoyo (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. Política 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 se especificó en un principio 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 fechas de creación y vencimiento de

las registraciones de nombres de dominio, servidores de nombres, 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: Información de referencia

Con posterioridad a la solicitud de algunos miembros del equipo responsable del EPDP, el Consejo de la GNSO solicitó a dicho equipo que continuase trabajando en dos temas, después de la finalización de la Fase 1 y Fase 2 de su trabajo, a saber: 1) la diferenciación de datos de registración de personas jurídicas y físicas, y 2) la posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme.

Datos de personas jurídicas vs. físicas - Instrucciones del Consejo al equipo responsable del EPDP

Personas jurídicas vs. físicas: se espera que el equipo responsable del EPDP analice el estudio realizado por la ICANN (tal como lo solicitó el equipo responsable del EPDP y lo aprobó el Consejo de la GNSO durante la Fase 1), junto con el asesoramiento legal que brindó Bird & Bird, así como los aportes sustanciales proporcionados sobre este tema durante el foro de comentario público sobre el anexo y responda:

i. Si se requieren actualizaciones a la recomendación de la Fase 1 del EPDP sobre este tema ("los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y personas jurídicas, aunque no están obligados a hacerlo");
ii. Qué pautas, si las hubiese, pueden brindarse a los registradores o registros que realizan la diferenciación entre registraciones de personas físicas y jurídicas.

Posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme - Instrucciones del Consejo al equipo responsable del EPDP

Se espera que el equipo responsable del EPDP analice el asesoramiento legal y considere propuestas específicas que proporcionen medidas de protección suficientes para abordar las cuestiones indicadas en el memorando legal. Los grupos que solicitaron más tiempo para considerar este tema, entre los que se incluyen el ALAC, el GAC y el SSAC, tendrán la responsabilidad de presentar propuestas concretas para abordar esta cuestión. Se espera que esta consideración aborde:

i. Si es factible que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme y, de ser así, si debería ser un requisito obligatorio.
ii. Si es factible, pero no es un requisito obligatorio, qué pautas, si las hubiese, pueden brindar las partes contratadas que desean implementar direcciones de correo electrónico anonimizadas uniformes.

Anexo B – Información de referencia general

Información de referencia 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 otros esfuerzos de Procesos de Desarrollo de Políticas de la GNSO, que están abiertos para cualquier persona que desee participar, 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 Grupo de Partes Interesadas de la GNSO, al Comité Asesor Gubernamental (GAC), a la Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO), al Comité Asesor At-Large (ALAC), al 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, se ha invitado a la Junta Directiva de la ICANN y a la Organización de la ICANN a asignar una cantidad limitada 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 en vigencia, 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 de consenso estipulado en los Estatutos de la ICANN".[48] El proceso de desarrollo de políticas de 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.

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 otros esfuerzos de Procesos de Desarrollo de Políticas de la GNSO, que están abiertos para cualquier

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

persona que desee participar, 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 Grupo de Partes Interesadas de la GNSO, al Comité Asesor Gubernamental (GAC), a la Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO), al Comité Asesor At-Large (ALAC), al 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, se ha invitado a la Junta Directiva de la ICANN y a la Organización de la ICANN a asignar una cantidad limitada de coordinadores de enlace para esta iniciativa.

El Consejo de la GNSO votó para adoptar las 29 recomendaciones incluidas en el 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 Organización en la Recomendación 12. Conforme a los estatutos de la ICANN, se llevó 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, está trabajando en la implementación de 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 Consejo de la GNSO aprobó el Informe Final de la Fase 2 durante su reunión celebrada el 24 de septiembre de 2020 por mayoría calificada. El Informe Final establece las recomendaciones del equipo responsable del EPDP para un Sistema Estandarizado de Acceso/Divulgación (SSAD) para los datos de registración de gTLD sin carácter público, así como recomendaciones y conclusiones para los temas denominados con “prioridad 2”, que incluyen, entre otros, la retención de datos y la omisión del campo que especifica la ciudad.

Como parte de su aprobación, el Consejo de la GNSO acordó solicitar una consulta con la Junta Directiva de la ICANN para debatir la sostenibilidad financiera del SSAD y algunas de las preocupaciones manifestadas en las diferentes declaraciones minoritarias, incluida la cuestión de si se debería realizar un nuevo análisis de costo-beneficio antes de que la Junta Directiva de la ICANN considere todas las recomendaciones relacionadas con el SSAD para su adopción.

Durante la reunión ICANN70, la Junta instruyó a la organización de la ICANN que iniciase una Fase de Diseño Operativo (ODP) para las recomendaciones relacionadas con el SSAD; la ODP está en curso actualmente. Para obtener más información sobre la ODP del SSAD, visite la siguiente página.

Dado que la consulta solicitada se relacionaba sólo con las recomendaciones relacionadas con el SSAD, la Junta decidió considerar las recomendaciones con Prioridad 2 de manera independiente y

coordinó un período de comentario público sobre dichas recomendaciones desde diciembre de 2020 hasta enero de 2021. La Junta coordinó otro período de comentario público sobre las recomendaciones relacionadas con el SSAD desde febrero a marzo de 2021.

Con posterioridad a la solicitud de algunos miembros del equipo responsable del EPDP, el Consejo de la GNSO solicitó a dicho equipo que continuase trabajando en dos temas como parte de la Fase 2A, a saber: 1) la diferenciación de datos de registración de personas jurídicas y físicas, y 2) la posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme.

Anexo C – Membresía y asistencia del equipo responsable del EPDP

Miembros y asistencia del equipo responsable del EPDP

Resumen de la actividad de las reuniones:

Reuniones plenarias:

- 42 llamadas plenarias (5 canceladas) durante 53,5 horas de llamadas para un total de 1924,5 horas-persona
- Índice de participación total del 85,3 %

Reuniones del Comité de Asuntos Jurídicos:

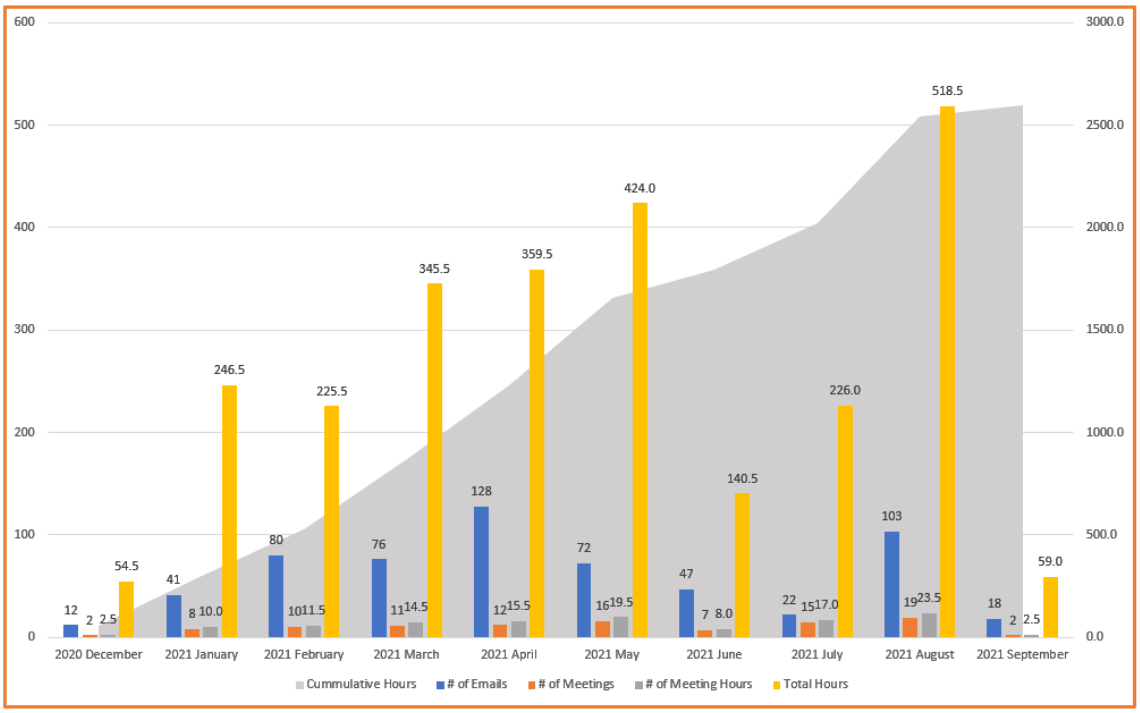
- 11 llamadas de subgrupos durante 17,5 horas de llamadas para un total de 232,5 horas-persona
- Índice de participación total del 89,2 %

Reuniones de equipos pequeños:

- 16 llamadas de subgrupos durante 17,5 horas de llamadas para un total de 180,0 horas-persona
- Índice de participación total del 99,0 %

Reuniones de líderes:

- 51 llamadas del liderazgo durante 39,0 horas de llamadas para un total de 268,5 horas-persona



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/.

El Equipo responsable del EPDP está integrado por las siguientes personas:

Grupo representado / Miembro	Manifestación de Interés (SOI)	Fecha de inicio	Fecha de salida	Asistió %	Función
Comité Asesor At-Large (ALAC)				**98,6 %**	
Alan Greenberg	SOI	15 nov. 2020		97,2 %	
Hadia Elminiawi	SOI	15 nov. 2020		100,0 %	LC
Unidad Constitutiva de Negocios (BC)				**88,9 %**	
Margie Milam	SOI	15 nov. 2020		86,1 %	LC
Mark Svancarek	SOI	15 nov. 2020		91,7 %	
Consejo de la GNSO				**88,7 %**	
Brian Beckham	SOI	18 feb. 2021		86,2 %	Vicepresidente, LC
Keith Drazek	SOI	12 marzo 2020		97,2 %	Presidente, LC
Philippe Fouquart	SOI	26 enero 2021		81,3 %	Coordinador de enlace, LC
Comité Asesor Gubernamental (GAC)				**74,1 %**	
Christopher Lewis-Evans	SOI	19 nov. 2020		88,9 %	
Laureen Kapin	SOI	19 nov. 2020		83,3 %	LC
Melina Stroungi	SOI	20 nov. 2020		50,0 %	LC
Junta Directiva de la ICANN				**73,6 %**	
Becky Burr	SOI	12 nov. 2020		75,0 %	Coordinador de enlace, LC
Matthew Shears	SOI	12 nov. 2020		72,2 %	Enlace
Unidad Constitutiva de Propiedad Intelectual (IPC)				**84,7 %**	
Brian King	SOI	20 nov. 2020		97,2 %	LC
Jan Janssen	SOI	20 nov. 2020		72,2 %	LC
Corporación para la Asignación de Nombres y Números en Internet (ICANN)				**93,1 %**	
Amy Bivins	Manifestación de Interés (SOI)	12 julio 2020		88,9 %	Coordinador de enlace, LC
Brian Gutterman	Manifestación de Interés (SOI)	12 oct. 2020		97,2 %	Enlace
Unidad Constitutiva de Proveedores de Servicios de Internet y Servicios de Conectividad (ISPCP)				**93,1 %**	
Christian Dawson	SOI	15 nov. 2020		94,4 %	
Thomas Rickert	SOI	15 nov. 2020		91,7 %	LC
Grupo de Partes Interesadas No Comerciales (NCSG)				**65,0 %**	
David Cake	SOI	12 marzo 2020		72,2 %	
Manju Chen	SOI	12 marzo 2020		97,2 %	
Milton Mueller	SOI	12 marzo 2020		58,3 %	
Stefan Filipovic	SOI	12 marzo 2020		13,9 %	LC
Stephanie Perrin	SOI	12 marzo 2020		83,3 %	LC
<Vacante>					

Grupo de Partes Interesadas de Registradores (RrSG)				**70,4 %**	
James Bladel	SOI	15 nov. 2020		27,8 %	
Sarah Wyld	SOI	15 nov. 2020		94,4 %	
Volker Greimann	SOI	15 nov. 2020		88,9 %	LC
Grupo de Partes Interesadas de Registros (RySG)				**94,4 %**	
Alan Woods	SOI	15 nov. 2020		91,7 %	LC
Marc Anderson	SOI	15 nov. 2020		97,2 %	
Matthew Crossman	SOI	15 nov. 2020		94,4 %	LC
Comité Asesor de Seguridad y Estabilidad (SSAC)				**98,5 %**	
Ben Butler	SOI	15 nov. 2020	14 ene. 2021	50,0 %	
Steve Crocker	SOI	2 oct. 2021		100,0 %	
Tara Whalen	SOI	15 nov. 2020		100,0 %	LC

LC = participó en el Comité de Asuntos Jurídicos

Los suplentes del equipo responsable del EPDP son:

Grupo representado / Suplente	Manifestación de Interés (SOI)	Fecha de inicio	Fecha de salida	Asistió %	Función
Comité Asesor At-Large (ALAC)					
Holly Raiche	SOI	15 nov. 2020		100,0 %	
<Vacante>					
Unidad Constitutiva de Negocios (BC)					
Steve DelBianco	SOI	15 nov. 2020		93,3 %	
Comité Asesor Gubernamental (GAC)					
Ryan Carroll	SOI	26 ene. 2021		100,0 %	
Velimira Nemiguentcheva-Grau	SOI	26 ene. 2021		100,0 %	
<Vacante>					
Junta Directiva de la ICANN					
León Felipe Sánchez Ambia	SOI	12 nov. 2020		86,7 %	
Unidad Constitutiva de Propiedad Intelectual (IPC)					
<Vacante>					
Unidad Constitutiva de Proveedores de Servicios de Internet y Servicios de Conectividad (ISPCP)					
Suman Lal Pradhan	SOI	15 nov. 2020		100,0 %	
Grupo de Partes Interesadas No Comerciales (NCSG)					
Bruna Santos	SOI	12 marzo 2020		100,0 %	
<Vacante>					
<Vacante>					
Grupo de Partes Interesadas de Registradores (RrSG)					
Matt Serlin	SOI	15 nov. 2020		100,0 %	
Owen Smigelski	SOI	15 nov. 2020		97,0 %	
Theo Geurts	SOI	15 nov. 2020		100,0 %	

Grupo de Partes Interesadas de Registros (RySG)					
Amr Elsadr	SOI	15 nov. 2020		100,0 %	
Beth Bacon	SOI	15 nov. 2020		100,0 %	
Sean Baseri	SOI	15 nov. 2020		100,0 %	
Comité Asesor de Seguridad y Estabilidad (SSAC)					
Greg Aaron	SOI	15 nov. 2020		100,0 %	
<Vacante>					

Los miembros del Equipo de Apoyo del equipo responsable del EPDP son:

Grupo representado / Personal asignado	Manifestación de Interés (SOI)	Fecha de inicio	Fecha de salida	Asistió %	Función
Andrea Glandon		15 nov. 2020			
Berry Cobb		15 nov. 2020			
Caitlin Tubergen		15 nov. 2020			LC
Julie Bisland		15 nov. 2020			
Marika Konings		15 nov. 2020			
Terri Agnew		15 nov. 2020			

Anexo D – Declaraciones minoritarias

Comité Asesor At-Large
Unidad Constitutiva de Negocios
Unidad Constitutiva de Propiedad Intelectual
Comité Asesor Gubernamental
Grupo de Partes Interesadas No Comerciales
Grupo de Partes Interesadas de Registradores
Grupo de Partes Interesadas de Registros
Comité Asesor de Seguridad y Estabilidad

COMITÉ ASESOR AT-LARGE
Informe Final de la Fase 2A del Proceso Expeditivo de Desarrollo de Políticas sobre la Especificación Temporaria para los Datos de Registración de los gTLD

Declaración minoritaria del ALAC

El ALAC reconoce y agradece el trabajo del equipo de la Fase 2A del EPDP, los esfuerzos del presidente, vicepresidente y coordinador de enlace al Consejo de la GNSO, así como la dedicación y los esfuerzos del personal de apoyo de la organización de la ICANN. No obstante, el ALAC considera que la Fase 2A no abordó correctamente su mandato. El resultado neto es que la importancia de los datos de registración para varios miembros de la comunidad, como agencias de protección del consumidor, autoridades responsables del cumplimiento de la ley e investigadores de ciberseguridad, y el rol crucial que desempeñan al proteger diariamente a usuarios de Internet, registratarios, clientes, empresas y toda la población en línea no se abordarán de manera adecuada.

Resulta importante lograr un equilibrio entre la protección de la información personal de los registratarios, y la experiencia y seguridad de los usuarios. La omisión de datos no protegidos por leyes de protección de datos no permite lograr el equilibrio correcto.

En esta declaración minoritaria, el ALAC muestra preocupación sobre los siguientes aspectos de las recomendaciones del Informe Final de la Fase 2A y su impacto en la seguridad de los usuarios diarios de Internet:

- No exigir la diferenciación entre datos de personas jurídicas y físicas,
- No exigir el uso de elementos de datos comunes por todas las partes contratadas,
- Falta de medios para ponerse en contacto con los registratarios
- “Proceso”

No exigir la diferenciación entre datos de personas jurídicas y físicas

El GDPR no protege los datos no personales de las personas jurídicas. Además, la cláusula 14 del GDPR de la Unión Europea que expresa “este reglamento no abarca el tratamiento 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 detalles de contacto de la persona jurídica”.

El EPDP recibió asesoramiento legal de que era razonable permitir que los registratarios se autodesignaran y que, con las pertinentes precauciones, descargos de responsabilidad y capacidades de corrección, existía un bajo riesgo de que las partes así lo hicieran. Esta posición fue respaldada por la carta del EDPB de julio de 2018 a Göran Marby. Este asesoramiento fue ignorado por el EPDP. Si bien la base instalada de 200 millones de registraciones demoraría en ser abordada (por ejemplo, al momento de la renovación), el EPDP ni siquiera recomendó que se realizara la diferenciación de las registraciones nuevas. Más concretamente, incluso el debate de llevar a cabo

dicha acción (tal como fue propuesta por miembros del EPDP del GAC) se desestimó rápidamente a principios de la Fase 2A, en vez de centrarse sólo en el "asesoramiento" que podría ignorarse. Teniendo en cuenta todo lo mencionado anteriormente y que el Servicio de Directorio de Datos de Registración de Nombres de Dominio (RDDS) es un bien público que protege a los usuarios en línea de todo el mundo, y que el GDPR y leyes de privacidad similares son un bien público que protegen los datos de registración de los registratarios, se necesita lograr un equilibrio correcto. No se puede lograr este equilibrio correcto si se omiten más datos de los exigidos por ley y el EPDP no hizo prácticamente ningún esfuerzo para conseguir este equilibrio.

No exigir el uso de elementos de datos comunes por todas las partes contratadas

Los elementos de datos comunes propuestos en la recomendación n.° 1 permiten ochos valores posibles, entre ellos, "No se realizó la distinción del estatus legal" y "No se determinó la presencia de datos personales". Estos estados permiten que las partes contratadas que no realizan la diferenciación usen el campo recién definido. No obstante, el EPDP omitió recomendar que los campos deben ser utilizados, incluso por los registradores que voluntariamente optan por hacer la distinción entre personal jurídica/física o identificar la presencia/ausencia de datos personales. No exigir el uso de los campos, INCLUSO CUANDO hay disponibles datos válidos y útiles, no tiene sentido. Asimismo, el EPDP no designó estos campos como elegibles para divulgación pública, aunque NO contengan información personal.

De acuerdo con las recomendaciones de los informes finales de las fases 1 y 2 del EPDP, las partes contratadas (CP) deben actualizar su servicio de directorio de datos de registración (RDDS) actual.

Exigir el uso de los elementos de datos comunes por las partes contratadas permitiría que todas las CP siguiesen procesos similares en todo el mundo, ya sea que realicen la diferenciación o no, y si están o no sujetas a normas de la UE.

Como resultado, estamos creando un elemento común que nadie tiene la obligación de usar, haciendo fracasar el propósito detrás de la creación de maneras comunes de realizar cosas y abriendo la puerta a la fragmentación.

Falta de medios para ponerse en contacto con los registratarios

El ALAC lamenta que el EPDP no haya llegado a una conclusión sobre metodologías a fin de abordar mejor la anonimización o seudonimización de las direcciones de correo electrónico de contacto. Siendo ese el caso, nos quedamos con las recomendaciones de la Fase 1 que permiten la anonimización, pero, en ausencia de eso, permiten formularios web para contacto. Desde la finalización de la Fase 1, se ha vuelto evidente que algunos registradores (principales) usan el tipo de formulario web que efectivamente no permite ninguna comunicación útil con un registratario. Se dictaminó que esta brecha evidente en las regulaciones estaba fuera de alcance, a pesar de las instrucciones de la GNSO de volver a analizar esta recomendación de la Fase 1. El efecto neto es que, para una parte significativa de la base de registraciones de gTLD, no existe una manera eficaz de establecer comunicaciones con los registratarios.

“Proceso”

El ALAC manifiesta su preocupación de que, a lo largo de este EPDP, el enfoque estuvo puesto exclusivamente en los procesos proyectados y los cronogramas estipulados con un serio impacto en la capacidad de determinar y recomendar una buena política.

A continuación, se presentan algunos ejemplos:

- Plazos que no permiten la deliberación suficiente de consulta con los grupos que respaldan este EPDP
- Definiciones de alcance que determinan que algunas cuestiones están fuera de alcance porque no están explícitamente mencionadas en las instrucciones de la GNSO, pero que permiten que sucedan otras desviaciones (como la recomendación sobre el código de conducta)
- Suspensión del debate sobre diferenciación en favor de “asesoramiento”, con la promesa de retomarla, pero que nunca se ha hecho.
- Estándares de “prueba” inconsistentes que permiten desechar algunos argumentos, mientras que otros siguen en pie.

Parece que existe una reticencia cada vez mayor de las partes contratadas respecto de aceptar CUALQUIER obligación nueva, sin importar los beneficios para otras partes o el bien público. Esto es preocupante para la dirección.

Resumen

La Fase 1 del EPDP determinó que la Fase 2 “determinaría y resolvería la cuestión de persona jurídica versus persona física en la Fase 2”. Esta cuestión se pospuso para la Fase 2A. Claramente, no lo hemos logrado. Además, si bien recomendamos la creación de elementos críticos del RDDS, estamos permitiendo que se ignoren por completo. El ALAC tiene una gran dificultad para etiquetar este esfuerzo como un éxito.

Declaración minoritaria de la Unidad Constitutiva de Negocios de la ICANN sobre el Informe Final de la Fase 2A del EPDP[49]
10 sept. 2021

Introducción

Se presenta esta declaración minoritaria en nombre de la Unidad Constitutiva de Negocios (BC) de la ICANN.[50]

La BC es un ferviente defensor de los derechos de privacidad y la intención protectora del GDPR. Sin embargo, en el contexto del trabajo del equipo responsable del EPDP sobre este Proceso Expeditivo de Desarrollo de Políticas (EPDP) -- un equipo que tenía la instrucción explícita de "preservar la base de datos del WHOIS en la mayor medida posible" mientras cumplía con las leyes de privacidad -- la política resultante supera lo necesario para proteger los datos de personas físicas.

El Consejo de la GNSO le encargó al equipo responsable de la Fase 2A del EPDP la tarea de centrarse en dos temas específicos: 1) la diferenciación de datos de registración de personas jurídicas y físicas y 2) la posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme. Nuestro comentario se centra en la distinción entre persona jurídica y física, la falta de resultados aplicables y, más importante aún, en la necesidad vital de responder al progreso legislativo europeo que impactará en la política desarrollada, o la falta de ello.

Como se indicó anteriormente, la BC cree enfáticamente que la diferenciación opcional entre personas jurídicas y físicas no es adecuada y que la política de la ICANN debe exigir la diferenciación a fin de garantizar la seguridad y estabilidad del DNS global.

En resumen, las recomendaciones de la fase 2A, al no hacer la distinción entre personas jurídicas y físicas, genera una gran cantidad de registros que se editan o que no están disponibles de algún otro modo. Esto es angustiante, e incluso frustrante, dado el predominio reconocido de daños en línea. Dicha frustración fue bien documentada en la encuesta reciente realizada por el Grupo de Trabajo Anti-Abuso de Mensajes, Malware y Móvil (M3AAWG)[51], que detalló las limitaciones sustanciales del acceso actual a los registros de registración de nombres de dominio sin carácter público y afirmó que las soluciones actualmente analizadas por la ICANN no satisfarían las necesidades de los actores responsables del cumplimiento de la ley y ciberseguridad.

Si bien el equipo responsable del EPDP designó sus recomendaciones como respaldadas por "consenso", la BC repite que no respalda los resultados de la Fase 2A, no respalda una designación por "consenso" y aquí brinda la justificación de su disenso.

[49] 3 de septiembre de 2021, Informe Final de la Fase 2A del EPDP, en https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20210903/4c231c0a/EPDPPhase2A-FINALREPORT-3September2021003-0001.pdf

[50] Entre los comentarios anteriores e informe minoritario de la BC sobre la Fase 2 del EPDP se incluyen:
- La BC y la IPC presentaron una declaración minoritaria conjunta para la Fase 2 del EPDP.
- Comentarios de la BC sobre el Informe Inicial de la Fase 2A

[51] https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

Opinión de la BC sobre el Informe Final de la Fase 2A del EPDP

Un precepto fundamental de la misión de la ICANN es establecer políticas de consenso que contribuyan a la seguridad y estabilidad del DNS, y hacer cumplir rigurosamente todas las obligaciones que resulten de dicha política. Sin embargo, la BC observa una tendencia reciente -- en particular, pronunciada en las deliberaciones y los resultados del Grupo de Trabajo de la Fase 2A -- hacia la dependencia de obligaciones "opcionales (por ejemplo, el uso de "debería" y "podría" en la redacción de las recomendaciones) que evita las obligaciones y no se compromete firmemente a mantener la seguridad y la estabilidad. Además, hay una dependencia creciente en la emisión de asesoramiento en vez de políticas vinculantes, lo que deja una latitud significativa para el cumplimiento de las partes contratadas y una política débil, diluida y probablemente no coercitiva. Este es un resultado desafortunado. La BC considera que la comunidad de la ICANN debería dedicar tiempo en políticas que se apliquen a todos los registradores y registros de manera uniforme -- no solamente a un subconjunto indefinido, que actúa a su propio antojo.

De hecho, la BC señala que, aparte de la primera parte de la recomendación n.°1 (que obliga a la ICANN a coordinar con la comunidad técnica para elaborar estándares técnicos para facilitar la diferenciación entre datos de registración de personas físicas y personas jurídicas), el Informe Final de la Fase 2A del EPDP no contiene políticas reales y no asigna obligaciones coercitivas a las partes contratadas. Esto representa un error desafortunado del proceso de múltiples partes interesadas.

La designación de "consenso" del equipo responsable del EPDP para el informe final no refleja las profundas divisiones en los resultados del grupo de trabajo. Resulta evidente que un segmento significativo de los miembros del WG, así como una parte considerable de la comunidad de la ICANN, considera que los resultados de la Fase 2A no son adecuados. Esta división no debería pasarse por alto, a pesar de que el WG insiste en posicionar este informe como uno respaldado por consenso.

Exigencia de la distinción entre personas jurídicas y físicas

Reiteramos que la imposibilidad de los usuarios de Internet de identificar con quién realizan transacciones en línea y la creciente incapacidad de los organismos de cumplimiento de la ley, expertos en ciberseguridad y profesionales del ámbito jurídico de identificar a los actores delictivos en línea a través de sus datos de registración de nombres de dominio, continúan debilitando seriamente el mandato de seguridad y estabilidad de la ICANN. Por ende, los intereses de estos usuarios no se ven reflejados adecuadamente en la política.

La incapacidad del equipo responsable de la fase 2A del EPDP de llegar a un consenso sobre la recomendación de cambios a la recomendación 17.1 de la Fase 1 y su fracaso para "determinar y resolver la cuestión sobre personas jurídicas y físicas" en sus deliberaciones tal como se exigió en la política de la Fase 1, no implican que la política definida en la recomendación 17.1 de la Fase 1 debería perdurar o debería convertirse en la política "por defecto" de la ICANN. De hecho, ocurrió lo opuesto. Debido a que el equipo responsable de la Fase 2A no pudo lograr consenso sobre esta recomendación, creemos que el registro debería indicar que no se logró, y aún no existe, una

opinión consensuada que permita la diferenciación opcional entre personas jurídicas y físicas por parte de los registradores y registros.

Directiva NIS2

La evolución de la Directiva NIS2 indica que el Parlamento Europeo no solo abordará e influirá en la cuestión de la diferenciación entre personas jurídicas y físicas, sino también otra política relacionada con el WHOIS, que incluya la exactitud, los elementos de datos vitales, la publicación oportuna de datos no personales y la respuesta oportuna a los solicitantes de acceso legítimos. La ICANN debería ser muy consciente de que las partes interesadas clave, incluidas las autoridades regulatorias de Europa y Estados Unidos, están supervisando estrechamente la participación del Parlamento Europeo en estas cuestiones mediante la Directiva NIS2. Es probable que surjan opiniones y decisiones por parte de las autoridades regulatorias de privacidad y de los tribunales, lo que podría acelerarse como resultado de los procedimientos relacionados con la NIS2. Es muy posible que el avance de la Directiva NIS2 pueda rápidamente adelantarse al desarrollo de políticas de la ICANN y la ICANN deberá volver a analizar el impacto de dicha directiva una vez adoptada.

Por ende, la ICANN debería verse obligada a responder adecuadamente a la Directiva NIS2 una vez que la Unión Europea la adopte. Eso le brinda tiempo a la ICANN a actualizar sus contratos y políticas antes de que la NIS2 se traslade por primera vez a las leyes de los estados miembro de la UE. Si esto no se hace, probablemente se genere un enfoque de industria fragmentada e inconsistente respecto de las obligaciones de la Directiva.

Recomendación n.° 1

La BC no respalda esta recomendación. Si bien respaldamos una obligación para que la ICANN defina un mecanismo técnico estándar para facilitar la diferenciación entre datos de registración de personas jurídicas y físicas, la BC lamenta la falta de obligaciones para las partes contratadas de usar este campo o incluso de indicar si realizaron la diferenciación. La falta de exigir el uso de este mecanismo técnico no generará un RDDS consistente y confiable, y constituye una oportunidad perdida de reducir la cantidad de solicitudes de datos no personales que fueron omitidos innecesariamente, como los datos de contacto de servicios de privacidad/representación (proxy) no afiliados. Este resultado no llega a satisfacer las necesidades de aquellos que participan en la investigación del uso indebido del DNS, la actividad ciberdelictiva, las violaciones a la propiedad intelectual y otras actividades que amenazan el bienestar de los consumidores.

Como se indicó anteriormente, la BC cree firmemente que la ICANN debe tomar medidas para actualizar la política del EPDP cuando la Directiva NIS2 haya sido adoptada por la Unión Europea.

Recomendación n.° 2

La BC se opone a la recomendación n.° 2 sobre fundamentos procesales y con respecto a su recomendación específica.

En cuanto al aspecto procesal, en contravención con los Estatutos de la ICANN y la carta orgánica del equipo responsable de la Fase 2 del EPDP, el equipo responsable de la Fase 2A del EPDP dedicó tiempo, en forma inexplicable, a elaborar pautas en vez de políticas de consenso vinculantes. En efecto, un subgrupo de los miembros del WG "se quedó sin tiempo"; dedicó la mayor parte de sus esfuerzos a crear pautas y demoró hasta las últimas semanas de la Fase 2A para debatir, de manera significativa y contundente, cómo crear políticas de consenso vinculantes.

El Anexo 2-A de los Estatutos de la ICANN especifica el proceso para la elaboración de pautas, el cual exige el inicio formal de un proceso para la elaboración de pautas por parte del Consejo de la GNSO. Este proceso no se siguió y, en consecuencia, no se pudieron elaborar pautas justificadamente.

Debido a esto, la política definida en la recomendación n.° 2 debería adoptarse como política de consenso y no simplemente como "asesoramiento", y se debería exigir su cumplimiento de manera adecuada.

Con respecto a la información específica de la recomendación, la BC considera que también es débil e no coercitiva, lo que perjudica aún más la posibilidad de usar los datos de registración de nombres de dominio con fines legítimos. La recomendación debería exigir que las partes contratadas sigan los preceptos de la recomendación 2.

Por último, notamos que hay un error en la página 20 del Informe Final, que debería corregirse de la siguiente manera:

"Por lo general, esto permite la publicación ~~divulgación~~ de datos de personas jurídicas porque está fuera de la competencia del GDPR; sin embargo, al tratar datos de personas jurídicas, las partes contratadas deberían implementar medidas de protección a fin de asegurar que la identificación de datos personales sobre una persona física no se publique ~~divulgue~~ dentro de los datos marcados como persona jurídica, ya que esto es un ejemplo de la información que está dentro del alcance del GDPR".

Se necesitan estas aclaraciones para garantizar la consistencia con las recomendaciones del informe de la Fase 1 del EPDP -- a saber, que la información de una persona física ***se puede divulgar cuando así se solicite***, con fines legítimos, siempre que exista un fundamento legal pertinente en virtud del GDPR.

Recomendación n.° 3

La BC observa que esta recomendación no define ninguna obligación coercitiva respecto de ninguna parte específica, ni recomienda el desarrollo de una. La recomendación de que el trabajo sobre un código de conducta "sea considerado" en "todo posible trabajo futuro dentro de la ICANN" es vaga e no coercitiva, y deja prioridades de la comunidad sin atender que merecen una debida atención.

De conformidad, la recomendación debería alentar a la ICANN a comenzar un proceso para

establecer un código de conducta. Si la ICANN lo hiciera, la BC se opondría firmemente a cualquier proceso que no implicase a todas las partes interesadas de la ICANN. La definición y la elaboración de un código de conducta deben ser llevadas a cabo de manera abierta, transparente e inclusiva, y no deben ser elaboradas fuera del proceso de múltiples partes interesadas de la ICANN (por ejemplo, mediante negociaciones privadas entre la organización de la ICANN y las partes contratadas).

Recomendación n.° 4

Fue desafortunado que el equipo responsable del EPDP no dedicase el tiempo adecuado para abordar este tema importante. La BC sigue creyendo que se debería ***exigir*** una dirección de correo electrónico seudónima basada en el registratario para facilitar la investigación del uso indebido del DNS al permitir la posibilidad de ponerse en contacto y de hacer referencia cruzada de las registraciones por parte de los registratarios.

Una vez más, la BC lamenta que esta recomendación no defina ninguna obligación coercitiva a las partes contratadas, lo que deja brechas significativas entre la recomendación y la implementación práctica. Es probable que recomendar que las partes contratadas analicen el asesoramiento legal y evalúen los riesgos, beneficios y medidas de protección resulte en una política excesivamente cautelosa, débil y, en última instancia, ineficaz.

Los autores de este comentario son Alex Deacon, Margie Milam, Steve DelBianco, Mark Svancarek, Drew Bennett y Mason Cole. Fue aprobado de conformidad con nuestra carta orgánica.

Declaración minoritaria de la IPC sobre la Fase 2A del EPDP

Las leyes de protección de datos, incluido el GDPR, no se aplican a datos no personales. De hecho, si bien el GDPR es, sin duda alguna, un poco ambiguo, podría incluso no aplicarse a datos personales pertenecientes a entidades legales.[52] En consecuencia, las bases de datos como el WHOIS/RDDS, que sirven a una multitud de propósitos del interés público, deberían omitir sólo los datos que sean datos que pueden demostrarse que son personales, que requieren un tratamiento distinto debido a las leyes de protección de datos. Sin embargo, la Fase 2A del EPDP, de manera inexplicable e inadecuada, trasladó la "carga de la prueba", o al menos la "carga de la persuasión" a aquellos que defienden el resultado del sentido común: no se deberían ocultar los datos no personales. La Unidad Constitutiva de Propiedad Intelectual (IPC) señala que la Fase 2A del EPDP comenzó su trabajo con el pie equivocado al asumir esta carga inadecuada y al intentar brindar asesoramiento en vez de crear políticas de consenso vinculantes. Este no es el rol del Proceso de Desarrollo de Políticas (PDP) - que está diseñado para elaborar políticas de consenso que sean vinculantes de manera equitativa para todas las partes contratadas. Asimismo, la IPC señala una tendencia preocupante en el desarrollo de políticas multisectorial a lo largo de las numerosas fases del EPDP: es posible tener poco éxito cuando algunas partes interesadas sólo desean actuar exclusivamente en pos de sus propios intereses con poca consideración del compromiso en pos del bien común. Ahora más que nunca, debemos reunir a nuestras partes interesadas en pos de la seguridad, estabilidad y flexibilidad del DNS y "promover el interés público global", como se establece en las actas constitutivas de la ICANN. Por último, notamos que la designación de "consenso" atribuida a las recomendaciones de la Fase 2A del EPDP refleja inadecuadamente la división dentro del grupo de trabajo en estos resultados y no refleja que la recomendación 17.3 de la Fase 1 del EPDP, "El Equipo responsable del EPDP determinará y resolverá el asunto de personas físicas vs. jurídicas en la Fase 2", sigue sin resolverse sin un requisito para realizar la diferenciación.

A continuación, se muestran comentarios específicos sobre la Fase 2A del EPDP.

I. Basarse en la autoidentificación de los registratarios

Una de las mayores decepciones por sentido común en las recomendaciones de la Fase 2A del EPDP es el concepto de que no debería exigir a las partes contratadas basarse en lo que les expresa un registratario sobre la naturaleza de los datos del RDS, y publicar u omitir los datos en consecuencia. El asesoramiento legal confirmó esta evaluación de sentido común, que denomina a los datos "baja sensibilidad", al riesgo "bajo", y que, incluso en el caso de una publicación errónea basada en una autodesignación incorrecta del registratario, "una orden para corregir el problema (probablemente acompañada por un período razonable durante el cual se deban implementar los cambios), en vez de una multa, parece más probable, y "no se encuentran ejemplos de acciones para el cumplimiento efectivo al respecto".[53]

[52] "Esta regulación no abarca el tratamiento 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". Cláusula 14 del GDPR

[53] https://community.icann.org/display/EOTSFGRD/EPDP+-P2A+Legal+subteam

Basándose en el fundamento de dicho asesoramiento jurídico, un grupo que realmente trabaja en pos del interés público debería haber acordado con facilidad publicar datos identificados por el titular de los datos como datos no personales. Y aún, no surgió un acuerdo de ese tipo.

II. Elementos de datos comunes

La IPC claramente respalda el desarrollo de uno o varios elementos de datos comunes para reflejar si los datos del RDS pertenecen a un registratario que es una entidad jurídica o una persona física, o si los datos en sí contienen datos personales. Si bien no es sorprendente como el resultado más impactante de la Fase 2A, la IPC respalda y valora que el modelo de múltiples partes interesadas llegue a un consenso sobre este elemento de datos estandarizado.

Dicho eso, la IPC y colegas de otras unidades constitutivas y comités asesores creen firmemente que dicho elemento de datos estandarizado debería ser obligatorio, en especial, ante la falta de publicación de datos con sentido común de acuerdo con la representación del registratario. Si bien el acuerdo nos alienta a elaborar este elemento de datos, dudamos del impacto probablemente positivo de este compromiso si dicho elemento de datos nunca logra el uso generalizado por las partes contratadas. De hecho, la IPC está realmente decepcionada y desanimada respecto de que el equipo de la Fase 2A no pudo acordar sobre cualquier uso mayor de este elemento de datos. Las posibilidades variaban desde la recopilación opcional para dominios nuevos sólo hasta la recopilación y publicación obligatorias del campo para todos los dominios bajo gestión. Incluso, el mínimo esencial - recopilación opcional -- fue el único resultado con la posibilidad de obtener consenso. Esto es muy decepcionante dado que el campo en sí no implica datos personales y, por lo tanto, no hay ningún riesgo de publicarlo. Además. las partes contratadas nunca dieron un motivo para oponerse a la recopilación o publicación obligatoria de este elemento de datos. Simplemente repitieron “no vemos el valor” (presumiblemente para ellos como registros y registradores) cuando presentaron el fundamento suministrado por las partes no contratadas, que incluye: utilidad para el SSAD, indicación de si presentar una solicitud del SSAD o una solicitud individual del registro/registrador, información sobre si se omitieron los datos por una causa o por conveniencia de la parte contratada, entre otros motivos.

III. Trabajo futuro sobre el código de conducta

Por último, si bien estaba posiblemente fuera del alcance de esta Fase 2A del EPDP, el Informe Final contiene una cláusula que requiere que la ICANN considere el asesoramiento que se presente en todo acuerdo futuro con el Comité Europeo de Protección de Datos sobre un código de conducta. Como asunto inicial, la recomendación es débil en cuanto a que no exige realmente la creación de un código de conducta. Además, la recomendación está redactada de manera ambigua para incluir encargados y responsables del tratamiento de datos, con una oración separada que alude a “la comunidad”. Algo más preocupante es que, cuando la IPC insistió en que el Informe final aclarase que los grupos que representan a los solicitantes de datos del RDS sean incluidos explícitamente como encargados o responsables del tratamiento de datos (para sus propios fines), algunas partes contratadas se opusieron, haciendo referencia a los solicitantes como “intereses de terceros”. En el

entorno multisectorial de la ICANN, la comunidad, en particular, la diversa comunidad representada en la GNSO, no debe ser relegada al estado de "observador" sobre algo que tiene tanto impacto como el estado legal de los datos del RDS que es tan fundamental para la seguridad, estabilidad y flexibilidad del DNS.

IV. Dirección de correo electrónico seudónima basada en el registratario

La IPC sigue creyendo que se debería publicar una dirección de correo electrónico seudónima basada en el registratario de manera obligatoria en el WHOIS/RDDS. El asesoramiento legal obtenido por el equipo responsable de la Fase 2A del EPDP identificó el riesgo de dicha publicación como "moderado", dado que dichos datos podrían usarse para identificar a un registratario que es una persona física cuando se combinan con otros datos personales. No obstante, los beneficios de interés público de dicha publicación superan los derechos de privacidad del titular de los datos ya que la capacidad de usar direcciones de correo electrónico seudonimizadas basadas en el registratario es vital para facilitar la correlación de titularidad entre dominios a fin de enfrentar grandes redes de amenazas a la seguridad, esquemas de phishing y sitios que infringen la propiedad intelectual. Notamos que la publicación de direcciones de correo electrónico basadas en el registratario parecería cumplir con e GDPR y notamos que varias entidades europeas en la cadena de suministro del DNS en realidad publican las direcciones de correo electrónicas *reales* del registratario sin entrar en conflicto con el GDPR, según se señala en el asesoramiento legal brindado al EPDP.[54] En el caso de que el Comité Europeo de Protección de Datos o una Autoridad de Protección de Datos individual considere que este enfoque no cumple con el GDPR, la política se puede revertir al requisito actual de publicar una dirección de correo electrónico anonimizada o un enlace al formulario web, con la divulgación de la dirección de correo electrónico real en respuesta a solicitudes válidas de terceros.

V. Conclusión

En conclusión, si bien la IPC respalda el consenso alcanzado para crear un elemento de datos estandarizado que refleje la naturaleza (jurídica vs. física) del registratario o los datos de registración, el Informe Final de la Fase 2A del EPDP no cumple su objetivo principal. La recomendación 17.3 de la Fase 1 del EPDP exigía que, además de la diferenciación opcional, "El equipo responsable del EPDP determinará y resolverá el asunto de personas físicas vs. jurídicas en la Fase 2". Lamentablemente, este tema aún no se resolvió. La exigencia de la ICANN de coordinar con la comunidad técnica en la creación de un elemento de datos que las partes contratadas tienen la opción de ignorar no llega de ningún modo a "resolver" la cuestión de personas jurídicas vs.

[54] "En su base de datos del WHOIS, el Registro Europeo de Dominios de Internet (EURid) publica las direcciones de correo electrónico de registratarios de nombres de dominio en el TLD .eu (tanto personas físicas como jurídicas).... De manera similar, si bien el RIPE-NCC se basa en el consentimiento para publicar información personal sobre contactos técnicos/administrativos, publica la información personal sobre los titulares de recursos basándose en el fundamento de que 'facilitar la coordinación entre los operadores de redes es el propósito principal que justifica la publicación de datos personales en la base de datos del RIPE-NCC y de que es evidente que el tratamiento de los datos personales que hacen referencia a un titular de recursos es necesario para el que el registro desempeñe su función, la cual se lleva a cabo en pos del interés legítimo de la comunidad de RIPE y el funcionamiento sin problemas de Internet a nivel mundial (y, por ende, está en conformidad con el artículo 6.1.f del GDPR)'". Memorando de Bird & Bird del 27 de abril de 2021, Informe Inicial del equipo responsable de la Fase 2A del EPDP en 56-57.

personas físicas. Y la falta de exigencia de realizar la diferenciación de datos personales y no personales no cumple con el objetivo primordial del EPDP de “preservar la base de datos del WHOIS en la mayor medida posible” mientras se acatan las leyes de privacidad.

Informe minoritario del Comité Asesor Gubernamental sobre el Informe Final de la Fase 2A del Proceso Expeditivo de Desarrollo de Políticas (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 y comentario general

El GAC valora el tiempo considerable y el compromiso que demostró el equipo responsable de la Fase 2A del EPDP, su liderazgo y el personal de apoyo de la ICANN para desarrollar estas recomendaciones de políticas complejas e importantes respecto del tratamiento de datos de registración de nombres de dominios de entidades jurídicas y contactos de correo electrónico seudonimizados. Si bien el GAC reconoce la utilidad de muchos componentes de las recomendaciones finales, el GAC sigue preocupado respecto de que casi ninguna de las recomendaciones finales crea obligaciones coercitivas. Por lo tanto, no cumplen con las expectativas del GAC respecto de las políticas que requerirían la publicación de los datos de registración de nombres de dominio que no están protegidos en virtud del Reglamento General de Protección de Datos (GDPR) de la Unión Europea, y crearían un marco adecuado para alentar la publicación de contactos de correos electrónicos seudonimizados con medidas de protección adecuadas.

A modo de contexto, tal como resaltó el GAC en aportes anteriores,[55] los organismos responsables del cumplimiento de la ley, protección del consumidor y otros que tienen la tarea de proteger al público de acciones maliciosas facilitadas por el DNS, necesitan acceso rápido y eficaz a los datos de registración de nombres de dominio. Hasta mayo de 2018, dicho acceso estaba a disposición del público mediante el sistema WHOIS. En respuesta al GDPR, la ICANN implementó políticas que permiten el enmascaramiento de muchos de estos datos, incluso datos no protegidos por el GDPR. Dado que el GDPR no protege la información de contacto de las personas jurídicas, muchos grupos de partes interesadas, incluido el GAC, cuestionaron el motivo por el cual las políticas de la ICANN permitían la omisión de información no protegida en los resultados del RDS/WHOIS. Por lo tanto, el GAC y otros grupos de partes interesadas insistieron en el desarrollo de políticas más precisas que protejan los datos personales y, a la vez, se publiquen los datos no personales, incluidos los datos de registración relacionados con entidades jurídicas, reconociendo así que la publicación de datos de registración de nombres de dominio no protegidos beneficia al interés público.

El alcance del trabajo de la Fase 2A del EPDP hizo un seguimiento de estas inquietudes y se centró en dos temas, a saber:

1. la diferenciación de los datos de registración de personas jurídicas vs. físicas, y

[55] Consulte los aportes del GAC sobre el Informe Final de la Fase 1 del EPDP (20 de febrero de 2019), Aportes del GAC sobre el Informe Inicial de la Fase 2 (24 de marzo de 2020), y comentario del GAC sobre el Anexo al Informe Inicial de la Fase 2 (5 de mayo de 2020). Consulte también el Comunicado del GAC pronunciado en Abu Dabi (1 de noviembre de 2017), Comunicados del GAC pronunciados en San Juan (15 de marzo de 2018) y Comunicado del GAC pronunciado en Barcelona (25 de octubre de 2018).

2. la posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada[56] uniforme.

Con respecto al primer tema, las preguntas abordadas fueron las siguientes:

i. Si se requieren actualizaciones a la recomendación de la Fase 1 del EPDP sobre este tema ("los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y personas jurídicas, aunque no están obligados a hacerlo");[57]
ii. Qué pautas, si las hubiese, pueden brindarse a los registradores o registros que realizan la diferenciación entre registraciones de personas físicas y jurídicas.

Con respecto al segundo tema "posibilidad de que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme", el equipo responsable del EPDP abordó las preguntas siguientes:

i. Si es factible que los contactos únicos tengan una dirección de correo electrónico anonimizada uniforme y, de ser así, si debería ser un requisito obligatorio; y
ii. Si es factible, pero no es un requisito obligatorio, qué pautas, si las hubiese, pueden brindar las partes contratadas que desean implementar direcciones de correo electrónico anonimizadas uniformes.

El GAC considera que las recomendaciones finales de la Fase 2A brindan varios componentes constructivos, entre ellos:

1. la creación de campos de datos para marcar/identificar a los registratarios que son personas jurídicas y a los datos personales;
2. pautas específicas sobre las medidas de protección que se deberían aplicar para proteger la información personal al realizar la diferenciación entre registraciones de nombres de dominio de personas jurídicas y físicas;
3. apoyo para la creación de un código de conducta que incluya el tratamiento de los datos de registratarios de nombres de dominio de entidades jurídicas;
4. apoyo para que la GNSO siga los desarrollos legislativos que pueden requerir revisiones a las recomendaciones de políticas actuales, y
5. contexto y pautas útiles para aquellos que desean publicar correos electrónicos seudonimizados.

Sin embargo, las recomendaciones finales no son suficientes porque, ante todo, proponen acciones opcionales en vez de acciones obligatorias, incluso cuando se aplican a información no protegida en virtud del GDPR, como los datos no personales de entidades jurídicas. Las acciones opcionales pueden generar un sistema fragmentado e incierto para los solicitantes y titulares de los datos, con diferentes políticas entre los diferentes registradores para la forma en que se protegen o divulgan los datos.[58]

[56] El equipo responsable del EPDP posteriormente concluyó que el término "seudonimizado" era el término más preciso. Consulte "Definiciones" en la pág. 24 del Informe Final de la Fase 2A del EPDP.
[57] Consulte la recomendación 17 contenida en el Informe Final de la Fase 1 del EPDP en: https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf.
[58] El GAC manifestó sus preocupaciones respecto de las políticas que pueden generar fragmentación en aportes anteriores, incluso en el Comunicado del GAC pronunciado en Barcelona (25 de octubre de 2018). Consulte también declaración minoritaria del GAC sobre el Informe Final de la Fase 2 del EPDP sobre datos de registración de gTLD (24 de agosto de 2020).

A modo de referencia, un porcentaje importante de nombres de dominio son registrados por entidades jurídicas y el GDPR, por lo general, no protege sus datos no personales de registración de nombres de dominio. Algunos análisis muestran que un conjunto mucho mayor de información de registración fue omitido en comparación con lo que se exige en el GDPR, es decir "quizá cinco veces más de lo necesario".[59] En efecto, los datos disponibles sugieren que solo aproximadamente el 11,5 % de los dominios pueden pertenecer a personas físicas que están sujetas al GDPR, mientras que los datos de contacto del 57,3 % de todos los dominios fueron omitidos.[60] Este enmascaramiento posiblemente innecesario de grandes cantidades de datos de registración impide muchos de los beneficios asociados con la transparencia respecto de la titularidad de los nombres de dominio.

Con respecto al tratamiento de los datos de personas jurídicas, el GAC considera que se debería exigir dicha diferenciación por muchos de los diferentes motivos (manifestados a continuación) que benefician al público.

En primer lugar, la publicación de datos de registración de nombres de dominio de entidades jurídicas aumentaría la información disponible para las entidades encargadas de proteger al público. Dado el predominio de delitos basados en Internet, la publicación de los datos de registración de entidades jurídicas ayudaría a los organismos responsables del cumplimiento de la ley, protección del consumidor y profesionales en ciberseguridad a investigar más rápida y eficazmente actividades ilícitas facilitadas por el DNS, incluidos los esfuerzos para combatir el ciberdelito. Asimismo, la publicación permite a los organismos responsables del cumplimiento de la ley o los Equipos Nacionales de Respuesta ante Emergencias Informáticas 1) identificar con rapidez la jurisdicción/ubicación de las empresas que son víctimas de ciberdelitos y 2) proporcionar, a gran escala, notificaciones y mensajes de protección a las entidades jurídicas en el caso de que sus dominios se hayan visto comprometidos.

En segundo lugar, exigir que los registradores publiquen los datos de registración de nombres de dominio de entidades jurídicas reduciría considerablemente la cantidad de solicitudes de divulgación de datos de registración de nombres de dominio y los obstáculos asociados con la obtención de respuestas a la divulgación,[61] porque el conjunto de datos ya estaría públicamente disponible. En tercer lugar, hacer que los datos no personales estén disponibles al público generalmente aumenta la confianza en el DNS, ya que brinda transparencia en cuanto a la titularidad de los nombres de dominio, incluso aquellos dominios que facilitan comunicaciones y transacciones en línea sensibles.

[59] Consulte el resumen ejecutivo del Estudio sobre la disponibilidad de los datos de contacto del WHOIS y la clasificación de los registratarios (25 de enero de 2021) en https://www.icann.org/en/system/files/correspondence/chapin-to-botterman-25jan21-en.pdf.

[60] Ibidem

[61] Consulte la sección 5.3.1 del Informe preliminar del Equipo de Revisión de RDS (31 de agosto de 2018) y la encuesta conjunta del Grupo de Trabajo Anti-Abuso de Mensajes, Malware y Móvil y del Grupo de Trabajo Anti-Phishing (18 de octubre de 2018).

Por último, el asesoramiento legal recibido hace hincapié en los bajos riesgos asociados con los datos de registración de entidades jurídicas. En la medida en que se incluya la información personal en los datos de registración de entidades jurídicas, es probable que sean de "baja sensibilidad" porque se relacionan con los detalles laborales de un empleado y no con su vida privada.[62] Además, si se siguen las medidas de protección adecuadas, los riesgos legales asociados con dicha publicación, incluso en el caso de errores accidentales, parecen ser bajos.[63]

En **resumen**, seguimos pensando que un proceso de diferenciación por las partes contratadas entre datos de personas jurídicas y datos de personas físicas debe ser obligatorio. El Informe Final no refleja suficientemente los diversos intereses en juego en el debate sobre la diferenciación y la posterior publicación de información no protegida. El GAC considera que el interés público tiene más importancia que las preocupaciones comerciales, en particular, porque la información públicamente disponible promovería la estabilidad, seguridad, estabilidad y flexibilidad del DNS.

Los comentarios siguientes identifican inquietudes específicas respecto de las recomendaciones finales.

Recomendación n.° 1 Campos para facilitar la diferenciación entre datos de registración de personas jurídicas y físicas

El GAC insistió en la creación y el uso de campos de datos para marcar a los registratarios que son personas jurídicas, y la presencia o ausencia de información personal en sus juegos de datos. Dichos mecanismos de marcado suministrarían el primer paso necesario para la diferenciación. La recomendación n.° 1 incluye varias obligaciones con respecto a la creación de campos para facilitar la diferenciación entre los datos de registración de personas jurídicas y físicas, y para identificar si esos datos de registración contienen datos personales o no personales. Además de crear estos campos, existen otras obligaciones:

- para la ICANN, la obligación de coordinar con la comunidad técnica, por ejemplo, el RDAP WG, a fin de elaborar los estándares necesarios asociados con dichos campos;
- para el SSAD, en consonancia con las recomendaciones de la Fase 2 del EPDP, la obligación de ser compatible con los campos a fin de facilitar la integración entre el SSAD y los sistemas de las partes contratadas; y
- para los campos, la obligación de ser compatibles con los valores específicos relacionados con el estado de las personas jurídicas, y la presencia o ausencia de datos personales.

El GAC especialmente valora la precisión de esta recomendación por especificar exactamente los valores que se deberían incluir en estos campos. No obstante, el GAC cree que la recomendación 1 sería más eficaz en la creación de la infraestructura necesaria para la diferenciación si:

1. exigiera a las partes contratadas no solo crear sino también usar estos campos;
2. brindara plazos específicos para que estos campos se implementen y estén operativos; y

[62] Consulte el memorando de Bird & Bird del 6 de abril de 2021.
[63] Ibidem

3. garantizara que los campos funcionen dentro de los sistemas actuales y contemplados para la recopilación y divulgación de datos.

Para mayor claridad, el GAC piensa que exigir que las partes contratadas completen estos campos para todas las registraciones futuras, independientemente de si las partes contratadas optan por realizar la diferenciación en el tratamiento de los datos de personas físicas y jurídicas, es eficiente y en pos del interés público, porque ofrecería un fundamento para marcar e identificar los datos que pueden ser objeto de futuras solicitudes expeditivas del SSAD o futuras obligaciones legales.[64]

El GAC también señala que el uso voluntario de dicho campo no está en consonancia con las fases anteriores del EPDP donde medidas tales como ediciones de datos se aplicaban a todo el sistema en vez de basarse en decisiones de las partes contratadas individuales.

Recomendación n.°2 Pautas para las partes contratadas que optan por la diferenciación

El equipo responsable del EPDP creó las pautas para la diferenciación en función de los principios aplicables del GDPR y el extenso asesoramiento legal. En particular, el asesoramiento legal identificó medidas de protección muy específicas para mitigar el riesgo de la divulgación injustificada y observó que, en cualquier caso, los datos implicados no eran tan sensibles como otras categorías de información personal porque se relacionaban con el trabajo y no con la vida privada. Por último, el asesoramiento legal observó que, si se siguieran las medidas de protección, aun así, sería poco probable que la divulgación accidental de información personal resultase en una acción coercitiva. Dado que las pautas adoptaron las medidas de protección recomendadas, los riesgos de responsabilidad resultantes son bajos y, como se analizó anteriormente, los beneficios para el público son altos.

Por los motivos identificados más arriba en el presente, el GAC considera que la recomendación debería haber exigido que las partes contratadas diferenciaran entre personas jurídicas y físicas, y, en consecuencia, debería haber exigido también que las partes contratadas aplicasen las pautas pertinentes identificadas en la recomendación 2 y publicaran todos los datos no personales de entidades jurídicas en los datos disponibles públicamente. El GAC también considera que es más adecuado hacer referencia a las medidas reflejadas en la recomendación 2 como “Mejores prácticas”.

Recomendación n.° 3 Códigos de conducta y escenarios de ejemplo.

El GAC acepta la recomendación del equipo responsable del EPDP respecto de que las pautas del equipo establecidas en la recomendación 2 deberían ser consideradas en todo posible trabajo futuro dentro de la ICANN por los responsables y encargados del tratamiento de datos pertinentes en relación con el desarrollo de un código de conducta del GDPR. El GAC señala que las partes

[64] A este respecto, el GAC recibe con agrado el apoyo del Informe Final a la GNSO para evaluar si es necesario llevar a cabo futuros trabajos en materia de políticas en virtud de los avances legislativos. Por ejemplo, el EPDP señaló los debates actuales y la adopción prevista de la Directiva Revisada sobre Seguridad de las Redes y los Sistemas de Información (“NIS2”). Consulte “Propuesta al Consejo de la GNSO” en la pág. 15 del Informe Final de la Fase 2A del EPDP.

interesadas afectadas por dicho código deberían tener la oportunidad de participar en la elaboración del código, incluidos los posibles solicitantes (y, por ende, posibles encargados del tratamiento de datos) de datos de registración de nombres de dominio.

El GAC también acepta las pautas proporcionadas en los escenarios específicos. El GAC considera que se debería mejorar la lógica y la claridad de estos tres escenarios si se exigiese la publicación o no divulgación bajo los escenarios aplicables. Cada escenario establece condiciones específicas que lógicamente exigen la publicación o no divulgación de datos de registración de nombres de dominio y, por ende, la palabra "debería" tiene que ser reemplazada por "debe".

Recomendación n.° 4 Direcciones de correo electrónico seudonimizadas

En relación a los contactos únicos y direcciones de correo electrónico seudonimizadas, el GAC acepta los pasos para brindar pautas sobre publicar una dirección de correo electrónico mediante el método de protección de datos de usar técnicas de anonimización y señala los niveles reducidos de riesgo que esto proporciona a la publicación, tal como se señala en los memorandos legales recibidos por el equipo responsable del EPDP.[65] Si bien el GAC reconoce que existen ciertos riesgos relacionados con la publicación de información seudonimizada, la cláusula 28 del GDPR destaca el uso de la seudonimización como un método para reducir estos riesgos para los titulares de los datos y ayudar a que los encargados y responsables del tratamiento de datos cumplan con sus obligaciones relacionadas con la protección de datos. Además, los correos electrónicos seudonimizados son muy usados por los servicios de privacidad/representación (proxy) con poco e incluso ningún impacto en muchos titulares de los datos. El GAC también destaca los beneficios que dicha publicación de correos electrónicos seudonimizados brindaría, en particular, respecto de permitir comunicaciones rápidas y eficaces con los registratarios de nombres de dominio. Hubo informes de que ciertos formularios web no constituyeron mecanismos eficaces para ponerse en contacto con los registratarios.

[65] Consulte el memorando de Bird & Bird del 9 de abril de 2021 sobre Opciones para el enmascaramiento de direcciones de contacto y el memerando de Bird & Bird del 4 de febrero de 2020 sobre Preguntas sobre un Sistema Estandarizado de Acceso/Divulgación ("SSAD), privacidad/representación (proxy) y correos electrónicos seudonimizados.

Declaración minoritaria del NCSG sobre el Informe Final de la Fase 2A del EPDP

El Grupo de Partes Interesadas No Comerciales (NCSG) está complacido de ver que se completaron las tareas finales de las Fases 1 y 2 del EPDP. También nos alegramos de que la ICANN finalmente cumple con las leyes de protección de datos, algo que estamos solicitando desde los primeros días de los debates sobre políticas del WHOIS. Sin embargo, el proceso para este EPDP ha sido largo y difícil sin necesidad y no refleja la gratitud por la responsabilidad de la ICANN de cumplir con las leyes de protección de datos sino, en cambio, la dificultad de hacer que muchas partes interesadas adopten el concepto de respeto por los derechos de los registratarios. Asimismo, pensamos que la proliferación de declaraciones minoritarias, que manifiestan posiciones argumentadas en forma repetitiva durante al menos los últimos nueve meses, o quizá durante los últimos tres años, es innecesaria. No obstante, no es la intención del NCSG basarse en el principio y rechazar el replanteo de nuestros propios argumentos.

En repetidas ocasiones, hemos mencionado los derechos del registratario. Por lo general, estuvimos solos remarcando los derechos del registratario; se deberían haber unido al menos el ALAC, el SSAC y el GAC, que tienen roles claros en la representación de los derechos de los registratarios. Afortunadamente, las partes contratadas también respaldan a sus clientes y señalaron sus propias obligaciones para con ellos en forma periódica. La ICANN también debería remarcar los derechos de los clientes en su rol de intermediario neutral del acuerdo multisectorial para administrar los gTLD.

La falta de claridad sobre el rol de la organización de la ICANN como responsable del tratamiento de datos en una relación de corresponsables del tratamiento de datos también ha enturbiado las cosas, lo que hizo más complejo imaginar la política. Con frecuencia, hemos manifestado que se debería haber aclarado la naturaleza precisa de los roles de la ICANN y las partes contratadas, sin duda con la ayuda de un asesor jurídico externo, desde el principio de este esfuerzo. La naturaleza de los acuerdos de corresponsables del tratamiento de datos es importante; se habría ahorrado más tiempo y evitado confusiones, si hubiésemos conocido más estas eventuales relaciones contractuales.

Varias partes han planteado la cuestión de reglamentaciones preliminares en Europa, lo que puede impactar en la aplicación del GDPR, y esto ha ralentizado el procedimiento. Nuestra posición es que no deberíamos intentar modificar el trabajo logrado en las primeras dos fases de este EPDP, en función de la especulación sobre posibles reglamentaciones. Una vez más, el deseo de frenar la implementación del GDPR años antes que dichas reglamentaciones se implementasen y presentasen en leyes nacionales, indica que no se valoran las leyes de protección de datos ni los derechos de privacidad de los registratarios.

Con respecto a las cuestiones precisas abordadas en este informe, hemos remarcado, a lo largo de este EPDP y en un PDP anterior sobre servicios de privacidad/representación (proxy), que la distinción entre personas jurídicas y físicas no resulta útil, al momento de decidir sobre la necesidad de proteger los datos en el RDS. Como manifestamos varias veces, se formuló la pregunta incorrecta, porque muchos trabajadores empleados por una persona jurídica o compañía tienen

derechos de privacidad con respecto a la divulgación de su información personal y sus datos de contacto. La persona jurídica no goza de derechos de privacidad, pero las personas sí. Incluso si a continuación de la pregunta de 'persona jurídica versus persona física', colocamos una pregunta aclaratoria que exija que el registratario testifique que no se incluye información personal en los datos suministrados, esto, de ningún modo, elimina los riesgos de divulgar información personal. Ambas preguntas son difíciles de responder para muchas organizaciones, en particular, las organizaciones que el NCSG representa, entre ellas, organizaciones sin fines de lucro, organizaciones de voluntarios, clubes y grupos de interés, grupos religiosos, organizaciones de derechos humanos, etc.

Esto también sucede con los contratistas independientes, algunas clases de profesionales y trabajadores por proyecto que son tratados como contratistas, pero, en realidad, funcionan en una relación de empleador/empleado. Mientras que, para las corporaciones con equipos de asuntos jurídicos, incluso aquellas con operaciones extensas a nivel mundial, es sencillo garantizar que pueden responder esa pregunta, no es sencillo para entidades más pequeñas con presupuestos más acotados y una manera no corporativa de participación con sus voluntarios y miembros.

Por lo tanto, nuestra posición es que, debido a que la distinción no es muy clara para muchas entidades, no es práctico o recomendable exigir la diferenciación y, aunque las partes contratadas elaboraron excelentes pautas para ayudar a sus miembros a decidir cómo tratar esta distinción, dichas pautas no deben formar parte de la política. Si son parte de la política, se transforman en asesoramiento sobre asuntos jurídicos; esto no es algo que la ICANN debería hacer. Las partes contratadas son perfectamente capaces de publicar estas pautas por sí solas y la ICANN es perfectamente capaz de señalarlas como mejores prácticas para el sector privado, no como pautas en virtud de su política e impuestas por la ICANN. Las partes contratadas deberían conocer mejor su propio riesgo legal y, dado que son los responsables del tratamiento de datos y los responsables de cualquier multa que pueda surgir como resultado de una acción coercitiva, deben tener la libertad de decidir cómo tratar la divulgación de la información de los clientes.
Notamos que esas partes que más insistieron con hacer esta distinción entre personas jurídicas y físicas también insistieron mucho sobre los campos para incluir los datos. Dado que las recomendaciones los dejarán como campos voluntarios, y depende de las partes contratadas, cuyos modelos comerciales varían mucho, decidir cómo usarán los campos, no creemos que las recomendaciones sobre la precisión del campo resulten útiles. Si la ICANN se encarga de ordenar al Grupo de Trabajo en Ingeniería de Internet (IETF), por ejemplo, cómo estandarizar el campo, ¿cómo es que la distinción y la recopilación y divulgación de los datos relevantes necesarios para realizar dicha distinción siguen siendo voluntarias? Este es un asunto que debe dejarse a las mejores prácticas del sector privado.

Asimismo, hablamos de los derechos de los trabajadores por proyecto, contratistas independientes y artistas independientes, ventas y comerciantes, aunque nos instruyeron que representemos a las partes interesadas no comerciales. Nadie más representa a estas personas, cuyos números crecen a paso acelerado a medida que los patrones de empleo se transforman con la economía de Internet global. Esta brecha muestra claramente el énfasis en las grandes empresas y la falta de enfoque en cuestiones competitivas que se ven exacerbadas por la política del DNS. Esperamos que las partes

contratadas aborden los derechos de estas personas y sean cautelosas con el fin de garantizar que sean tratadas de manera justa y con el debido respeto de las normas de privacidad cuando se implemente esta política.

Grupo de Partes Interesadas de Registradores

Los representantes del Grupo de Partes Interesadas de Registradores (RrSG) en el Grupo de Trabajo para la Fase 2A del EPDP desean agradecer al personal de la ICANN y a todos los demás miembros del EPDP WG por su ardua labor a lo largo de esta fase del EPDP. La siguiente declaración tiene el fin de complementar nuestro voto de consenso y aportes a lo largo del trabajo sobre la Fase 2A del EPDP.

Comentarios Generales

En las deliberaciones sobre la fase 2A del EPDP, el equipo del RrSG enfatizó que cada registrador individual debe poder determinar el nivel de riesgo que asume, dentro de una base que permita el cumplimiento de las obligaciones legales relevantes. De modo similar, cada registrador debe poder determinar qué considera comercial y técnicamente factible para su propio negocio.

Aunque las recomendaciones propuestas por el Grupo de Trabajo de la Fase 2A del EPDP permiten que se realice la autodeterminación, y ofrecen opciones y pautas para los registradores y registros que opten por realizar la diferenciación en función de la presencia de datos personales en el registro de registración, o que opten por publicar un correo electrónico de contacto basado en el registratario o en la registración, resulta desalentador que la obtención de este resultado fuese el producto de una gran batalla. Durante el trabajo sobre esta Fase, el Grupo de Trabajo volvió a analizar cuestiones en varias ocasiones sin agregar nada muy nuevo al debate y analizó temas que estaban fuera de alcance. Quizá algo más importante es que el Grupo de Trabajo no se mostró interesado o preocupado por los riesgos legales y financieros que algunas obligaciones propuestas crearían para las partes contratadas en varias jurisdicciones o en diferentes modelos comerciales, o los riesgos para los registratarios en sí.

Por último, notamos que los posibles beneficios resultantes de obligaciones de políticas obligatorias en estas áreas, que negarían la capacidad vital de que los registradores eligieran sus propios riesgos legales, comerciales y técnicos, no se mostraron de forma clara y convincente para demostrar la necesidad absoluta de dichas obligaciones en comparación con opciones menos problemáticas sugeridas por el equipo de registradores. Las obligaciones de políticas sugeridas no mostraron los fundamentos para una necesidad estricta o para mejoras generalmente aceptables para el ecosistema de dominios, los que pudieron haber brindado justificación para exigirlas. Por lo tanto, el equipo de RrSG está seguro de que el resultado del trabajo de la Fase 2A, inclusive las pautas y los requisitos opcionales para la diferenciación y el uso de una dirección de correo electrónico basada en el registratario o en la registración, es el resultado adecuado.

Personas jurídicas vs. personas físicas

El equipo de RrSG respalda mantener la recomendación 17 (1) de la Fase 1 y considera que esta es una resolución al problema como se menciona en la recomendación 17 (3) de la Fase 1. Si bien los diversos grupos representados en el Grupo de Trabajo de la Fase 2A del EPDP no llegaron a un

acuerdo sobre este tema, todos los aportes relevantes fueron analizados y tratados en detalle durante las deliberaciones y no se prevén ni planean más deliberaciones al respecto; así que se ha resuelto la cuestión. Además, esta en la resolución *correcta*. Cada registrador debe tener el control de realizar su propio análisis de riesgo/beneficio y considerar su propio panorama jurisdiccional a fin de determinar si realizará la diferenciación y, de ser así, cómo la hará; y esta solución conserva la capacidad de hacerlo.

El equipo de registradores enfatiza que el método de diferenciación variará en función de los registradores. Tanto el uso de "marcadores" o "campos" para indicar el tipo de persona o la presencia de datos personales, así como el contenido de las pautas, se han definido dentro de esta Fase como opcionales, en vez de obligatorios para todos los registradores. Estas pautas son generales y el producto de un compromiso significativo; resultan útiles, pero no se aplican a todas las situaciones o a todos los registradores a nivel mundial. Por ende, *deben* seguir siendo opcionales. Todo código de conducta o pauta obligatoria solo puede ser creado por las partes contratadas relevantes, con toda la debida consideración de los aportes de la comunidad.

Factibilidad de contactos únicos

El equipo de RrSG está de acuerdo en que la publicación de una dirección de correo electrónico basada en la registración o en el registratario en el RDDS público es una actividad de tratamiento de datos y agradece los aportes útiles y detallados que brindó Bird & Bird sobre este tema. Si bien algunas implementaciones de esta opción de publicación pueden presentar menos riesgos que otras, señalamos, una vez más, que cada registrador debe poder determinar el grado al cual asume riesgos legales, en vez de que el Grupo de Trabajo sobre la Fase 2A del EPDP tome la decisión por él. En consecuencia, recomendamos a todos los lectores de este Informe Final analizar el asesoramiento legal brindado sobre este tema (incluido como Anexo F al Informe Final) y prevemos que habrá más pautas y apoyo disponibles para los miembros del Grupo de Partes Interesadas de Registradores, según sea necesario.

Para conocer más las visiones del equipo de RrSG sobre estos temas, consulte también nuestra publicación en Circle ID: Privacidad, personas jurídicas vs. físicas y el interminable EPDP de la ICANN. Gracias.

Grupo de Partes Interesadas de Registros

Declaración minoritaria sobre el Informe Final de la Fase 2A del Proceso Expeditivo de Desarrollo de Políticas sobre datos de registración de gTLD

Después de más de tres años de diligencia, el RySG se complace en celebrar la resolución del Proceso Expeditivo de Desarrollo de Políticas sobre la Especificación Temporaria para los Datos de Registración de los gTLD ("EPDP"). Este fue un esfuerzo casi sin precedentes, impulsado por la promulgación del GDPR, que requirió que la comunidad de la ICANN. se reuniese para abordar incompatibilidades de larga data con las obligaciones relativas a la protección de datos. El RySG está muy agradecido por el arduo trabajo y compromiso de nuestros presidentes y vicepresidentes, del incansable equipo de apoyo al personal de la ICANN y de los miembros del equipo responsable del EPDP que participaron de buena fe para llegar al denominador común y a un entendimiento sobre estos temas muy complejos.

El RySG está convencido de que, como en fases anteriores de este trabajo, logramos el equilibrio adecuado entre la protección de los derechos de privacidad del titular de los datos y el cumplimiento de nuestras obligaciones legales, sin crear obstáculos innecesarios ni impedimentos operativos para nuestros clientes o nuestras empresas.

I. La cuestión sobre personas jurídicas vs. físicas está resuelta

La Fase 2A resolvió la cuestión de la diferenciación entre personas jurídicas y físicas. Un PDP no tiene que generar recomendaciones de consenso para resolver una cuestión. El hecho de que el grupo de trabajo no haya acordado cambios a la recomendación anterior (recomendación 17 de la Fase 1) sobre personas jurídicas vs. física es un resultado valorable y aceptable. Después de tres fases de deliberación del EPDP, un estudio que llevó a cabo la organización de la ICANN y asesoramiento legal de un asesor externo sobre la cuestión sobre personas jurídicas vs. física, ya es hora de admitir que este tema está cerrado.

De hecho, el equipo responsable del EPDP siguió con diligencia las instrucciones del consejo de la GNSO para "responder". . si se requieren actualizaciones a la recomendación de la Fase 1 del EPDP sobre este tema ("los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y personas jurídicas, aunque no están obligados a hacerlo");[66] La respuesta a esa pregunta específica requirió consideración de toda la recomendación dividida en

[66] Instrucciones del Consejo de la GNSO para personas jurídicas vs. naturales en la Fase 2A: "[S]e espera que el equipo responsable del EPDP analice el estudio realizado por la ICANN (tal como lo solicitó el equipo responsable del EPDP y lo aprobó el Consejo de la GNSO
durante la Fase 1), junto con el asesoramiento legal que brindó Bird & Bird, así como los aportes sustanciales proporcionados sobre este tema durante el foro de comentario público sobre el anexo y responda:

I. Si se requieren actualizaciones a la recomendación de la Fase 1 del EPDP sobre este tema ("los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y personas jurídicas, aunque no están obligados a hacerlo");
II. Qué pautas, si las hubiese, pueden brindarse a los registradores o registros que realizan la diferenciación entre registraciones de personas físicas y jurídicas".

tres partes de la Fase 1.[67] El argumento de que el equipo responsable del EPDP no ha satisfecho la recomendación 17.3 ("El Equipo responsable del EPDP determinará y resolverá el asunto de personas físicas vs. jurídicas en la Fase 2") toma, en forma deliberada, una visión acotada del texto de la recomendación e ignora el lenguaje simple de las instrucciones del Consejo de la GNSO. El RySG se muestra preocupado porque algunos sugirieron que esta cuestión no se resolvió. Esta cuestión se debatió en tres fases diferentes del EPDP y el resultado, en cada una de ellas, fue que las partes contratadas pueden realizar la diferenciación, pero no están obligados a hacerlo. Esto demuestra claramente que este asunto fue tratado de manera adecuada y coherente. La percepción de que este trabajo de algún modo no se resolvió podría ser perjudicial para la comunidad de la ICANN y podría considerarse que menoscaba la eficacia del modelo de múltiples partes interesadas. También sería injusto para los miembros del grupo de trabajo y las innumerables horas que dedicaron a la deliberación y resolución de la cuestión.

II. La diferenciación opcional sigue siendo un buen resultado

El RySG cree firmemente que mantener las recomendaciones de políticas de la Fase 1 como opcionales y no como obligatorias[68] para los datos de registración de personas jurídicas vs. físicas es objetivamente un buen resultado de nuestro trabajo sobre desarrollo de políticas. Este resultado no se trata solo de mantener el estatus quo. Creemos que el equilibrio logrado (después de mucha consideración) en el lenguaje de la Recomendación 17 de la Fase 1 es de vital importancia, en particular, dada la incertidumbre normativa que muchos del equipo responsable del EPDP aducen en reiteradas ocasiones como su justificación para cambiar la recomendación de la Fase 1. En cambio, esa incertidumbre es, en parte, el motivo por el cual la recomendación 17 es una solución adecuada, flexible y elegante a la cuestión de la diferenciación entre personas jurídicas y físicas.

a. Se debe permitir que las partes contratadas controlen sus propios riesgos legales

Tal como el RySG explicó a lo largo de la Fase 2A, la flexibilidad inherente en permitir pero no exigir la diferenciación es importante para que las partes contratadas puedan controlar sus propios riesgos legales y mitigar los riesgos para sus clientes. Los registros y registradores manifestaron varias veces que esto era como una premisa fundamental durante todo el EPDP.

---

[67] El Informe Final de la Fase 1 del EPDP contiene la siguiente recomendación sobre la cuestión de las personas jurídicas vs. físicas:
Recomendación 17.1: "El Equipo responsable del EPDP recomienda que los registradores y operadores de registro tengan permitido diferenciar entre las registraciones de personas físicas o jurídicas, aunque no están obligados a hacerlo".
Recomendación 17.2: "El Equipo responsable del EPDP recomienda que, tan pronto como sea posible, la organización de la ICANN realice un estudio, cuyos términos de referencia sean elaborados en consulta con la comunidad, que considere:

- La viabilidad y los costos, incluidos los costos de implementación y de posible responsabilidad para diferenciar entre personas físicas y jurídicas;
- Ejemplos de industrias u otras organizaciones que han diferenciado entre personas físicas y jurídicas exitosamente;
- Riesgos de privacidad para los titulares del nombre registrado ante la diferenciación entre personas físicas y jurídicas; y
- Otros posibles riesgos (si los hubiese) para los registradores y registros resultantes de la falta de diferenciación".

Recomendación 17.3: "El equipo responsable del EPDP determinará y resolverá el asunto de personas físicas vs. jurídicas en la Fase 2".

[68] Recomendación 17.1: "El equipo responsable del EPDP recomienda que los registradores y operadores de registro tengan permitido diferenciar a las registraciones de persona físicas o jurídicas, aunque no están obligados a hacerlo".

Los memorandos legales manifiestan con claridad, "[s]i 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".[69] De manera similar, "[s]i existe un riesgo razonable de que los titulares de los datos se identifiquen erróneamente, entonces no informar a los titulares de los datos sobre las consecuencias de la autoidentificación podría resultar en una responsabilidad por no cumplir con el principio de legalidad, equidad y transparencia".[70]

El RySG valora que Bird & Bird haya suministrado asesoramiento sobre cómo mitigar dichos riesgos. No obstante, la cuestión de cómo adoptar dichos procedimientos y de qué manera, sin mencionar cómo determinar qué es un riesgo aceptable, debe ser la responsabilidad exclusiva de las partes contratadas que asumen ese riesgo. En cualquier otro acuerdo comercial, esto sería una proposición indiscutible. Como expresamos desde el comienzo de este PDP, donde las partes contratadas asumen la responsabilidad de tratar los datos, las decisiones sobre esos datos deben recaen en los registros y registradores en vez de en terceros que no asumen ningún riesgo y no tienen intereses compartidos en cuanto a la protección de los datos de nuestros clientes.

b. Se recomienda la flexibilidad

Mantener políticas flexibles en vez de prescriptivas sobre la diferenciación entre personas jurídicas y físicas garantiza que los registradores y registros tengan la habilidad y la capacidad de responder con rapidez a futuros cambios normativos que puedan impactar en la publicación de los datos de personas jurídicas, sin requerir la elaboración de políticas adicionales. El RySG reconoce que la Directiva Revisada sobre Seguridad de las Redes y los Sistemas de Información ("NIS 2") tiene el potencial, una vez adoptada, de afectar la forma en que los registradores y registros tratan los datos de personas jurídicas. La incertidumbre en torno a cómo y cuándo los estados miembro de la UE implementarán la Directiva NIS 2 es precisamente el motivo por el cual es imperativo que los registros y registradores tengan la flexibilidad de autodeterminar su cumplimiento con el cambiante panorama legal y normativo. El cambiante panorama de la privacidad refuerza la recomendación de la Fase 1 y afirma la opción de que las partes contratadas realicen la diferenciación entre personas jurídicas y físicas.

c. Justificación insuficiente de que es necesario e incluso beneficioso tener requisitos adicionales

[69] "Asesoramiento sobre responsabilidad en relación con la autoidentificación del registratario como persona física o no física en virtud del Reglamento General de Protección de Datos (Reglamentación (UE) 2016/679) ("GDPR")," por Ruth Boardman & Gabe Maldoff, publicado el 25 de enero de 2019: https://community.icann.org/download/attachments/102138857/Natural%20vs.%20Legal%20Memo.docx

[70] Id

Si bien el RySG confía mucho en la recomendación 17 de la Fase 1 por sus propios méritos, también notamos que no se brindó una justificación convincente en cuanto al motivo por el cual la diferenciación obligatoria sería necesaria o incluso recomendable. Sin más información, no entendemos con exactitud qué problema está intentando resolver la diferenciación obligatoria entre las registraciones de personas jurídicas y físicas.

III. El RySG confía en el proceso de la GNSO para determinar cuándo se requieren futuros trabajos sobre políticas

El RySG respalda marcar la Directiva NIS 2 al Consejo de la GNSO para su supervisión continua. Sin embargo, no consideramos que la actual NIS 2 preliminar necesite un nuevo trabajo sobre políticas y dudamos en predeterminar un resultado que lo necesite. El RySG respalda y se remite al rol del Consejo de la GNSO en determinar cuándo se requiere trabajo sobre políticas. Los procedimientos y prácticas de la GNSO evidencian que no se requieren políticas de la ICANN para instruir o duplicar obligaciones a las que están sujetas las partes contratadas por ley. La ICANN inició este EPDP para abordar la promulgación del GDPR; el trabajo de política en esa instancia era necesario debido a conflictos directos entre los requisitos de nuestros acuerdos con la ICANN y los requisitos del GDPR. No se puede decir lo mismo de la posible legislación de la NIS 2 preliminar. Mientras tanto, algunas leyes de protección de datos se han aprobado o han entrado en vigencia en California, Virginia, Japón, India y China (por nombrar solo algunos) que algunas o todas las partes contratadas deben cumplir. Nadie sugirió (de manera acertada) que la ICANN elabore políticas para garantizar el cumplimiento de dichas obligaciones porque no hay conflicto directo con nuestros acuerdos. En última instancia, la decisión de si se debe iniciar un nuevo trabajo sobre políticas, y, de ser así, cuándo hacerlo, debe recaer en el Consejo de la GNSO, siguiendo los procesos existentes.

IV. La recomendación n.° 1 está fuera de alcance y plantea importantes preguntas sobre la implementación

A modo de recordatorio, sobre la cuestión de la diferenciación entre personas jurídicas y físicas de la Fase 2A, el Consejo de la GNSO indicó al EPDP que respondiese dos preguntas muy concretas: (1) si se requieren actualizaciones a la recomendación de la Fase 1 del EPDP sobre este tema ("los registradores y operadores de registro tienen permitido diferenciar entre las registraciones de personas físicas y personas jurídicas, aunque no están obligados a hacerlo"); y (2) qué pautas, si las hubiese, pueden brindarse a los registradores o registros que realizan la diferenciación entre registraciones de personas físicas y jurídicas.[71]

La observancia del alcance acordado de un PDP es de vital importancia para el desarrollo de buenas políticas. Lamentablemente, el trabajo de la Fase 2A ha sufrido constantes intentos de ampliar el alcance de nuestra tarea, lo que finalmente resultó en una recomendación de crear un elemento de datos que, en varias ocasiones, marcamos también como muy fuera del alcance de nuestras instrucciones del Consejo de la GNSO. La creación obligatoria de un nuevo elemento de datos no tiene ningún nexo con el lenguaje de la recomendación 17 de la Fase 1 y, por ende, no se justifica como una respuesta a la primera parte de nuestra tarea de la GNSO. En vez de solicitar aclaraciones

[71] Carta orgánica de la Fase 2A de la GNSO, disponible en https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-2-priority-2-items-10sep20-en.pdf

sobre el alcance al principio de la consideración de esta cuestión, el presidente del EPDP determinó que la creación de un elemento de datos se relaciona con las pautas dentro del alcance del EPDP. Además, "si el Consejo de la GNSO considera que lo que estamos elaborando está fuera de alcance, debería comunicarlo".[72]

En consecuencia, el RySG solicita respetuosamente que el Consejo de la GNSO primero examine la recomendación n.° 1 desde la perspectiva de si la propuesta está en realidad dentro del alcance del trabajo de la Fase 2A antes de considerar la aprobación de la recomendación. Como explicamos, creemos que no lo está. Si la GNSO determina que la recomendación n.° 1 está dentro del alcance, el RySG aún tiene grandes preocupaciones sobre la pertinencia y la implementación práctica de dicha recomendación.

a. La recomendación n.° 1 no se relaciona con nuestras instrucciones del Consejo

Consideramos que la creación obligatoria propuesta de un nuevo elemento de datos, que requiere la participación con el IETF, y posiblemente la participación adicional en otras áreas, no califica como el "asesoramiento" al que se hace referencia en las instrucciones de la GNSO. La existencia (o inexistencia) de un elemento de datos estandarizado no hace nada para asistir a las partes en el proceso de diferenciación, simplemente captura el resultado de ese proceso. El hecho de enfocarse en el resultado en vez de en el proceso no es asesoramiento, al menos no asesoramiento práctico que sea significativo y, por ende, no se ajusta a las instrucciones del EPDP del Consejo.

De manera similar, al considerar la posibilidad de un elemento de datos estandarizado, no estamos de acuerdo en que recomendar un nuevo elemento de datos se relacione con el asesoramiento simplemente porque el elemento de datos se menciona en ese asesoramiento. No podemos incluir elementos dentro del alcance del PDP de esta forma. El EPDP no debería ir más allá del alcance de sus instrucciones y nuestras recomendaciones deben centrarse en un sentido similar.

b. La creación de un nuevo elemento de datos plantea cuestiones importantes sobre la implementación

Si la GNSO determina que la recomendación n.° 1 está dentro del alcance de la Fase 2A, el RySG aun considera que existen cuestiones importantes sobre la implementación que la GNSO y la ICANN deben considerar con atención antes de adoptar esta recomendación.

El elemento de datos propuesto no es algo que la ICANN pueda crear por su propia cuenta. Los estándares de Internet del RDAP y EPP (las especificaciones técnicas), los cuales constituyen las bases para la mayoría de los canales de comunicación usados para los datos de registración, son controlados por el IETF. El IETF tiene un proceso independiente de la ICANN dentro de una comunidad técnica compuesta por no solo las partes relacionadas con la ICANN, lo que posiblemente cree obstáculos para la implementación.

[72] "Con respecto a su punto sobre el alcance, el equipo de liderazgo y el personal han analizado esto. Yo pienso que lo que estamos debatiendo aquí en cuanto a lo relacionado a las pautas está dentro del alcance de la carta orgánica del EPDP y las pautas que nos brindaron, las preguntas que nos entregaron. Y pienso que si el Consejo de la GNSO considera que lo que estamos elaborando está fuera de alcance, debería comunicarlo. Y tenemos un coordinador de enlace aquí con Philippe, que también es el presidente de la GNSO, que gestionará cualquier cuestión en ese sentido que se relacione con el alcance". Presidente del EPDP, reunión de la Fase 2A, 5 de agosto de 2021.

Debido a las preocupaciones importantes planteadas respecto de la adopción de este elemento de datos, notamos que no se ha brindado una justificación convincente sobre el motivo por el cual este elemento de datos es necesario o beneficioso, en particular, como parte del RDDS público. Los fundamentos propuestos, entre ellos (i) rastrear en qué medida las partes contratadas implementan la diferenciación; (ii) permitir que el público verifique la exactitud de una designación de persona jurídica o física; (iii) determinar el cumplimiento de las leyes aplicables; (iv) pasar las referencias a "consistencia", y (v) 'qué daño' existe al adoptar el elemento de datos, no mencionan un beneficio específico y probablemente se puedan lograr mediante los mecanismos existentes. Ninguno de los fundamentos presentados tiene mucho sentido práctico y mucho menos son necesarios o lo suficientemente convincentes para justificar dichos cambios significativos y fuera de alcance a la política existente.

Como se mencionó anteriormente, la existencia (o inexistencia) de un elemento de datos estandarizado no hace nada para asistir a las partes que desean realizar la diferenciación entre personas jurídicas y físicas, simplemente captura el resultado de ese proceso. Al considerar la posibilidad de un elemento de datos estándar, los registros acordaron que, con fines de integración con un posible sistema SSAD futuro, como se recomienda en la Fase 2, puede tener sentido para un modo estandarizado de indicar si una registración contiene o no datos personales. Si bien admitimos que puede haber un caso práctico vinculado a las decisiones de divulgación en el SSAD, preferiríamos aplazar dichas decisiones, según resulte adecuado, hasta el desarrollo del SSAD antes de tomar medidas ahora que puedan limitar la utilidad de este elemento de datos una vez que el SSAD esté en funcionamiento.

La recomendación se extiende más allá de esto, ya que requiere que la ICANN cree este campo en coordinación con la comunidad técnica para usarlo con el EPP y el RDDS. Para que resulte claro, el RySG no respalda usar este campo en el EPP ni en el RDDS. Como compromiso, acordamos que este campo es totalmente opcional que puede ser utilizado por las partes contratadas que optan por hacer la diferenciación entre personas jurídicas y físicas o por indicar si la registración contiene datos personales; pero su uso no es de ningún modo obligatorio.

Con el fin de colaborar de buena fe hacia una solución de compromiso, los registros acordaron la creación de un elemento de datos estandarizado y que las partes contratadas podrían, si así lo eligiesen, usar ese elemento de datos estándar. Tenemos muchas dudas respecto del uso de dicho campo en el EPP o el RDDS, y debemos dejar en claro que no respaldamos su uso en ninguno de los dos. No escuchamos un fundamento convincente sobre el motivo por el cual se debería usar un campo en cualquiera de los casos, y nuestro apoyo a la creación de dicho campo no indica asesoramiento o una recomendación de que debiera utilizarse.

V. El asesoramiento elaborado sobre la diferenciación entre personas jurídicas y físicas no es suficiente

El RySG respalda el concepto de asesoramiento que ayuda a las partes contratadas transitar los desafíos legales y técnicos complejos que los registradores y registros enfrentan, en forma periódica, al llevar a cabo las operaciones de nuestros negocios. Según nuestra experiencia, el mejor asesoramiento es elaborado por aquellos con la experiencia y los intereses adecuados para

enfrentar la complejidad y ofrecer claridad sobre preguntas difíciles y ambiguas. A pesar de las continuas objeciones y sugerencias de las partes contratadas para realizar mejoras, el asesoramiento incluido en este informe sobre diferenciación entre personas jurídicas y físicas no cumple con ninguno de estos criterios.

Al elaborar el asesoramiento contenido en la recomendación n.° 2, el grupo de trabajo acordó que se trata de un asesoramiento opcional que las partes contratadas que optan por diferenciar entre registraciones de personas jurídicas y físicas pueden aprovechar a su criterio. Sin embargo, el lenguaje del informe final de la recomendación n.° 2 estipula que las partes contratadas que optan por realizar la diferenciación DEBERÍAN seguir este asesoramiento. El RySG considera que el uso de la palabra DEBERÍA aquí no captura con exactitud lo que acordó el grupo de trabajo. En virtud de la RFC 2119, "DEBERÍA . . . significa que pueden existir motivos válidos en ciertas circunstancias para ignorar un elemento en particular, pero se deben comprender y sopesar con cautela todas las implicancias antes de elegir un rumbo diferente". Dado que el cumplimiento de este asesoramiento sobre diferenciación es opcional, el término más apropiado aquí es PUEDE ("un elemento es realmente opcional"). Si bien en pos de colaborar de buena fe hacia una solución de compromiso, los registros optaron por respaldar la recomendación, debemos señalar que no estamos de acuerdo con el uso de DEBERÍA y que las partes contratadas deben considerar si el asesoramiento es útil y aplicable para ellos antes de decidir si lo adoptan.

En resumen, el asesoramiento contenido en este informe sobre la diferenciación entre personas jurídicas y físicas es muy inadecuado si su propósito es ayudar a una parte contratada que desea realizar la diferenciación. El asesoramiento no es suficiente por diversos motivos. En primer lugar, el asesoramiento está orientado al resultado de manera intencional y poco razonable. Aquellos que defendieron la necesidad de este asesoramiento minimizaron el proceso por el cual se realiza la diferenciación, y las consideraciones y los requisitos legales asociados. Este enfoque opaca casi intencionalmente en vez de enfrentar las complejidades y los riesgos implicados en el proceso de diferenciación, que no hace nada para ayudar al usuario del asesoramiento a comprender y abordar dichos riesgos y complejidades.

En segundo lugar, el asesoramiento no es práctico. Una vez más, al no enfrentar las complejidades y los riesgos inherentes a la diferenciación, el asesoramiento resultante es apenas más que un parafraseo de la ley y los resultados esperados. Por ejemplo, el asesoramiento manifiesta lo siguiente:

"Los registradores deberían asegurarse de comunicar claramente la naturaleza y las consecuencias de que un registratario se identifique como persona jurídica. Estas comunicaciones deberían incluir:

- *Una explicación de qué es una persona jurídica en lenguaje simple que sea fácil de comprender.*
- *Pautas para el registratario (titular de los datos)35 641 por parte del registrador respecto de las posibles consecuencias de:*
  - *Identificar los datos de registración de su nombre de dominio como persona jurídica;*
  - *Confirmar la presencia de datos personales o datos no personales, y;*

- *Prestar consentimiento. Esto también está en consonancia con la sección 3.7.7.4 del Acuerdo de Acreditación de Registradores (RAA)".*

Lamentablemente, para un usuario de este asesoramiento, esta breve sección plantea más preguntas que respuestas. ¿Qué es una persona jurídica? ¿Qué sucede si el registratario no es el titular de los datos? ¿Cuáles son las consecuencias del marcado para el titular de los datos? ¿Qué pasos se deben realizar para garantizar que el titular de los datos comprenda este mensaje (por ejemplo, pruebas A/B, paneles del usuario)? ¿Cuáles son los riesgos si no se siguen estos pasos? ¿Cómo se obtiene el consentimiento informado, en especial, en los casos en que el registratario puede no ser el titular de los datos? ¿La instrucción o la notificación al registratario es suficiente para mitigar los riesgos? La simple reformulación de las obligaciones que ya son ampliamente ordenadas por ley sirve muy poco aquí para ayudar realmente a un usuario del asesoramiento a transitar estas cuestiones.

De manera similar, el asesoramiento manifiesta en el último párrafo lo siguiente:

La distinción entre personas jurídicas y físicas registratarias por sí sola puede no ser determinante de la forma en que se debería tratar la información (hacerla pública o estar enmascarada), ya que los datos suministrados por personas jurídicas pueden incluir datos personales que están protegidos por leyes de protección de datos, como el GDPR.

Esta es, de hecho, la cuestión más difícil y riesgosa de la diferenciación entre registraciones de personas jurídicas y físicas. Como el EDPB instruyó a la ICANN, "[e]l simple hecho de que un registratario sea una persona jurídica no necesariamente justifica la publicación ilimitada de datos personales relacionados con las personas físicas que trabajan para esa organización o que la representan".[73] Este asesoramiento no contempla o ni siquiera explica mínimamente cómo un registrador podría comenzar a abordar la cuestión. Abordar este reto fundamental casi incidentalmente menoscaba seriamente la utilidad de este asesoramiento y aumenta nuestra preocupación sobre la factibilidad general del mismo.

Con el fin de colaborar de buena fe, el RySG acordó respaldar la publicación de este asesoramiento a pesar de las preocupaciones manifestadas anteriormente, ya que la recomendación deja en claro que el asesoramiento es realmente opcional y las partes contratadas (incluso aquellas que optan por la diferenciación) no están de ningún modo obligadas a cumplir con la recomendación n.° 2. Somos escépticos de que este asesoramiento se adopte a nivel general, no porque no se desee un asesoramiento sobre esta cuestión, sino porque estos asesoramientos no hacen nada para guiar la implementación práctica y no ofrecen tranquilidad a las partes que asumen los riesgos legales.

VI. Conclusión

Por todos los motivos recién expuestos, dado el apoyo continuo de las diversas partes del equipo responsable del EPDP para la publicación de este informe final y las recomendaciones tal como se manifestaron, e independientemente de nuestras preocupaciones relacionadas con el alcance de las recomendaciones, el RySG no se opone a la aprobación de este informe y las recomendaciones

[73] Carta del EDPB a Göran Marby, con fecha de julio de 2018, disponible en https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

manifestadas. Sin embargo, se señala que este apoyo se basa en la buena fe de que todas las partes mantengan el nivel de consenso acordado. Si bien el RySG no respalda varios aspectos de este informe, en defensa y apoyo del modelo de múltiples partes interesadas, hemos transigido.

Declaración minoritaria del SSAC sobre Informe Final de la Fase 2A del Proceso Expeditivo de Desarrollo de Políticas sobre las Especificaciones Temporarias para los Datos de Registración de los gTLD[74]

1 Introducción

El Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN agradece la distribución del Informe Inicial del Equipo de la FASE 2A del Proceso Expeditivo de Desarrollo de Políticas (EPDP) sobre la Especificación Temporaria para los Datos de Registración de los gTLD (en adelante, denominado "Informe Inicial de la Fase 2A del EPDP"),[75] y agradece al grupo de trabajo la oportunidad de comentar al respecto.

En este documento, el SSAC presenta los comentarios generales sobre el Proceso Expeditivo de Desarrollo de Políticas general y comentarios específicos sobre las recomendaciones individuales contenidas en el Informe Inicial de la Fase 2A del EPDP. El SSAC se complacería en debatir estos comentarios con el equipo responsable del EPDP cuando sea conveniente para explicar cualquier punto que sea poco claro y requiera más elaboración.

El SSAC desea reconocer todo el tiempo y el esfuerzo que dedicaron los miembros del equipo responsable del EPDP y agradecerles por su contribución es este tema importante.

2 Información de referencia

En esta sección, analizamos las preguntas que el Grupo de Trabajo (WG) sobre la Fase 2A está considerando, realizamos algunas observaciones sobre el Proceso Expeditivo de Desarrollo de Políticas general y, luego, describimos nuestro enfoque. En la sección siguiente, presentamos nuestras recomendaciones, algunas de las cuales se aplican al esfuerzo general y otras son específicas al esfuerzo de la Fase 2A.

2.1 Preguntas en consideración por el Grupo de Trabajo para la Fase 2A del EPDP

2.1.1 Distinción entre personas jurídicas y físicas

El Reglamento General de Protección de Datos (GDPR) brinda protección específica para personas físicas (es decir, seres humanos) y ninguna protección para personas jurídicas (es decir, empresas).[76,77] El EPDP WG, y en particular el WG para la Fase 2A del EPDP, ha puesto mucha

[74] El documento se publicó como SAC118, disponible en https://www.icann.org/en/system/files/files/sac-118-en.pdf

[75] Consulte el Informe Inicial del Equipo de la FASE 2A del Proceso Expeditivo de Desarrollo de Políticas (EPDP) sobre la Especificación Temporaria para los Datos de Registración de los gTLD, https://www.icann.org/en/system/files/files/epdp-phase-2a-initial-report-02jun21-en.pdf

[76] Consulte la cláusula 14 del GDPR: "La protección brindada por este Reglamento se debería aplicar a personas físicas, sin importar nacionalidad o lugar de residencia, en relación con el tratamiento de sus datos personales. "Esta reglamentación no abarca el tratamiento 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". https://gdpr-info.eu/recitals/no-14/

[77] Consulte el artículo 4 del GDPR, disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1

atención a esta distinción. Entre las preguntas que el EPDP WG ha considerado se encuentran las siguientes:

1. ¿Debería haber un elemento de datos específico para registrar si el registratario es una persona física o una persona jurídica?
2. ¿Se debe exigir a cada registratario que realice la determinación para cada registración?
3. ¿Qué prueba se debería exigir para realizar esta determinación?
4. ¿Cuáles son los riesgos si la determinación del registrador es incorrecta?
5. ¿Se debería exigir al registratario que declare si es una persona física o una persona jurídica, y el registrador debería confiar en esa declaración?
6. ¿Los datos de contacto de registratarios clasificados como personas jurídicas siempre deberían estar disponibles públicamente?[78]
7. ¿Los datos de contacto de registratarios clasificados como personas jurídicas no deberían nunca estar disponibles públicamente?
8. ¿El estado del registratario debería estar disponible públicamente?
9. ¿Cómo proceder cuando la información de identificación personal (PII) de una persona física está incluida como parte de la registración de una persona jurídica?

2.1.2 Factibilidad de contactos únicos

Se le solicitó al equipo responsable del EPDP que considerase las siguientes preguntas:

- Si es factible un contacto único en forma de una dirección de correo electrónico anonimizada uniforme y, de ser factible, si debería ser un requisito obligatorio
- Si es factible, pero no es un requisito obligatorio, ¿qué pautas, si las hubiese, pueden brindarse a las partes contratadas de la ICANN que deseen implementar direcciones de correo electrónico anonimizadas uniformes?

El equipo responsable del EPDP observó que el término “contactos únicos” es ambiguo y que hay dos objetivos distintos estipulados por aquellos que propugnan los contactos únicos. Estos son: (1) la capacidad de ponerse en contacto de manera rápida y eficaz con el registratario sin divulgar datos personales y (2) un identificador común que ayude a los investigadores a asociar las registraciones de dominio con un contacto en común.

El equipo responsable del EPDP intentó eliminar la ambigüedad de estos propósitos al proponer dos términos:

- **Contacto de correo electrónico basado en el registratario:** un correo electrónico para todos los dominios registrados por un único registratario [patrocinado por un registrador específico] O [entre registratarios], que tiene el propósito de ser datos seudónimos al ser tratados por partes no contratadas.

[78] Por lo general, el EPDP WG trata el proceso de solicitud y respuesta como si los datos “públicos” estuvieran publicados para que cualquiera los pudiera ver. En todos los escenarios previstos, todo acceso a los datos de registración se realiza mediante el proceso de solicitud y respuesta. Es decir, los datos de registración no se publican en el sentido en que generalmente se entiende la publicación. En este documento, usamos la frase “disponibles públicamente” en el sentido de que los datos están disponibles a cualquiera que los solicite sin restricciones en el uso y sin atribución.

- **Contacto de correo electrónico basado en la registración:** un correo electrónico de uso único separado para cada nombre de dominio registrado por un único registratario, que tiene el propósito de ser datos anónimos al ser tratados por partes no contratadas.

Después de deliberarlo durante un tiempo, el equipo responsable del EPDP no brindó una respuesta concluyente sobre la factibilidad del contacto de correo electrónico basado en el registratario o en la registración. El equipo responsable del EPDP recomendó que "las partes contratadas que optan por publicar una dirección de correo electrónico basada en el registratario o en la registración en el Servicio de Directorio de Datos de Registración de Nombres de Dominio (RDDS) de acceso público deberían garantizar las medidas de protección adecuadas para el titular de datos en consonancia con el asesoramiento relevante sobre técnicas de anonimización proporcionado por sus autoridades de protección de datos y el asesoramiento legal anexado".
El SSAC señala que algunos registradores ya implementaron algunos métodos diferentes para respaldar el uso del contacto de correo electrónico basado en el registratario. Por ejemplo, se han creado direcciones de correo electrónico exclusivas basadas en el registratario para cada registratario, las cuales se alojan en un dominio del registrador. Los mensajes dirigidos a estas direcciones de correo electrónico, al ser recibidos por el registrador, son redirigidos al destinatario real. Algunos registradores brindan un formulario basado en la Web que se puede usar para dirigir un mensaje al registratario de un nombre de dominio en particular. En la mayoría de los casos, el remitente del mensaje original no sabe si se entregó o se abrió el mensaje reenviado. La Especificación Temporaria no proporciona ningún requisito de nivel de servicio para el reenvío de correo electrónico.[79,80]

Hasta el momento, el SSAC no conoce alguna solución implementada que cumpla con los requisitos de contacto de correo electrónico basado en la registración como se define más arriba en el presente. Por cierto, una pequeña cantidad de soluciones se habían propuesto, pero ninguna logró consenso.

2.2 Observaciones del SSAC

En función de la participación en el EPDP, el SSAC ofrece dos comentarios respecto del esfuerzo general por lograr un sistema de acceso diferenciado que cumpla con varios objetivos. Por sistema de acceso diferenciado, el SSAC quiere decir un sistema que brinde la capacidad de condicionar la respuesta en función del solicitante y el propósito de la solicitud. El Sistema Estandarizado de Acceso/Divulgación (SSAD) es un ejemplo específico de este tipo de sistema.

2.2.1 intereses contrapuestos

Desde la perspectiva del SSAC, hay tres intereses contrapuestos en el trabajo en las deliberaciones sobre políticas.

[79] Especificación Temporaria para los Datos de Registración de los gTLD; Apéndice A: Servicio de Directorio de Datos de Registración de Nombres de Dominio, párrafo 2. Https://www.icann.org/resources/pages/gtld-registration-data-specs-en

[80] Ha habido problemas documentados con las implementaciones de capacidad de contacto en los registradores. Consulte las págs. 55-59 de
Datos de registración de nombres de dominio en la encrucijada: el estado de protección de datos, cumplimiento y capacidad de contacto en la ICANN". http://www.interisle.net/domainregistrationdata.html

1. **Defensores de la privacidad.** Algunas partes desean asegurarse de que los datos de contactos de personas físicas no estén disponibles públicamente, a menos que la persona física preste consentimiento explícito e informado para permitir la disponibilidad al público. Quieren que esta protección se aplique a personas jurídicas también si los datos de contacto incluyen PII o si la PII se puede inferir de los datos de contacto.
2. **Solicitantes de datos.** Los solicitantes desean la cantidad máxima de datos que puedan obtener. Los solicitantes desean que las protecciones de datos sean tan cercanas como sea posible a solo lo que se exige por ley. Quieren que las solicitudes se completen de manera confiable, rápida y económica.
3. **Responsables del tratamiento de datos.**[81] Aquellos que recopilan los datos y hacen que estos estén disponibles públicamente, por ejemplo, registradores y operadores de registro, desean minimizar los costos y los riesgos.

Individuales u organizaciones en particular pueden representar más de uno de esos intereses contrapuestos.

2.2.2 Una preocupación tácita

El SSAD es un mecanismo nuevo propuesto para gestionar de forma centralizada las solicitudes de datos de registración sin carácter público, que se describe en las recomendaciones 1-18 del Informe Final sobre la Fase 2 del Proceso Expeditivo de Desarrollo de Políticas (EPDP) de la GNSO sobre la Especificación Temporaria para los Datos de Registración de los gTLD.[82]

Un sistema de acceso bien diseñado permitirá que los solicitantes con necesidades legítimas accedan a los datos sin carácter público, de manera confiable, rápida y económica.

En este momento, es incierto si podemos lograr un sistema de control de acceso diferenciado satisfactorio. En la actualidad, la Junta Directiva de la ICANN ha solicitado una evaluación de la Fase de Diseño Operativo (ODP) durante seis meses para informar sus deliberaciones sobre recomendaciones de políticas. El SSAD propuesto aún no tiene una fecha programada de entrega. La estimación de costo inicial fue criticada por la comunidad por ser muy costosa. También hay una falta de definición en cuanto a qué datos estarán disponibles a qué solicitantes y bajo qué circunstancias. Por último, las partes contratadas pueden estar realizando revisiones manuales de las solicitudes de datos, porque el EPDP no pudo acordar los casos de automatización.

Debido a la falta de claridad acerca del SSAD, parece que algunos participantes del EPDP suponen que los únicos datos a los que posiblemente puedan acceder en el futuro previsible son los datos disponibles públicamente y están presionando para mantener la protección de la privacidad al mínimo exigido por ley. El resultado es la incapacidad de resolver muchas cuestiones en el EPDP.

---

[81] El término también incluye otros que recopilan y tratan los datos recopilados durante la registración (por ejemplo, los revendedores).

[82] Consulte 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, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf

2.3 Enfoque del SSAC

El SSAC considera que es importante que los investigadores de seguridad tengan acceso a los datos de registración de nombres de dominio. Al mismo tiempo, resulta también importante que aquellos que merecen protección la obtengan. Estas dos alternativas pueden coexistir. Pero no pueden coexistir en el contexto de un argumento confrontado sobre si cada contacto debería ser público o no como única opción.

Debería ser posible que la información de contacto considerada personal se mantenga de manera privada y esté disponible en los casos adecuados para las personas que la necesitan. Desde la perspectiva del SSAC, un sistema de acceso diferenciado oportuno, confiable, eficaz y eficiente permitiría lograr un resultado que sería una mejora para todos los intereses contrapuestos.

Por ende, el SSAC considera que la atención de la comunidad de la ICANN y la organización de la ICANN debería centrarse en crear y operar un SSAC eficaz.

Tal como están las cosas, el debate sobre el acceso a datos sin carácter público está fuera del alcance de la Fase 2A del EPDP y el debate de los informes de las Fases 1 y 2 está cerrado. En consecuencia, en este informe, formulamos dos clases de recomendaciones.

1. Recomendaciones generales sobre el acceso diferenciado y el SSAD.
2. Dentro del alcance de la Fase 2A del EPDP, ofrecemos algunas recomendaciones detalladas que, si se adoptan, sacan el mejor provecho de una situación imperfecta.

3 Recomendaciones

3.1 Recomendación a la GNSO y a la organización de la ICANN

Recomendación 1: El SSAC recomienda que la Organización de Apoyo para Nombres Genéricos (GNSO) y la organización de la ICANN centren su atención en crear y operar un sistema de acceso diferenciado eficaz.

Se necesita un sistema de acceso diferenciado con las propiedades siguientes:

Oportuno	Debe empezar a funcionar pronto.
Confiable	Debe operar de manera predecible y uniforme, tanto en el funcionamiento del sistema como en la toma de decisiones por parte de los participantes del sistema.
Útil	Debe proporcionar resultados que beneficien a los solicitantes.
Eficiente	Debe brindar respuestas a las solicitudes de datos legítimas de manera rápida y a un costo que sea aceptable para el propósito de todas las partes.
De fácil acceso	La obtención y el mantenimiento de las credenciales deben funcionar lo suficientemente bien para facilitar el uso, en vez de impedirlo.

Este documento usa el término “eficaz” para hacer referencia a un sistema de acceso diferenciado que cumpla con todos los requisitos recién mencionados y, por supuesto, que incluya las funciones necesarias para gestionar distintas solicitudes y respuestas a varias combinaciones de solicitantes y propósitos, tal como se manifiesta en la sección 2.2.

3.2 Recomendaciones a la Fase 2A del EPDP

3.2.1 Personas jurídicas vs. físicas

Desde la perspectiva de un profesional de la seguridad, debe estar disponible la cantidad máxima de datos de registración para investigación, ya sea mediante un sistema de acceso diferenciado que sea eficaz o bien haciendo que dichos datos estén disponibles en el RDDS público.

Recomendación 2: El SSAC recomienda lo siguiente respecto de las personas jurídicas y físicas:

A. Se debería definir un elemento de datos que denote el estado legal del registratario. En principio, proponemos tres valores admisibles: Persona física, Persona jurídica y No especificado. “No especificado” sería el valor predeterminado hasta que el registratario se identifique como persona física o jurídica. Este cambio debería poder admitir valores de estado en función de las futuras decisiones sobre políticas.
B. Este elemento de datos se debería mostrar como parte de los datos disponibles públicamente.
C. Los registratarios deberían clasificarse como personas físicas o jurídicas. Esto se debería exigir al momento de la registración, para todas las registraciones de dominios nuevas. Para las registraciones existentes, el valor puede seguir siendo “No especificado” hasta que se complete en un momento posterior. Los registradores deberían estar obligados a preguntar en momentos relevantes, como al momento de renovación del dominio o en la consulta anual sobre exactitud, si el registratario es una persona física o jurídica, con el objetivo final de obtener esos datos de todos los registratarios y reducir el valor “No especificado” al nivel más bajo posible.
D. En la actualidad, los registratarios pueden y deben continuar teniendo la opción de que sus datos de contacto estén disponibles públicamente. Los registratarios que son personas jurídicas también deberían tener la posibilidad de proteger sus datos mediante servicios de privacidad y representación (proxy).
Estas recomendaciones están en consonancia con el asesoramiento anterior del SSAC.[83]

3.2.2 Factibilidad de contacto de correo electrónico seudónimo

Recomendación 3: El SSAC recomienda lo siguiente respecto de la factibilidad de contacto de correo electrónico seudónimo:

A. Los dos objetivos relacionados con políticas - a saber (1) la capacidad de ponerse en contacto de manera rápida y eficaz con el registratario sin divulgar datos personales y (2) un

[83] Consulte el documento SAC104, sección 3.6. https://www.icann.org/en/system/files/files/sac-104-en.pdf

identificador común que ayude a los investigadores a asociar las registraciones de dominio con un contacto en común - se deberían considerar en forma separada.

B. Para logar el objetivo sobre políticas (A1), los registradores deberían implementar (o seguir implementando) métodos para admitir contactos de correo electrónico basados en registratarios (consulte la sección 2.1.2, debate de los dos métodos). El SSAC también recomienda que se elaboren requisitos uniformes para las medidas de protección para el contacto de correo electrónico basado en el registratario. Los requisitos deberían incluir mantener la privacidad del registratario según resulte adecuado y acuerdos de nivel de servicio para establecer las expectativas respecto del uso del servicio. Estas medidas de protección son independientes del método elegido (por ejemplo, direcciones de correo electrónico únicas o formularios basados en la web).

C. Para lograr el objetivo sobre políticas (A2), se necesita más investigación sobre los métodos, su eficacia, y sus ventajas y desventajas. Recomendamos que la Fase 2A del EPDP *no* especifique un método para asociar las registraciones con un contacto común en este momento.

Anexo E - Aportes de la comunidad

E.1. Solicitud de comentarios

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.

El equipo responsable del EPDP solicitó aportes sobre estos dos temas como parte de los aportes iniciales solicitados durante las Fases 1 y 2, y en consecuencia, dicho equipo analizó y consideró los aportes brindados hasta ese momento (consulte https://community.icann.org/x/Ag9pBQ yhttps://community.icann.org/x/Ag9pBQ) en parte de sus deliberaciones.

E.2. Foro de comentario público sobre el Informe Inicial

El 3 de junio de 2021, el equipo responsable del EPDP publicó su Informe Inicial para comentario público. El Informe Inicial destacó las conclusiones del equipo hasta ese momento y estaba destinado a servir como herramienta para solicitar aportes de la comunidad, en particular, sobre áreas donde aún había divergencias significativas. Si bien las recomendaciones preliminares se incluyeron en el Informe Inicial, el equipo responsable del EPDP solicitó que se consideraran estas recomendaciones junto con un conjunto de preguntas planteadas para ayudar a informar la finalización de su informe.

El equipo responsable del EPDP utilizó un formulario de Google para facilitar la revisión de los comentarios públicos. Se recibieron dieciséis 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 brindados están disponibles aquí: https://docs.google.com/spreadsheets/d/1aRxF19pd5tEyO07_zaj7YvzOPjfIBfgi4WRy-nx8yY/edit?resourcekey#gid=1754667842.

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 (consulte https://community.icann.org/x/coMZCg). 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 a realizarse a las recomendaciones o al informe.

Anexo F – Memorandos legales de Bird & Bird

Respuesta a las preguntas 1 y 2 (personas jurídicas vs. físicas)

MEMORANDO

Para:	Corporación para la Asignación de Nombres y Números en Internet, equipo responsable del EPDP
De:	Ruth Boardman y Phil Bradley-Schmieg
Fecha:	6 de abril de 2021
Asunto:	Preguntas de marzo de 2021 sobre personería jurídica, consentimiento, etc.

Información de referencia

1. El EDPB, en una carta de julio de 2018 a Göran Marby, manifestó lo siguiente:

"los datos personales que identifican a los empleados individuales (o a terceros) que actúan en nombre del registratario no deberían estar disponibles públicamente por defecto en el contexto del WHOIS".

Consentimiento

2. El Apéndice A de la Especificación Temporaria establece lo siguiente:

"En las respuestas a las consultas de nombres de dominio, el registrador y el operador de registro DEBEN tratar a los siguientes campos como "omitidos", a menos que el contacto (por ejemplo, administrativo o técnico) haya otorgado el consentimiento para publicar sus datos: (...)".

3. La recomendación 6 del Informe Final de la Fase 1 del EPDP, que adoptó la Junta de la ICANN en mayo de 2019, establece:

"tan pronto como sea comercialmente razonable, el registrador debe ofrecer al titular del nombre registrado la oportunidad de proporcionar su consentimiento para publicar información de contacto editada, así como la dirección de correo electrónico, en el RDS del registrador patrocinador":

4. El Informe Final de la Fase 2 del equipo responsable del EPDP, con fecha 31 de julio de 2020, también señaló, en la nota al pie 83, que:

"Otro tema que alentaría un procesamiento menos manual sería estudiar qué mecanismos permitidos por ley 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".

5. Bird & Bird brindó asesoramiento sobre esta cuestión, en particular, en nuestro memorando con fecha 13 de marzo de 2020, "*Asesoramiento sobre las opciones de consentimiento con el fin de hacer públicos los datos personales en el RDS y los requisitos del [GDPR]*" (el "**Memorando de consentimiento**").

Personas jurídicas vs. personas físicas

6. En mayo de 2019, la Junta Directiva de la ICANN también adoptó la recomendación 17 del Informe Final de la Fase 1 del EPDP, que manifiesta lo siguiente:

"1) El Equipo responsable del EPDP recomienda que los registradores y operadores de registro tengan permitido diferenciar a las registraciones de persona físicas o jurídicas, aunque no están obligados a hacerlo.

2) El equipo responsable del EPDP recomienda que, tan pronto como sea posible, la organización de la ICANN realice un estudio, cuyos términos de referencia sean elaborados en consulta con la comunidad, que considere:

- *La viabilidad y los costos, incluidos los costos de implementación y de posible responsabilidad para diferenciar entre personas físicas y jurídicas;*

- *Ejemplos de industrias u otras organizaciones que han diferenciado entre personas físicas y jurídicas exitosamente;*

- *Riesgos de privacidad para los titulares del nombre registrado ante la diferenciación entre personas físicas y jurídicas; y*

- *Otros posibles riesgos (si los hubiese) para los registradores y registros resultantes de la falta de diferenciación.*

3) El equipo responsable del EPDP determinará y resolverá el asunto de personas físicas vs. jurídicas en la Fase 2".

7. Bird & Bird brindó asesoramiento relevante a esta cuestión, en particular, en:

7.1 nuestro Memorando con fecha 25 de enero de 2019, "*Asesoramiento sobre responsabilidad en relación con la autoidentificación del registratario como persona física o no física en virtud del [GDPR]*" (el **Memorando sobre persona física vs. jurídica**"): y

7.2 nuestro Memorando con fecha 9 de abril de 2020, "*Asesoramiento sobre el principio de exactitud en virtud del [GDPR]: consultas de seguimiento sobre los memorandos "Personas jurídicas vs. físicas" y "Exactitud""* (el "**Memorando de seguimiento sobre exactitud**).

8. Los miembros del EPDP también quizá recuerden que el artículo 83(2) del GDPR enumera los factores que se deben considerar cuando una autoridad supervisora decide si imponer una multa administrativa (y, de ser así, el monto de ella). Entre estos se incluyen la cantidad de titulares de los datos afectados, la naturaleza de los datos, el carácter intencional o negligente de la infracción, las

acciones llevadas a cabo por el responsable del tratamiento de datos para mitigar el daño y el grado de responsabilidad del responsable del tratamiento de datos al tener en cuenta las medidas técnicas y organizacionales que implementó en virtud de los artículos 25 y 32 del GDPR.

9. En entre contexto, ustedes han planteado varias preguntas interrelacionadas.

Pregunta 1

Pregunta presentada: En el marco de la política de consenso adoptada, los registradores brindarán a los registratarios la oportunidad de prestar consentimiento a la publicación de los datos personales incluidos en sus datos de registración. Les pido que comparen los riesgos legales para las partes contratadas asociados con: 1) publicar los datos personales en función del consentimiento del registratario, por un lado, y 2) publicar los datos en función de (i) la autoidentificación que realiza el registratario de los datos respecto de si contienen datos de personas jurídicas solamente o si también contienen datos de personas físicas (organización o individuo) antes de la publicación y (ii) llevar a cabo los procedimientos de verificación descriptos en el memorando de Bird & Bird del 25 de enero de 2019 (es decir, notificar/explicar; confirmar; verificar; oportunidad de corregir), por otro lado.

Análisis

10. Suponemos que esta pregunta, y aquellas que figuran más abajo, se formulan sobre el escenario planteado como una cuestión por el EDPB en su carta a Göran Marby en el párrafo 1 más atrás arriba; es decir, en el caso en que el registratario es una persona jurídica y uno de sus empleados (o agentes) completa una registración en nombre del registratario brinda sus propios datos personales o aquellos de otros titulares de los datos (por ejemplo, al nombrar un colega como contacto administrativo).

11. En dicho escenario, de estas dos medidas, la última (que a los fines de este memorando la denominaremos “Autocaracterización verificada, “VSC”, por sus siglas en inglés) representa un riesgo jurídicamente menor para las partes contratadas. Puede ser posible combinar las dos.

Consentimiento

11.1 Un titular de los datos debe decidir si desea prestar su consentimiento. Esto significa que, en el escenario que se está analizando, la persona que completa la registración de un dominio en nombre del registratario (persona jurídica) solo podría prestar consentimiento a la publicación de sus propios datos personales. No puede prestar consentimiento en nombre de sus colegas u otros (“terceros titulares de los datos”), si se brindan detalles de cualquiera de ellos. En esa situación, sólo podría *transmitir* el resultado de la decisión de consentimiento de ese tercero a una parte contratada.

11.2 En dicho caso, que prevemos que no es algo inusual, la primera opción (dependencia en el consentimiento del registratario) puede hacer que las partes contratadas no puedan demostrar en forma concreta que (i) el tercero titular de los datos realmente prestó consentimiento; o (ii) que dicho

consentimiento cumplió con todos los requisitos del GDPR para que fuera válido (los requisitos se explican en los párrafos 13-18 del Memorando de consentimiento).

11.3 El Memorando de consentimiento presentó cinco opciones para un enfoque guiado por el consentimiento (Memorando de consentimiento, párrafo 24). No resulta claro cuál de estas opciones es considerada con los fines de la presente pregunta.

11.4 El Memorando de consentimiento explicó que:

11.4.1 un esquema en el cual los responsables del tratamiento de datos solicitan consentimiento válido directamente de todos los titulares de los datos (a diferencia de lo que la presente pregunta parece proponer) representaría un riesgo menor que simplemente confiar en las afirmaciones del registratario de que se obtuvo un consentimiento válido de los titulares de los datos; y

11.4.2 *si*, de todas formas, el sistema fuera diseñado en torno a la confirmación del registratario de que obtuvo un consentimiento válido de los titulares de los derechos, sería preferible que las partes contratadas verificaran el consentimiento directamente con las personas o exigiesen que el registratario mostrara *pruebas* de que se obtuvo un consentimiento válido.

Autocaracterización verificada

11.5 La segunda opción brindada en la pregunta presentada, VSC, presumiblemente sugiere que, como regla, los datos personales **no** se publicarán en los datos de registración (y, en caso que se incluyan por defecto, se realizará una verificación que consistirá en ponerse en contacto con el contacto de los detalles proporcionados).

11.6 Por lo tanto, *si* se incluyen datos personales en los datos de registración, esto sería un caso inusual y accidental.[84] En resumen, el GDPR no debería, en su gran mayoría, ser aplicable, salvo en casos excepcionales accidentales.

11.7 En esos casos excepcionales teóricamente inusuales, varios factores mitigarían la responsabilidad de la parte contratada (en particular, en virtud del artículo 83(2) del GDPR, analizado en el párrafo 8 más atrás arriba) – ya sea si se debe a la inexactitud o al tratamiento de datos personales sin fundamento legal (por ejemplo, consentimiento). En particular:

11.7.1 Se tomaron medidas importantes para verificar que los datos no sean datos personales; y

11.7.2 Se proporcionó un medio sencillo para la corrección de errores.

11.8 Puede incluso haber un argumento, basado en jurisprudencia del Tribunal de Justicia de la UE ("CJEU"), de que esta es una situación en la que las partes contratadas solo deberían ser responsables, por lo general, si omiten abordar adecuadamente un reclamo sobre los datos – es decir, solo una vez que reciben una notificación sobre la supuesta ilegalidad y por la cual tienen la oportunidad de "verificar" los méritos del reclamo.[85] Esto conlleva algunos paralelismos con otros regímenes de

[84] Atribuible al propio error del registratario o una falla en los mecanismos de verificación implementados por una parte contratada.

[85] En su dictamen en el Caso C-136/17 *GC y otros*, el CJEU explicó que las obligaciones del GDPR relacionadas con la solicitud de borrado ("Derecho al olvido") se aplican "*al operador de un motor de búsqueda en el marco de sus responsabilidades, facultades y capacidades como el responsable del tratamiento de datos llevadas a cabo en relación*

responsabilidad de la UE para los operadores de servicios en línea que procesan – sin darse cuenta – contenido que infringe la legislación de la UE.[86] Como se analiza en la nota al pie 88 más adelante, esto es posiblemente admitido en (al menos algunas) decisiones de las autoridades supervisoras del GDPR

Combinación

11.9 Si bien la VSC ofrece un riesgo menor para las partes contratadas, tiene una desventaja: significa que los datos personales no son (normalmente) publicados. Para algunas partes interesadas, esto parece una oportunidad perdida para maximizar la disponibilidad de los datos de registración disponibles públicamente.

11.10 Por ende, las partes contratadas pueden considerar una combinación de mecanismos: solicitar que el individuo complete la registración, si los datos que proporciona son datos personales. Si se niega, entonces verificar este reclamo comunicándose con los detalles de contacto suministrados (VSC). En cambio, si acepta, preguntarle si los datos personales se relacionan con él y, de ser así, si desea que se publiquen esos detalles.

11.11 A veces, la exactitud se presenta como una preocupación del GDPR con respecto a la publicación de los datos de registración. Aunque nuestras investigaciones no descubrieron un precedente sustancial para la exigencia de cumplimiento en una situación tal como la que se debate aquí, nos parece que, en el marco de este modelo de combinación (VSC + consentimiento):

11.11.1 Si el registratario (o la persona que lo representa) caracteriza en forma incorrecta los datos personales como no personales, el proceso de verificación que este hecho impulsa debería otorgar protección razonable frente a la responsabilidad del Principio de Exactitud del GDPR para las partes contratadas, como se explica en el párrafo 11.7 más arriba, como podría hacerlo el argumento legal manifestado en el párrafo 11.8 más atrás arriba.

11.11.2 De manera alternativa, si el registratario (o la persona que lo representa) caracteriza en forma incorrecta los datos no personales como datos personales, entonces, ya sea que con posterioridad preste o no consentimiento a su publicación, los datos incluso no serían realmente datos personales, de manera que no puede plantearse la responsabilidad del GDPR.

PREGUNTA 2

Pregunta presentada: Los párrafos 17 al 25 del memorando de Bird & Bird con fecha 25 de enero de 2019 [Memorando sobre personas físicas vs. jurídicas] analizaron los posibles riesgos para los registradores asociados con basarse en (i) la autodesignación como persona jurídica del registratario y (ii) la confirmación de que los datos de registración no contienen

con la actividad del motor de búsqueda, en el caso de una verificación realizada por dicho operador, bajo la supervisión de las autoridades nacionales competentes, después de una solicitud por parte del titular de los datos". Como el Abogado General explicó en ese caso, "dicho operador puede actuar sólo dentro del marco de sus responsabilidades, facultades y capacidades. *En otras palabras, dicho operador puede no tener la capacidad de garantizar el efecto pleno de las disposiciones de [la ley de protección de datos de la UE], precisamente debido a sus responsabilidades, facultades y capacidades limitadas*. . . Un control anterior de páginas de Internet a las que se hace referencia como el resultado de una búsqueda no recae dentro de las responsabilidades o capacidades de un motor de búsqueda". No podría saber, desde el momento que indexó una página web, que el contenido de esa página estaba (por ejemplo) desactualizado (como en el dictamen original de Google Spain / Costeja) o (en el caso GC y otros) eran datos de "categoría especial" o "delito penal" para los que se requirió consentimiento.

[86] Consulte, por ejemplo, el artículo 14 de la Directiva sobre el Comercio Electrónico 2000/31/EC y su transposición a las leyes nacionales de los estados miembro de la UE/EEE y el Reino Unido.

datos personales. Los memorandos identificaron diversos pasos que los registradores podrían realizar para mitigar el riesgo de publicación accidental de datos personales.

Por ejemplo, el memorando sugería que los registradores podrían realizar ciertos pasos para mejorar la exactitud de la autodesignación/afirmación, por ejemplo: brindar divulgaciones independientes y claras, incluidas descripciones de las consecuencias de autodesignación como persona jurídica y solicitar a los registratarios que confirmen que no están presentando datos personales; evaluar la claridad/legibilidad de dichas divulgaciones; correos electrónicos de seguimiento periódicos a los registratarios o contacto técnico; y ofrecer un mecanismo para cambiar la autodesignación, o corregir u objetar la publicación de datos personales.

Pregunta 2(1): Suponiendo que un registrador realiza los pasos de mitigación identificados por Bird & Bird, y en función de su experiencia y precedente aplicable, describa el nivel de riesgo, probabilidad de acciones coercitivas, multas, asesoramiento legal, etc. que surjan de la posterior publicación accidental de datos personales contenidos en los datos de registración de una persona jurídica.

Pregunta 2(2): Ampliando la pregunta [2(1)], describa qué nivel de riesgos (por ejemplo, acciones coercitivas, multas, asesoramiento legal, etc.) enfrenta una parte contratada con respecto a la publicación de datos personales si un correo electrónico de confirmación enviado por un registrador al registratario o a los contactos técnicos del registratario (i) manifiesta en forma clara que el registratario se designó como persona jurídica y aseveró que no se incluyeron datos personales en los datos de registración; (ii) explica que en función de esas dos manifestaciones todos los campos de los datos de registración se publicarán en Internet; y (iii) brinda un mecanismo fácil de usar mediante el cual se pueda rescindir la autodesignación y un individuo que recibe el correo electrónico pueda objetar la publicación de sus datos personales o rectificar cualquier dato inexacto. ¿El registrador debe exigir la respuesta afirmativa del registratario o contacto técnico al correo electrónico de confirmación? ¿La respuesta difiere en función del medio de la notificación (por ejemplo, correo tradicional vs. correo electrónico)?

Pregunta 3(2): ¿Hay pasos adicionales o alternativos de mitigación o verificación que una parte contratada puede realizar para reducir aun más o eliminar la responsabilidad asociada con la publicación accidental de datos personales en relación con la confianza en la autodesignación de un registratario, por ejemplo, confirmar la existencia de identificadores corporativos (Inc., GmbH, Ltd. etc.), revisar los datos del titular de la cuenta en busca de indicios de personaría jurídica, etc.? ¿En qué medida cada uno de dichos pasos adicionales reduciría la responsabilidad?

12. Con respecto a la pregunta 2(1) (*nivel de riesgo, por lo general, si se adoptan las medidas de la VSC descriptas*): a pesar de que hemos buscado precedentes en varios estados miembro de la UE/EEE, no tenemos conocimiento de un precedente comparable. Además, tengan en cuenta que las tendencias de exigencia del cumplimiento y las políticas de acción normativas evolucionan de manera constante, al igual que la viabilidad de juicios civiles por los litigantes.

13. Sin embargo, según nuestro punto de vista, el riesgo para las partes contratadas parece bajo, si toman las medidas descriptas en la pregunta presentada, para evitar que los datos personales se publiquen (o si se reporta, que permanezcan publicados) en los datos de registración.

14. Nuestro punto de vista se basa en los siguientes factores (también teniendo en cuenta el artículo 83 (2) del GDPR, analizado en el párrafo 8 más atrás arriba):

14.1 La inclusión errónea de datos personales, a pesar de las medidas descriptas allí (suponiendo que se implementaron bien) parece que ocurriría solo en casos excepcionales. Como asesoramos en el Memorando sobre personas físicas vs. jurídicas, sería recomendable que la ICANN y las partes contratadas estudiasen (por ejemplo, recopilasen estadísticas) a fin de supervisar si las medidas funcionan de la manera prevista.

14.2 Si se incluyen erróneamente datos personales en los datos de registración publicados, ocurriría en este escenario a pesar de los pasos sustanciales (VSC) realizados por las partes contratadas y se debería principalmente a las acciones/omisiones del registratario. Esto probablemente lo tengan en cuenta los titulares de los datos, las autoridades supervisoras de protección de datos y los tribunales.

14.3 Los datos en cuestión probablemente sean poco sensibles. El escenario previsto aquí (inclusión errónea de datos personales en datos de registración publicados) parece ser el más probable que ocurra cuando una entidad jurídica (por ejemplo, una compañía o una organización sin fines de lucro) registra/mantiene sus propios dominios. En dichos escenarios, suponemos que los datos personales que pueden ser divulgados se relacionarían comúnmente con los detalles laborales de un empleado (por ejemplo, una dirección de correo electrónico de la compañía), no con la vida privada de un individuo. Si bien el GDPR brinda protección incluso en el espacio de trabajo, los datos en cuestión aquí posiblemente pueden causar menos daño a un individuo que los datos relacionados con la vida privada del titular de los datos.[87]

14.4 En casos más sensibles (por ejemplo, divulgar que una persona trabaja en una compañía en un sector sensible o "vergonzante"), un registratario se estaría exponiendo a un riesgo grave de reclamos de sus propios empleados. Por ende, los registratarios ya están incentivados a evitar errores que puedan ocasionar consecuencias graves a su propio personal.

14.5 Las medidas previstas incluyen la posibilidad de corregir el error. Resulta obvio que la naturaleza de la Internet global es que puede resultar difícil eliminar por completo datos publicados por error de espejos /cachés/ archivos, si algunos servicios están configurados para realizar esta acción. Por ende, recomendamos las medidas complementarias previstas para la pregunta 2(2) más abajo.

14.6 Por último, como se señaló anteriormente, es posible basar los argumentos en el caso *GC y otros*, de que la responsabilidad debería ser atribuida a una parte contratada solo si no aborda de manera adecuada los reclamos sobre la inclusión de datos personales en los datos de registración publicados – y no desde el momento anterior de la publicación accidental de los datos. Dicho esto, esto parece ser condicional respecto de que el responsable del tratamiento de datos haya tomado las

[87] Como explicamos anteriormente, entendemos que esta pregunta se refiere a escenarios en los que los registratarios son personas jurídicas, en virtud de la cita del EDPB en el párrafo 1. Con respecto a los registratarios individuales (personas físicas), las cuestiones serán muy similares: si una persona física manifiesta de manera incorrecta que sus datos no son datos personales, entonces (i) las medidas de verificación deberían evitar que se publiquen los datos, dado que brindarán al titular de los datos la oportunidad de corregir su error; (ii) los factores de mitigación y los argumentos jurídicos descriptos en los párrafos 11.7 y 11.8 y en los párrafos 14.1 - 14.6 aquí, deberían otorgar una protección legal razonable para las partes contratadas.

medidas razonables para evitar dicha inclusión (por ejemplo, las medidas de VSC mencionadas en el presente documento).

Con respecto a la pregunta 2(2) (*nivel de riesgo si se envía un correo electrónico de confirmación, que ofrece un medio sencillo de rescindir la autodesignación/rectificar inexactitudes*):

15. Según nuestra opinión, este método de verificación es recomendable y ayudará a reducir el riesgo. Esta reducción del riesgo será mucho mayor si existe un período de gracia razonable dentro del cual se pueda presentar una objeción, *antes* de que los datos en cuestión sean publicados en los datos de registración.

16. Las partes contratadas necesitarían considerar los plazos del correo postal ("correo tradicional") si se usa ese medio – puede demorar un poco que el correo sea entregado a la organización y luego encontrar a la persona correcta (que puede estar fuera de la oficina, por ejemplo, con licencia anual) y luego ser tratado por esa persona. El correo electrónico, por lo general, no tendría esa demora en la entrega; el período de gracia entonces solo necesitaría considerar una posible ausencia en el trabajo o la incapacidad temporaria del destinatario de tratar el correo electrónico por otros motivos.

17. Según nuestro punto de vista, exigir una respuesta afirmativa a los correos de verificación parece demasiado cauteloso, a menos que estudios demuestren que las medidas adoptadas no pueden mantener enormes cantidades de datos personales al margen de los datos de registración publicados. Sin embargo, si un correo electrónico de verificación "rebota" (es decir, una parte contratada sabe que no fue entregado), entonces sería mejor que no se procediera con la publicación (es decir, se debería considerar que la verificación VSC no fue exitosa en ese caso).

18. No podemos excluir la posibilidad de que algunos tribunales o reguladores vean las cosas de otra manera. Aun así, una orden para corregir el problema (probablemente acompañada de un período razonable durante el cual se deban implementar los cambios), en lugar de una multa, parece mucho más probable, teniendo en cuenta los factores del artículo 83(2) del GDPR mencionados en el párrafo 8 más atrás arriba. Después de haber verificado en una selección de estados miembro, no podemos encontrar ejemplos de exigibilidad de cumplimiento al respecto. Por ende, hay pocas pautas disponibles, además de lo estipulado en el mismo GDPR.

19. *Con respecto a la pregunta 2(3) (pasos adicionales o alternativos para reducir la responsabilidad en virtud de la VSC)*: nuestro asesoramiento en los párrafos 21-25 del Memorando de seguimiento sobre exactitud es muy pertinente aquí. Gran parte de esa discusión, y la tabla de 16 posibles medidas adicionales que se podrían realizar para minimizar o compensar posibles inexactitudes en los datos de registración, sigue siendo relevante aquí.

20. La pregunta, tal como la plantearon, ya reitera muchas de esas medidas, a saber: "*brindar divulgaciones independientes y claras, incluidas descripciones de las consecuencias de autodesignación como persona jurídica y solicitar a los registratarios que confirmen que no están presentando datos personales; evaluar la claridad/legibilidad de dichas divulgaciones; correos electrónicos de seguimiento periódicos a los registratarios o contacto técnico; y ofrecer un mecanismo para cambiar la autodesignación, o corregir u objetar la publicación de datos personales*".

21. La pregunta presente también sugiere "*confirmar la existencia de identificadores corporativos (Inc., GmbH, Ltd. etc.) [o] revisar los datos del titular de la cuenta en busca de indicios*

de personaría jurídica". Además, solicitar el número de registración de una compañía puede ser otro medio de verificar la personería jurídica.

22. Dicho eso: muchos empleadores podrán brindar el número de compañía o el nombre de compañía que finaliza en Ltd., PLC, SA, BV, GmbH, *etc.* – y, aun así, podrían brindar datos personales sobre sus empleados, por ejemplo, como contactos para el dominio. En consecuencia, dicha verificación, incluso si fuera viable, solo confirma que el registratario es una persona jurídica. *No* confirma que un registratario que es persona jurídica no ha proporcionado (también) datos personales, por ejemplo, sobre su personal. Entonces, esta medida ayuda a evitar que los registratarios que son personas físicas identifiquen de manera errónea sus propios datos – pero ese no sería un gran riesgo (desde la perspectiva del GDPR), dado que dichas personas en cualquier caso están incentivadas para declarar correctamente su estado como persona física y su declaración puede ser verificada poniéndose en contacto con ellas. El riesgo alternativo y posiblemente mayor – que un empleador incluya los datos personales de sus empleados – no se ve afectado por dicha medida. Por ende, dicha medida tiene beneficios limitados del GDPR.

23. Lo que puede ser útil, de ser factible, sería una herramienta técnica que se use para evaluar si las direcciones de correo electrónico incluyen el nombre de una persona o resultan ser genéricas. Esta medida sola no sería suficiente; las direcciones de correo electrónico pueden estar relacionadas con un individuo que pueda ser identificado (es decir, que sean datos personales), a pesar de no usar su nombre. Dicha herramienta, por lo tanto, solo se puede considerar como parte de un conjunto de medidas. En cuanto a los números de teléfono: si se recopilaran, una herramienta técnica podría verificar los prefijos típicos asociados con los teléfonos celulares (que, por lo general, están vinculados a un solo individuo, quizá con más frecuencia que los números de línea fija).

24. Dichas funciones deberían someterse a evaluaciones exhaustivas, dado que el índice de falsos positivos y falsos negativos puede ser significativo, en especial, dada la naturaleza internacional del sistema de nombres de dominio supervisado por la ICANN (incluso en inglés, suponemos que direcciones de correo electrónico tales como "@johndeere.com" o "@annsummers.com" podrían presentar desafíos).

25. En vez de actuar de manera automática sobre los hallazgos de dichas herramientas, quizá algunas partes contratadas estén preparadas para evaluar "manualmente" los datos sospechosos – si bien esto probablemente implicaría un esfuerzo sustancial en nombre de las partes contratadas. Parece más probable que dicha herramienta en cambio presente un aviso al registratario ("*Parece que ha proporcionado detalles de contacto de una persona individual,* (…)"), mediante el cual le solicita si desea descartar ese aviso o actuar al respecto.

26. Por ende, en principio, dichas herramientas, si se implementan, pueden funcionar mejor un "estímulo" adicional (inteligente y con conocimiento del contenido) para los registratarios, no como un determinante automatizado de si puede proceder con la publicación de los datos.

27. Dada la viabilidad y los méritos poco claros de dicho enfoque, podría ser, por ejemplo, algo guardado como un elemento a más mediano/largo plazo para exploración y pruebas; su desarrollo e implementación completos podrían estar condicionados a mostrar no solo que es técnicamente viable, sino también a que la experiencia muestre que esas medidas adicionales sean, en realidad, necesarias.

28. Por último, no podemos prever ahora otras medidas que se requieran o se esperen de las partes contratadas, además de aquellas ya debatidas en la pregunta presentada.

29. Es posible que existan diferencias de opinión en este punto. Asimismo, gran parte podría dirigirse hacia *cómo* se implementan las medidas sugeridas, incluidas aquellas propuestas en la pregunta presentada. Por ejemplo, existen algunos precedentes en Hungría respecto de cuándo la exactitud de los datos es objetada, el tratamiento de los datos (por ejemplo, la publicación) puede ser suspendido en forma temporaria, salvo en la medida necesaria para verificar y actuar respecto de la inexactitud informada [88] – al parecer, ya sea que el sujeto de datos haya o no invocado de manera explícita al artículo 18(1) del GDPR (derecho a solicitar la restricción de datos mientras se verifican las inexactitudes). Si bien el diseño sugerido aquí no parece requerir o prestarse a dicha suspensión temporaria (dado que lo titulares de los datos podrían rectificar al instante una autocaracterización que consideren inexacta – es decir, las acciones de informar y rectificar deberían ser, por lo general, simultáneas), recomendamos tener esto en cuenta si los planes evolucionan y, en última instancia, resultan en la posibilidad de una diferencia de tiempo entre el informe y la rectificación de los datos inexactos.

30. Explicamos en el Memorando de seguimiento sobre exactitud, en el párrafo 21, que *"la ICANN o las partes contratadas estarán mejor posicionadas para evaluar si los procedimientos actualmente implementados son suficientes o si sería razonable tomar medidas adicionales para cumplir con el principio de exactitud – y, de ser así, evaluar qué medidas serían más adecuadas"*. Ese mismo memorando recomendó en el párrafo 24 que *"[e]l uso de estadísticas y la supervisión del número de solicitudes de corrección de los titulares de los datos también son medidas que podrían contribuir a asegurar un nivel adecuado de exactitud. Por ejemplo, el monitoreo de tendencias en las solicitudes de rectificación podría permitir identificar una brecha de exactitud o donde una medida puede no ser completamente eficaz, y tomar los pasos para cubrir la brecha o reemplazar la medida por una más adecuada"*.

* * *

[88] Decisión de la NAIH en el caso número NAIH/2019/363/2; disponible en línea en https://www.naih.hu/files/NAIH-2019_363_hatarozat.pdf ; a continuación, se incluye una traducción automática del párrafo relevante: La Autoridad acuerda con el [demandante] que el responsable del tratamiento de datos no tiene la obligación de borrar datos en el caso en que la exactitud de los datos anteriormente suministrados por el cliente sea puesta en duda por un tercero y no se demuestre que los datos ya no están a disposición del cliente, sino a disposición de la persona que realiza la notificación. *Sin embargo, las medidas tomadas por el responsable del tratamiento de datos en función de la notificación deberían promover el principio de exactitud e impedir el uso de datos inexactos*. En dicho caso, la Autoridad considera que el responsable del tratamiento de datos debería limitar, en forma temporaria, el tratamiento de datos inexactos mediante la aplicación de medidas razonables".

Respuesta a la pregunta 3 (personas jurídicas vs. físicas)

M E M O R A N D O

Para:	Corporación para la Asignación de Nombres y Números en Internet, equipo responsable del EPDP
De:	Ruth Boardman y Phil Bradley-Schmieg
Fecha:	27 de abril de 2021
Asunto:	Pregunta de marzo de 2021 en referencia a la UE y el reconocimiento de intereses de publicación de datos de registración por terceros

Información de referencia

31. El EDPB, en una carta de julio de 2018 a Göran Marby ("Carta del EDPB de julio de 2018").[89] manifestó lo siguiente:

"los datos personales que identifican a los empleados individuales (o a terceros) que actúan en nombre del registratario no deberían estar disponibles públicamente por defecto en el contexto del WHOIS".

32. Esto ha generado varias preguntas relacionadas con el GDPR, más recientemente en nuestro memorando con fecha 6 de abril de 2021 ("**Memorando de opciones de consentimiento y VSC**"), en el cual se analizaron dos preguntas ("**Pregunta 1 y Pregunta 2**") que debaten dos enfoques diferentes (y los riesgos resultantes) con respecto a (i) publicación de datos de registro condicionada al consentimiento; y (ii) publicación de datos de registración si se relacionan (sólo) con una persona jurídica (por ejemplo una empresa), en lugar de ser datos personales (y cómo estos se pueden verificar) – es decir, Autocaracterización verificada, "VSC".

33. También preguntaron, en la pregunta presentada más abajo, si ciertas disposiciones de la legislación de la UE o las prácticas de dos terceros (EURid y el RiPE NCC), crean precedentes útiles en este ámbito. Este memorando aborda esa tercera pregunta.

Pregunta presentada: La reglamentación de la Comisión (EC) N.° 874/2004 del 28 de abril de 2004 que estipula reglas de política pública concernientes a la implementación y las funciones del dominio de alto nivel .eu y los principios que rigen la registración ('Reglamentación de .eu') establece las reglas de política pública concernientes a la implementación y las funciones del dominio de alto nivel (TLD) .eu y los principios de política pública sobre registración de nombres de dominio en el TLD .eu.

El artículo 16 de la reglamentación de .eu se titula 'base de datos de WHOIS' y proporciona:

[89] Carta del EDPB a Göran Marby con fecha 5 de julio de 2018, disponible en línea en https://edpb.europa.eu/sites/default/files/files/news/icann_letter_en.pdf

'El propósito de la base de datos de WHOIS será brindar información razonablemente exacta y actualizada sobe los puntos de contacto administrativos y técnicos que gestionan los nombres de dominio bajo el TLD .eu.

La base de datos de WHOIS contendrá información sobre el titular de un nombre de dominio que sea relevante y no excesiva en relación con el propósito de la base de datos. En cuanto a la información que no sea estrictamente necesaria en relación con el propósito de la base de datos y si el titular del nombre de dominio es una persona física, la información que se colocará para que esté disponible públicamente estará sujeta al consentimiento inequívoco del titular del nombre de dominio. La presentación intencional de información inexacta constituirá un fundamento para considerar que la registración del nombre de dominio ha incumplido los términos de la registración'.

A partir del 13 de octubre de 2022, la reglamentación de .eu será reemplazada por la reglamentación 2019/517, la cual estipula, en el artículo 12, denominado base de datos de WHOIS:

'*1. El registro establecerá y gestionará, con debida diligencia, un servicio de base de datos de WHOIS con el fin de garantizar la seguridad, estabilidad y flexibilidad del TLD .eu; para ello, suministrará información de registración exacta y actualizada sobre los nombres de dominio bajo el TLD .eu.*

2. La base de datos de WHOIS contendrá información relevante sobre los puntos de contacto que administran los nombres de dominio bajo el TLD .eu y los titulares de los nombres de dominio. La información sobre la base de datos de WHOIS no deberá ser excesiva en relación con el propósito de la base de datos. El registro deberá cumplir con la reglamentación (UE) 2016/679 del Parlamento Europeo y del Consejo'.

En la actualidad, la base de datos de WHOIS es administrada por EURid, una organización sin fines de lucro designada por la Comisión Europea para administrar el registro .eu. En su base de datos del WHOIS, el Registro Europeo de Dominios de Internet (EURid) publica las direcciones de correo electrónico de registratarios de nombres de dominio en el TLD .eu (tanto personas físicas como jurídicas). EURid distingue entre personas físicas y entidades jurídicas mediante la publicación de la información de dirección postal de las entidades jurídicas, mientras que no publica esta información cuando se trata de personas físicas.

Mediante el artículo 16 de la reglamentación de .eu, EURid puede basarse en el artículo 6(1)(e) del GDPR, el cual brinda un fundamento legal para tratar los datos personales que sean necesarios para la realización de una tarea llevada a cabo en pos del interés público o en el ejercicio de la autoridad oficial representada en el responsable del tratamiento de datos. Si bien entendemos que el fundamento de interés público de este artículo 16 no está disponible fuera del dominio .eu, la existencia de este fundamento legal para el tratamiento de los datos de EURid podría ser interpretado como que sugiere que la legislatura de la UE reconoció que la divulgación de los datos del registratario sirve un interés legítimo para la estabilidad, seguridad y flexibilidad. Además, para el cumplimiento de su mandato en

virtud del artículo 16, EURid determinó que la publicación del correo electrónico del registratario "no sea excesiva en relación con el propósito de la base de datos".

De manera similar, si bien el RIPE-NCC se basa en el consentimiento para publicar información personal sobre contactos técnicos/administrativos, publica la información personal sobre los titulares de recursos basándose en el fundamento de que "facilitar la coordinación entre los operadores de redes es el propósito principal que justifica la publicación de datos personales en la base de datos del RIPE-NCC y de que es evidente que el tratamiento de los datos personales que hacen referencia a un titular de recursos es necesario para que el registro desempeñe su función, la cual se lleva a cabo en pos del interés legítimo de la comunidad de RIPE y el funcionamiento sin problemas de Internet a nivel mundial (y, por ende, está de conformidad con el artículo 6.1.f del GDPR)".

Comprendemos que el fundamento de interés público estipulado en el artículo 16 no está disponible para las partes contratadas fuera del dominio de alto nivel .eu. En función de su experiencia y los precedentes aplicables, ¿en qué medida, si corresponde: (i) la existencia del artículo 16 de la reglamentación de la UE; (ii) la decisión de EURid de publicar las direcciones de correo electrónico del registratario en consonancia con el artículo 16, (iii) decisión del RIPE-NCC de publicar las direcciones de correo electrónico de los titulares de recursos; y (iv) lenguaje preliminar respecto del acceso a los datos de registración en la recién propuesta Directiva NIS2 crean precedente de que reducirían el riesgo de la parte contratada en relación con la publicación de la dirección de correo electrónico del registratario que es una persona jurídica, incluso si contiene información personal? ¿Estos hechos afectan a sus respuestas a las Preguntas [1-2]? Si no afectan a sus respuestas, explique por qué.

34. Creemos que, en general, los documentos citados no afectan a nuestras respuestas a las Preguntas 1 y 2 del Memorando de Opciones de consentimiento y VSC. De manera más específica, creemos que los documentos citados limitaron el impacto en el riesgo de las partes contratadas en relación con la publicación de la dirección de correo electrónico de un registratario que es una persona jurídica, incluso si contenía datos personales. Nuestro punto de vista se basa en los motivos manifestados a continuación.

La reglamentación (UE) 2019/517, que reemplaza a la reglamentación de la Comisión (EC) N.° 874/2004 (la "reglamentación nueva de .EU")

35. Cuando la reglamentación (UE) 2019/517 (la "reglamentación nueva de .EU) reemplace a la reglamentación de la Comisión (EC) N.° 874/2004 (la "antigua reglamentación de .EU"), eliminará una disposición de la reglamentación antigua de .EU que permitía la publicación "no estrictamente necesaria" de datos personales en los datos de registración (si el titular de los datos había prestado consentimiento expreso para ello). Se citan las disposiciones relevantes en la pregunta presentada.

36. La reglamentación nueva de .EU no manifiesta, en forma expresa, que un enfoque basado en el consentimiento haya demostrado ser poco práctico o que no cumple con las normas; sólo no ofrece comentarios sobre dicho enfoque. De hecho, la reglamentación nueva de .EU ahora no expresa ningún comentario específico sobre la publicación de datos personales, si son "estrictamente necesarios" o algo distinto. Se limita a exigir que el tratamiento de datos cumpla con el GDPR (si corresponde), sin mencionar cómo. En particular, la cláusula 22 de la reglamentación (UE) 2019/517 requiere, en

particular, que el registro de .eu opte por una implementación de la base de datos de WHOIS y los sistemas relacionados que cumpla con la "protección de datos personales desde el diseño y protección de datos por defecto", "necesidad" y "proporcionalidad".

37. La referencia más directa a la distribución de los datos de registración, si son datos personales, puede encontrarse en la cláusula 21. Esta menciona solo el intercambio de datos con los *organismos de cumplimiento de la ley* o el acceso que estos organismos tienen, en virtud de "[UE) o leyes nacionales" – *no* del público en general *ni* de las partes interesadas como los titulares de derechos de propiedad intelectual:[90]

"21. El registro debería brindar apoyo a los organismos de cumplimiento de la ley en la lucha contra el delito mediante la implementación de medidas técnicas y organizacionales dirigidas a permitir que las autoridades competentes tengan acceso a los datos del registro a los efectos de la prevención, detección, investigación y proceso judicial de delitos, tal como lo estipula la legislación nacional o de la Unión".

38. En esencia, la reglamentación nueva de .EU manifiesta aquí una posición que es, en gran medida, neutral y poco concluyente. Por lo general, posterga los requisitos del GDPR y, *de manera específica*, exige respetar la proporcionalidad y la privacidad por defecto. El hecho de que debate el acceso legítimo por grupos de partes interesadas específicos no necesariamente excluye un sistema en el cual algunos datos se hagan públicos, por ejemplo, con el consentimiento del titular de los datos. No obstante, la reglamentación nueva de .EU omitió palabras (encontradas en su predecesor) que aceptan, de manera explícita, un enfoque fundado (en parte) en el consentimiento; es posible que un tribunal o una autoridad supervisora pueda solicitar extraer una conclusión contraria de esto.

Confianza de EURid en el fundamento legal de "tarea pública" del GDPR

39. La pregunta presentada sugiere que EURid se basa en el artículo 16 de la antigua regulación de .EU para afirmar que su publicación (parcial) de los datos personales de los registratarios está permitida en virtud del artículo 6(1)(e) del GDPR.

40. El artículo 6(1)(e) del GDPR permite el tratamiento de datos necesario para la realización de una tarea llevada a cabo en pos del interés público o en el ejercicio de la autoridad oficial conferida al responsable del tratamiento de datos. Estos deben estar estipulados en la legislación de la UE o de un estado miembro de la UE.

41. Si la sugerencia de la pregunta es correcta,[91] entonces EURid asevera, de manera implícita, que dicha publicación es "estrictamente necesaria en relación al propósito de la base de datos". Si ese no

[90] Otras referencias a intereses más amplios no analizan el intercambio de datos de los registratarios con dichos organismos. Por ejemplo, la cláusula 20 estipula: "[e]l registro debería adoptar políticas claras destinadas a garantizar la identificación oportuna de nombres de dominios de registración abusivos y, donde sea necesario, debería cooperar con las autoridades competentes y otros organismos públicos relevantes a la ciberseguridad y seguridad de la información que participan específicamente en la lucha contra dichas registraciones, tales como los equipos de respuesta ante emergencias informáticas (CERT) nacionales". La "cooperación *podría* comprender el intercambio de datos personales, pero (quizá de manera intencional), la reglamentación nueva de .EU no manifiesta nada sobre esta cuestión.

[91] No pudimos confirmar esto; la actual notificación de privacidad de EURid no manifiesta de manera específica qué fundamento legal del GDPR justifica la publicación de datos de registración, si bien manifiesta que "Tenemos la obligación de mantener una base de datos completa y exacta de todos los nombres de dominio registrados. El servicio de búsqueda de WHOIS (https://whois.eurid.eu/en/ tiene como objetivo brindar información exacta y actualizada sobre las personas de contacto técnico y administrativo que gestionan los nombres de dominio. Esto nos ayuda a crear y mantener un entorno de Internet confiable y seguro". La referencia a las publicaciones que son "requeridas" parece estar en consonancia con el artículo 6(1)(e) (tarea pública) *o* el artículo 6(1)(c) (obligación legal) del GDPR.

fuera el caso, EURid estaría operando en incumplimiento del artículo 16 de la antigua reglamentación de .EU, dado que este manifiesta que "En cuanto a la información que no sea estrictamente necesaria en relación con el propósito de la base de datos y si el titular del nombre de dominio es una persona física, la información que se colocará para que esté disponible públicamente estará sujeta al consentimiento inequívoco del titular del nombre de dominio". Basándonos en la pregunta planteada, entendemos que EURid no obtiene dicho consentimiento.

42. Por otro lado, esta supuesta posición indica que al menos un registro (EURid) propugna la importancia ("necesidad estricta") de publicar (algunos) datos en el WHOIS incluso si son datos personales, y sin consentimiento o medidas como VSC (siempre que, al menos, se omitan algunos de los datos personales, según la política de EURid sobre el tema).[92]

43. Sin embargo, la visión que tiene EURid no refleja necesariamente las visiones de los tribunales o autoridades supervisoras que exigen el cumplimiento del GDPR – y no es vinculante para ellos. Es la visión de un registro, entre otros. El hecho de que las políticas de este registro en particular también estén sujetas a la supervisión de la Comisión Europea[93] tiene el casi el mismo valor de precedente limitado; incluso si, en forma hipotética, esta es una pregunta que se haya debatido entre EURid y la Comisión Europea, esta última no exige el cumplimiento del GDPR ni habla por aquellos que sí lo exigen.

44. La pregunta presentada además expresa que "EURid distingue entre personas físicas y entidades jurídicas mediante la publicación de la información de dirección postal de las entidades jurídicas, mientras que no publica esta información cuando se trata de personas físicas". La política de registración actual de EURid explica que "En los casos en que no se especifica el nombre de una empresa u organización, la persona que solicita la registración del nombre de dominio será considerada el registratario; si se especifica el nombre de la empresa u organización, la empresa u organización es considerada el registratario".

45. Esto puede significar que se supone que los detalles postales suministrados por una organización (un registratario que es persona jurídica) *no* contienen datos personales; o simplemente que, si los contiene, estos son estrictamente necesarios o de bajo riesgo para las personas. EURid, como el responsable del tratamiento de los datos en cuestión, estará mejor posicionado que nosotros para determinar si dicha suposición es verdadera en la práctica.

46. Incluso si dicha suposición es, hipotéticamente, verdadera para EURid y las direcciones postales que publica como datos de registración de .eu de personas jurídicas, notamos que, en vista de los comentarios del EDPB a la ICANN,[94] quizá no sea recomendable extrapolar de esta a otra

[92] Notamos con interés que la pregunta planteada afirma que EURid invoca el artículo 6(1)(e) del GDPR – tarea en pos del interés público / autoridad pública – *no* el artículo 6(1)(f) del GDPR, intereses legítimos. EURid no es una autoridad pública, por lo que, en principio, tiene la capacidad de invocar intereses legítimos para su publicación de datos personales. No tenemos conocimiento del razonamiento de EURid para evitar el fundamento de "intereses legítimos" y, por ende, no podemos ofrecer un comentario sustancial sobre esta observación; dicho esto, es posible que no sea útil/confiable para otras partes contratadas; a diferencia de EURid, la mayoría de las partes contratadas se basan en el artículo 6(1)(e) del GDPR porque, a diferencia de EURid, no hay legislación de la UE o de estados miembro que avale su propio tratamiento de datos relacionado con el WHOIS.

[93] Por ejemplo, la cláusula 11 de la reglamentación nueva de .EU indica: "La Comisión debería celebrar un contrato con el registro designado, que debería incluir los principios y procedimientos detallados que se apliquen al registro para la organización, administración y gestión del TLD .eu".

[94] "El mero hecho de que un registratario sea una persona jurídica no necesariamente justifica la publicación ilimitada de datos personales relacionados a personas físicas que trabajan para dicha organización o que la representan", tales como personas físicas que gestionan cuestiones administrativas o técnicas en nombre del registratario. Por ejemplo, la publicación de la dirección de correo electrónico personal de una persona de contacto técnico que consta de firstname.lastname@company.com puede revelar información respecto de su empleador actual, así como su función

información de contacto (por ejemplo, direcciones de correo electrónico, que pueden referirse específicamente a una persona pueda ser identificada fácilmente dentro de la organización).

47. En función de dichas observaciones, además de una apreciación de que EURid opera dentro de un marco legislativo de algún modo único que le brinda la opción de basarse en algo que no sea el consentimiento ni los intereses legítimos – a diferencia de otras partes contratadas – es, por ende, difícil llegar a una conclusión general respecto del enfoque de EURid.

Decisión de RIPE NCC de publicar las direcciones de correo electrónico de los titulares de recursos

48. La pregunta planteada cita la publicación de un blog de 2018 escrito por el Director de Asuntos Legales de RIPE NCC, titulado "Cómo estamos implementando el GDPR: Fundamentos legales para el tratamiento de datos personales legítimos y la base de datos de RIPE".

49. En dicha publicación del blog, como la pregunta planteada indica de manera correcta, el RIPE NCC manifiesta que se basa en los intereses legítimos (fundamento legal del artículo 6(1)(f) del GDPR) para publicar datos personales, en particular, detalles de contacto, para colaborar con el funcionamiento adecuado de un importante sistema de Internet.

50. No obstante, se debería tener en cuenta que la publicación del blog también expresa:

"Sin embargo, cuando el titular de recursos designa a otra persona para desempeñar esta función [es decir, como punto de contacto], debe obtener el consentimiento de la persona cuyos datos personales se incluirán en la base de datos de RIPE antes de que se incluyan sus datos (en consonancia con el artículo 6.1.a dl GDPR)."

51. En otras palabras, nos parece que cuando el titular de recursos es una persona jurídica, (i) el RIPE NCC considera a los intereses legítimos como un fundamento legal adecuado en casos de primera parte (es decir, cuando la persona que completa/actualiza una registración brinda sus propios detalles de contacto y, por ende, es el titular relevante de los datos), pero (ii) el RIPE NCC, en cambio, había (al menos, en 2018 preferido hacer esto sólo con el consentimiento del titular de los datos en casos de terceros (por ejemplo, cuando los detalles de contacto son de un colega de la persona que completa/actualiza la registración).

52. Esta distinción puede deberse al temor de que sería más difícil aseverar que los propios intereses del tercero estén alineados con aquellos del titular de recursos o el RIPE NCC (y las partes interesadas relacionadas); o el temor de que haya riesgos mayores para terceros titulares de los datos (por ejemplo, porque es más difícil suministrar una notificación de privacidad del GDPR a ellos, por lo que pueden tener menos conocimiento de sus derechos). Dichas preocupaciones, por ende, pueden haber impulsado al RIPE NCC a preferir depender del consentimiento de aquellos en situaciones donde participan "terceros".

53. Si bien el RIPE NCC debe solicitar su propio asesoramiento legal sobre la cuestión, nuestro punto de vista en cuanto al EPDP de la ICANN es que no es necesario que dicha distinción sea exigida por ley. El artículo 6(1)(f) del GDPR (el fundamento de intereses legítimos) no exige que los intereses del titular de los datos estén alineados con aquellos de los responsables del tratamiento de datos – simplemente, debe haber un *equilibrio* adecuado entre los intereses en juego (aquellos del responsable del tratamiento de datos o de terceros), en comparación con los "derechos y libertades fundamentales

dentro de la organización. Junto con la dirección del registratario, también puede revelar información sobre su lugar de trabajo". Carta del EDPB de julio de 2018, en la pág. 5.

del titular de los datos que requieren la protección de los datos personales". En este caso, el RIPE NCC y sus propios asesores legales tendrán la mejor visión respecto de los diversos intereses y riesgos, aunque a nosotros nos parece que:

53.1 Los intereses *del responsable del tratamiento de datos y de las partes interesadas en general* parecerían generalmente idénticos, ya sea que se trate de los detalles de contacto de una primera persona o de un tercero; por ejemplo, cualquier conjunto de detalles de contacto suponen ser importantes para la investigación y resolución adecuadas de interrupciones a un sistema clave de Internet;

53.2 En cuanto a los riesgos, los detalles de contacto de primeras personas o de terceros podrían ser usados indebidamente de igual modo, por ejemplo, para marketing no deseado; puede haber otros tipos de riesgo, pero, una vez más, aquellos parecen ser probablemente similares ya sea que se trate titulares de datos que sean primera parte o terceros;

53.3 En cuanto a la notificación, el GDPR acepta de manera específica que habrá situaciones en las que los datos no son recopilados directamente de un titular de los datos y, por ende, se debe entregar una notificación a ellos (consulte, en particular, el artículo 14(5) del GDPR). Por ende, esto no es un motivo automático para descartar el posible uso de intereses legítimos en casos donde participan terceros; y

53.4 Este puede ser el motivo por el cual la carta del EDPB dirigida a la ICANN en junio de 2018, avaló la posible dependencia en los intereses legítimos incluso para los datos de terceros, y manifestó que los registratarios no están *obligados* a brindar dichos datos de terceros, pero pueden, en cambio, brindar los propios.[95] Entendemos que este es realmente el caso para el sistema supervisado por el RIPE NCC.

54. Es probable que el RIPE NCC considere que los reguladores y los tribunales, en principio, aceptarían la autonomía y el control que ofrece la dependencia en el consentimiento, en vez de un fundamento legal no consensuado del GDPR como los intereses legítimos. No obstante, dichas autoridades pueden también reconocer las desventajas prácticas de dicho enfoque:

54.1 La misma publicación del blog de RIPE NCC reconoce las dudas que a veces giran en torno al consentimiento obtenido en los contextos laborales (es decir, que dicho consentimiento, si lo solicita un empleador, puede no haber sido prestado libremente por un empleado).

54.2 El RIPE-NCC también termina dependiendo de las manifestaciones de la primera persona de la que obtuvo un conocimiento válido del tercero ("El RIPE NCC considera que es responsabilidad del que introduce los datos en la base de datos de RIPE (es decir, el responsable de mantenimiento) garantizar que haya obtenido el consentimiento válido para que se realice el tratamiento de los datos"). Esto dificultaría, en teoría, que el RIPE NCC (como responsable del tratamiento de datos) demuestre que dichos consentimientos cumplieron con todos los requisitos del GDPR.

54.3 Las partes contratadas podrían enfrentar las mismas cuestiones del GDPR con respecto a los datos de registración de nombres de dominio.

[95] Carta del EDPB de julio de 2018, en las págs. 2-3.

55. Los puntos de vista del RIPE NCC, como los de EURid, no necesariamente reflejan la posición de las autoridades encargadas del cumplimiento efectivo del GDPR, y ciertamente no son vinculantes para ellas.

56. Además, el ejercicio de equilibrio de intereses legítimos que realizará el RIPE NCC es diferente de aquel de la ICANN y las partes contratadas; los datos en cuestión se relacionan con diferentes recursos (IPv4, IPv6 y recursos de Números de AS, por lo general, asignados por el RIPE NCC – en bloques – a organizaciones muy grandes; en comparación con nombres de dominios específicos que a veces son registrados por personas específicas para uso privado).

57. Por ende, es difícil llegar a una conclusión general desde el enfoque del RIPE NCC.

Lenguaje preliminar respecto del acceso a los datos de registración en la Directiva NIS2 recién propuesta

58. En diciembre de 2020, la Comisión Europea publicó su versión preliminar de una directiva revisada sobre medidas para un alto nivel común de ciberseguridad en la Unión ("NIS2").

59. Las cláusulas de la Directiva NIS2 propuesta estipulan lo siguiente:

"15. Defender y preservar un sistema de nombres de dominio (DNS) confiable, flexible y seguro es un factor clave para mantener la integridad de Internet y es esencial para su funcionamiento continuo y estable, ya que de ello dependen la sociedad y la economía digital. Por lo tanto, esta Directiva se debería aplicar a todos los proveedores de servicios de DNS junto con la cadena de resolución del DNS, incluidos operadores de servidores de nombres raíz, servidores de nombres de dominio de alto nivel (TLD), servidores de nombres autoritativos para nombres de dominio y resolutores recursivos.

(…)

(59) Mantener bases de datos exactas y completas de nombres de dominio y datos de registración (denominados 'datos de WHOIS') y brindar acceso legítimo a dichos datos es esencial para garantizar la seguridad, estabilidad y flexibilidad del DNS, que, a cambio, contribuye a un alto nivel común de ciberseguridad dentro de la Unión. En los casos en que el tratamiento incluya datos personales, dicho tratamiento deberá cumplir con las leyes de protección de datos de la Unión.

(60) La disponibilidad y accesibilidad oportuna de estos datos a autoridades públicas, incluidas las autoridades bajo la Unión o legislación nacional para la prevención, investigación o proceso judicial de delitos penales, CERT, CSIRT, y con respecto a los datos de sus clientes a proveedores de redes de comunicaciones electrónicas, y servicios y proveedores de tecnologías de seguridad, y servicios que actúan en nombre de dichos clientes, son esenciales para evitar y combatir el uso indebido del Sistema de Nombres de Dominio, en particular, para impedir, detectar y responder a incidentes de ciberseguridad. Dicho acceso debería cumplir con las leyes de protección de datos de la Unión en lo que respecta a los datos personales.

(61) A fin de garantizar la disponibilidad de datos de registración de nombres de dominio exactos y completos, los registros de TLD y las entidades que prestan servicios de registración de nombres de dominio para TLD (denominados registradores) deberían recopilar y garantizar la integridad y disponibilidad de los datos de registración de nombres de dominio. En particular, los registros de TLD y las entidades que prestan servicios de registración de nombres de dominio para TLD deberían establecer políticas y procedimientos para recopilar y mantener datos de registración exactos y

completos, así como para evitar y corregir datos de registración inexactos de conformidad con las normas de protección de datos de la Unión.

(62) Los registros de TLD y las entidades que prestan servicios de registración de nombres de dominio para ellos deberían hacer que estén disponibles públicamente los datos de registración de nombres de dominio que no están incluidos en el alcance de las normas de protección de datos de la Unión, como los datos que corresponden a personas jurídicas. Los registros de TLD y las entidades que brindan servicios de registración de nombres de dominio para TLD deberían también permitir el acceso legítimo a datos de registración de nombres de dominio específicos concernientes a personas físicas a solicitantes de acceso legítimos, de conformidad con las leyes de protección de datos de la Unión. Los estados miembro deberían garantizar que los registros de TLD y las entidades que prestan servicios de registración de nombres de dominio para ellos respondiesen, sin demora indebida, a las solicitudes de los solicitantes de acceso legítimo respecto de la divulgación de datos de registración de nombres de dominio. Los registros de TLD y las entidades que brindan servicios de registración de nombres de dominio para ellos deberían establecer políticas y procedimientos para la publicación y divulgación de datos de registración, incluidos acuerdos de nivel de servicio para tratar solicitudes de acceso de solicitantes de acceso legítimos. El procedimiento de acceso puede incluir el uso de una interfaz, un portal u otra herramienta técnica para proporcionar un sistema eficaz de solicitud y acceso a los datos de registración". Con la visión de proporcionar prácticas armónicas en todo el mercado interno, la Comisión puede adoptar pautas sobre dichos procedimientos, sin perjuicio de las competencias del Comité Europeo de Protección de Datos.

(…)

69. El tratamiento de datos personales, en la medida que sea estrictamente necesario y proporcionado a los efectos de garantizar la seguridad de las redes y la información por las entidades, autoridades públicas, CERT, CSIRT y proveedores de servicios y tecnologías de seguridad debería constituir un interés legítimo del responsable del tratamiento de datos implicado, tal como se hace referencia en la Reglamentación (UE) 2016/679. Se deberían incluir medidas relacionadas con la prevención, detección, análisis y respuesta a incidentes, medidas para crear conciencia en relación con amenazas cibernéticas específicas, intercambio de información en el contexto de la solución de vulnerabilidades y divulgación coordinada, así como el intercambio voluntario de información sobre dichos incidentes, y amenazas cibernéticas y vulnerabilidades, indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración. Dichas medidas pueden requerir el tratamiento de los siguientes tipos de datos personales: direcciones IP, localizadores uniformes de recursos (URL), nombres de dominio y direcciones de correo electrónico".

60. Las cláusulas 59-62 inclusive están entonces reflejadas en el artículo 23 de la Directiva NIS2 preliminar.

61. Las cláusulas 15, 59-61 inclusive y 69, y el artículo 23(1-3) de la Directiva NIS2, apoyan ampliamente el tratamiento de datos de registración completo, siempre que se cumpla con el GDPR. La última oración de la cláusula 61 también respalda en forma expresa las medidas diseñadas para promover el cumplimiento del principio de exactitud del GDPR, tal como aquellas mencionadas en nuestros memorandos anteriores.

62. Sin embargo, la cláusula 62 y el artículo 23(4-5) son más específicamente relevantes a las cuestiones en discusión en este memorando, ya que se refieren a la publicación/difusión de datos de registración, no solo a su mera recopilación y retención. Dichas disposiciones de la Directiva NIS2 marcan una distinción clara entre datos personales y no personales, y solo respaldan de manera expresa la publicación de datos no personales. Con respecto a los datos personales, la Directiva NIS2

se limita a analizar lo que parece ser *acceso restringido* por "los solicitantes de acceso legítimos, de conformidad con las leyes de protección de datos de la Unión" (y la redacción equivalente del artículo 23(5)).

63. Según nuestro punto de vista, por ende, la actual Directiva NIS2 preliminar no parece considerar un sistema en el cual algunos datos personales puedan estar abiertamente publicados (de manera legítima), por ejemplo, con el consentimiento del registratario. No resulta claro si esto se debe solo a que los redactores no consideraron esa opción *o* a que los redactores no consideraron que dicho enfoque merecía la pena o que cumplía con los requisitos. Sin embargo, significa que la actual Directiva NIS2 preliminar no ofrece un apoyo/reducción del riesgo importante para un sistema basado, por ejemplo, en el consentimiento del registratario (aunque tampoco subestima de manera expresa dicho enfoque).

* * *

Respuesta a la pregunta 4 (respecto de las opciones para enmascaramiento de direcciones de contacto)

MEMORANDO

Para:	Corporación para la Asignación de Nombres y Números en Internet, equipo responsable del EPDP
De:	Ruth Boardman y Phil Bradley-Schmieg
Fecha:	9 de abril de 2021
Asunto:	Respuesta a la pregunta 4 respecto de las opciones para enmascaramiento de direcciones de contacto

---

Información de referencia

64. El Comité Europeo de Protección de Datos ("EDPB"), en una carta de julio de 2018 a Göran Marby, manifestó lo siguiente:

"los datos personales que identifican a los empleados individuales (o a terceros) que actúan en nombre del registratario no deberían estar disponibles públicamente por defecto en el contexto del WHOIS".

65. Frente a este contexto y en función de asesoramiento anterior que recibieron en esta cuestión, ustedes plantearon la siguiente pregunta.

Pregunta presentada: El memorando de B&B con fecha 4 de febrero de 2020 respecto de la información de contacto de correo electrónico analizó dos opciones: (a) un "contacto de correo electrónico seudónimo" donde el titular de los datos usa una única cadena de caracteres para varias registraciones, y (b) un "contacto de correo electrónico anónimo" donde una cadena de caracteres de correo electrónico única distinta se usa para cada una de dichas registraciones. B&B opinó que la publicación de (a) o (b) sería tratada como publicación de datos personales en la Web porque el fin de hacer que esta dirección de correo electrónico enmascarada esté disponible es permitir que terceros se contacten directamente con el titular de los datos y que los terceros con intereses legítimos y proporcionados tengan acceso a los datos subyacentes.

En la revisión, el Equipo de Asuntos Legales del EPDP ha propuesto describir las opciones (a) y (b) propuestas de la siguiente manera:

- La frase "contacto de correo electrónico seudónimo" (opción (a)) debería ser reemplazada por la frase "**contacto de correo electrónico basada en el registratario**" que se define como: "un correo electrónico para todos los dominios registrados por un único registratario, *que tiene la intención de ser datos seudónimos al ser tratados por terceros usuarios* (es decir, partes no contratadas). (La pregunta de si el correo electrónico debería

ser común entre los registradores acreditados por la ICANN requiere una determinación de políticas A DEFINIRSE).

- La frase "contacto de correo electrónico anónimo" (opción (b)) debería ser reemplazada por la frase "**contacto de correo electrónico basado en la registración**", que se define como "un correo electrónico de uso exclusivo separado para cada nombre de dominio registrado por un registratario único*, que tiene el fin de ser datos prácticamente o "esencialmente" anónimos cuando son tratados por terceros usuarios* (es decir, partes no contratadas)".

Al responder las preguntas que se incluyen a continuación, por favor, suponga, a los efectos de análisis, que terceros usuarios de la información de contacto de correo electrónico basado en la registración no pueden identificar al titular de los datos sin un esfuerzo desproporcionado de manera que el riesgo de identificación parezca, en realidad, ser insignificante.

1. Basándose en su experiencia y precedente aplicable, por favor, compare el nivel de riesgo, probabilidad de acciones coercitivas, multas, asesoramiento legal, etc. asociados con (a) publicación en la Web o (b) divulgación automática de (i) un contacto de correo electrónico basado en el registratario, por un lado, y (ii) un contacto de correo electrónico basado en la registración, por el otro. Al responder esta pregunta considere:
   a. Si el supuesto hecho de que el riesgo de identificación del titular de los datos por un tercero (es decir, parte no contratada) mediante el contacto de correo electrónico basado en la registración parece ser insignificante, ¿esto haría que dichos correos electrónicos sean eficazmente "anónimos" con respecto a terceros bajo la norma *Breyer*?
   b. De no ser así, ¿de qué manera la elección del contacto de correo (basado en el registratario o en la registración) afectaría el resultado de la prueba de equilibrio de intereses legítimos en virtud del artículo 6(1)(f)? ¿En qué medida el uso de un contacto de correo electrónico basado en la registración reduciría el impacto de publicación en los intereses o derechos fundamentales y libertades del titular de los datos?

¿La respuesta a estas preguntas cambia si el propósito principal de publicar un correo electrónico enmascarado es respaldar la investigación y el análisis estadísticos, y no comunicarse con el titular de los datos?

Análisis

66. Nuestra respuesta comienza abordando su subpregunta; "*Si el supuesto hecho de que el riesgo de identificación del titular de los datos por un tercero (es decir, parte no contratada) mediante el contacto de correo electrónico basado en la registración parece ser insignificante, ¿esto haría que dichos correos electrónicos sean eficazmente "anónimos" con respecto a terceros bajo la norma Breyer?*", para explicar el motivo por el cual consideramos que el GDPR seguiría siendo aplicable en el caso de un contacto de correo electrónico basado en la registración. Luego, abordamos los aspectos más amplios del cumplimiento del GDPR de su pregunta.

Anonimato

67. Mantenemos nuestro punto de vista, expresado en nuestro memorando con fecha 4 de febrero de 2020, que, con cualquiera de las opciones (contacto de correo electrónico basado en el registratario

o en la registración), sigue existiendo una alta probabilidad de que la publicación o divulgación automatizada de dichas direcciones de correo electrónico sean consideradas como el tratamiento de datos personales.

68. Para que el GDPR se aplique al tratamiento de datos electrónicos (suponiendo que se cumple la prueba de territorialidad del GDPR y que sus exclusiones de asuntos no son aplicables), se aplica una prueba que consta de dos partes:

68.1 En primer lugar, debe haber tratamiento de información que se relacione a una persona individual *en particular*, teniendo en cuenta el contenido, propósito o efecto de los datos (y su tratamiento). Esta es la prueba "*Nowak*"[96] / "se relaciona a".

68.2 En segundo lugar, esa persona individual en particular debe ser "identificada o identificable", lo que significa que deben existir "medios que puedan ser usados razonablemente, como la individualización, ya sea por el responsable del tratamiento de datos o por otra persona para identificar a la persona física, ya sea de manera directa o indirecta".[97] "Identificación" no significa necesariamente encontrar el nombre real de una persona; en cambio, tiene un significado más amplio, que, por lo general, gira en torno a la capacidad de "individualizar" específicamente a alguien para un tratamiento diferente (individualización), [98] o tener la capacidad de recopilar/conectar más datos sobre ella (inferencia o vinculación).[99] Un identificador técnico, incluso uno que fue generado de forma aleatoria, puede ser suficiente para dichos propósitos, en particular, si está vinculado a otra información sobre la persona que facilita distinguirla de otra persona. [100] No existen "medios razonablemente probables" de reidentificación si dicha actividad está "prohibida por ley o es prácticamente imposible a causa del hecho de que requiere un esfuerzo desproporcionado en cuanto a tiempo, costo y mano de obra, de manera que el riesgo de identificación parece, en realidad, ser insignificante"[101]. Esta es la prueba "*Breyer*" / de "identificabilidad".

69. Nuestro punto de vista, expresado anteriormente, es que el tratamiento de esos alias de correo electrónico aún podría ser considerado como que cumple ambas pruebas, en la medida que el propósito del tratamiento sea brindar un medio para contactarse con los titulares de los datos.

Prueba *Nowak*

70. Respecto de la prueba *Nowak*: cuando un contacto es una persona física, dichas direcciones serán alias enmascarados para una dirección de correo electrónico real que usa esa persona. En vista de esto:

70.1 En los casos en los que el propósito/efecto previsto del tratamiento de dichos datos es permitir correspondencia con el destinatario (es decir, a menudo, con un titular de datos específico), entonces,

---

[96] Dictamen del CJEU en el caso C-434/16 *Nowak,* ECLI:EU:C:2017:994, en el párrafo 35.
[97] Cláusula 26 del GDPR
[98] Como se citó anteriormente, la cláusula 26 del GDPR se refiere específicamente a "individualización" al analizar los medios que son razonablemente probables de usar a fin de identificar al titular de los datos.
[99] Individualización, posibilidad de vinculación e inferencia son tres partes de la prueba de anonimización propuesta por el Grupo de Trabajo sobre el Artículo 29, en su opinión 05/2014 sobre técnicas de anonimización ("WP 216"), disponible en línea en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[100] Sobre este punto, consulte la cláusula 30 del GDPR ("Las personas físicas pueden estar asociadas con identificadores en línea proporcionados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de protocolo de Internet, identificador de cookies u otros identificadores tales como marcas de identificación de radiofrecuencia. Esto puede dejar rastros que, en particular, cuando se combinan con identificadores únicos y otra información que los servidores reciben, pueden utilizarse para crear perfiles de personas físicas e identificarlas").
[101] Dictamen del CJEU en el caso C-582/14 *Breyer,* ECLI:EU:C:2016:779, en los párrafos 45 y 46.

considerando la prueba del Tribunal de Justicia de la UE ("CJEU") en *Nowak*, ese "propósito" o "efecto" significa que existe un vínculo con una persona individual *en particular*.[102]

70.2 Por el contrario, el tratamiento puramente estadístico dirigido a crear mediciones *agregadas* (que describen cohortes relativamente grandes) – por ejemplo, contar la cantidad de dichos alias de contacto que se han creado – puede posiblemente *no* estar sujeto al GDPR. Esto se debe a que el *contenido* de un alias de contacto generado de manera aleatoria no se vincula específicamente a una persona individual en particular, al menos en el caso de un contacto de correo electrónico basado en la registración; y – de nuevo, posiblemente – ni el *propósito* ni el *efecto* de crear resultados agregados de investigación estadística tiene un vínculo a una persona *en particular*; en cambio, las estadísticas agregadas describen y diferencian entre *cohortes/grupos* (por ejemplo, por nación, registro, registrador, etc.). La prueba *Nowak* puede posiblemente no ser cumplida con respecto a esa clase de tratamiento (pero tenga en cuenta que esta se debe distinguir de las estadísticas dirigidas a generar información nueva sobre un titular de datos específico, o una clasificación de este – por ejemplo, contar la cantidad de nombres de dominio asociados con un contacto de correo electrónico basado en el registratario).

70.3 Sin embargo, en la práctica, no creemos que sea razonablemente posible decir que el único propósito de crear y publicar los alias de contacto es para el tratamiento estadístico agregado recién descripto. Si así fuese, no habría necesidad de proporcionar una dirección de correo electrónico. El hecho de que se proporcione una dirección de correo electrónico sugiere que un propósito significativo para la creación y publicación de alias de contacto siempre será brindar un medio de contactar personas específicas. Por consiguiente, si bien *algún* tratamiento (para estadísticas agregadas) puede no estar dentro del alcance del GDPR en la prueba *Nowak*, el GDPR parece seguir siendo una preocupación sobre cumplimento al menos con respecto al *otro* propósito de tratamiento.

70.4 También deberíamos advertir sobre la dependencia excesiva en los argumentos basados en *Nowak*. A pesar de la decisión que se hace eco de las pautas anteriores del Grupo de Trabajo sobre el Artículo 29,[103] no tenemos conocimiento de que la prueba *Nowak* se haya estado aplicando en forma sistemática en los análisis y asesoramientos de tribunales y autoridades supervisoras que aplican el GDPR. Por ejemplo, a principios de abril de 2021, una búsqueda del sitio web de la Autoridad de Protección de Datos de Bélgica, en todos los idiomas disponibles, arroja (i) solo dos referencias directas al caso *Nowak* y solo en puntos no relacionados; y (ii) al parecer, ninguna mención de la frase clave "contenido, propósito o efecto" de *Nowak*. La explicación de esa autoridad (en su glosario) del término "datos personales" se concentra en forma exclusiva en la prueba Breyer – es decir, identificabilidad de un titular de los datos.[104] Otras autoridades pueden tener un punto de vista diferente (por ejemplo, la autoridad del Reino Unido sí analiza la prueba de "contenido, propósito o efecto", y resume su impacto de la siguiente manera: "La información debe 'relacionar a' la persona individual identificable con los datos personales. Esto implica que no los identifica solamente – deben estar relacionados de algún modo con la persona individual. (…) Los datos pueden hacer referencia a una persona identificable y no ser datos personales sobre dicha persona, ya que la información no se relaciona con ella").[105]

[102] En algunas ocasiones, una dirección de contacto de destinatario puede ser un buzón de correo compartido (por ejemplo, enquiries@example.com), en cuyo caso la dirección de contacto enmascarada posiblemente no sean datos personales, ya sea por la aplicación de las pruebas *Nowak* o *Breyer*.
[103] WP 136, en la pág. 10.
[104] https://www.autoriteprotectiondonnees.be/citoyen/vie-privee/lexique
[105] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-the-meaning-of-relates-to/#pd5

70.5 Además, las autoridades en este campo no siempre ponen especial énfasis en *Nowak*, pero *si* lo hicieran, también podrían tener enfoques diferentes respecto de su interpretación. Las diferencias de opinión podrían particularmente girar en la periferia del "contenido" de la prueba de "contenido, propósito o efecto". El Grupo de Trabajo sobre el Artículo 29, *Opinión 4/2007 sobre el concepto de datos personales* (WP 136)[106] explicó que "[e]l elemento "contenido" está presente en los casos en que – en correspondencia con el entendimiento más evidente y común en una sociedad de la palabra "relacionar" – la información se brinda sobre una persona particular, independientemente de cualquier propósito de parte del responsable del tratamiento de datos o de un tercero, o el impacto de dicha información en el titular de los datos". Si esa explicación es correcta, entonces un tribunal o regulador podría concluir que la publicación de una dirección de correo electrónico (incluso una generada de manera aleatoria) para un contacto que se asocie con una registración de dominio es la publicación *inherente* de la información "sobre" esa persona – porque nos dice cómo contactarse con dicha persona. No obstante, este es un punto de vista problemático ya que "toma prestado" el razonamiento de las pruebas de *propósito* y *efecto* (observa un posible propósito para la información, *no* el contenido de la información en sí), *y* se basa en un propósito/efecto hipotético, no el propósito/efecto real del tratamiento – lo que pone en corto circuito a dos tercios de la prueba de "contenido, propósito o efecto". Tanto desde la perspectiva lógica como de principio (claridad/certidumbre), esto es problemático. Desde un punto de vista más simple, algo generado en forma aleatoria (as876bnk@example.com) es una pura expresión del ruido "aleatorio" -- una toma instantánea del estado eléctrico de un circuito "generador de números aleatorios" de una computadora. No "*contiene*", ni puede contener, información sobre una persona. Si brindase información sobre una persona, es lógico que no sería algo aleatorio. Desde ese punto de vista, una dirección generada en forma aleatoria no aprueba la prueba de "contenido"; en cambio, se debería centrar en el propósito o efecto del tratamiento de los datos.

70.6 Resulta claro, entonces, que existe un gran riesgo de desacuerdo con al menos algunas autoridades si los argumentos se basan en el caso *Nowak*.

Prueba *Breyer*

71. En cuanto a la prueba Breyer: en ese caso, el CJEU elaboró un experimento de pensamiento; si se produciría un ciberataque, un responsable del tratamiento de datos que tiene una dirección IP (y, suponemos – aunque el tribunal no es explícito en este punto – una marca de tiempo que indica cuándo un dispositivo/persona de interés usó dicha dirección IP), podría comunicar esa información a las autoridades judiciales/policiales. El CJEU esperaba que las autoridades estuvieran facultadas para luego exigir la información correspondiente del proveedor de acceso a Internet que asignó la dirección IP y, así, iniciar un proceso judicial (si bien el CJEU solicitó a los tribunales nacionales referentes verificar dicho supuesto). El CJEU entonces sostuvo que, a menos que este escenario estuviese prohibido por ley o fuese prácticamente imposible, existían "medios razonablemente probables" de identificar a un titular de los datos.

72. El punto clave aquí es que, si bien un tercero puede conocer a un contacto de correo electrónico basado en el registratario o en la registración, las autoridades competentes podrían asociar esto a datos de registración sin carácter público mantenidos por las partes contratadas, permitiendo así la reidentificación. Hasta donde sabemos, esto no siempre requeriría niveles "prácticamente imposibles" de esfuerzo, ni sería universalmente prohibido por ley.

[106] Grupo de Trabajo sobre el Artículo 29, opinión *4/2007 sobre el concepto de datos personales* (WP 136), en la pág. 10. Disponible en línea en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

73. Entonces, incluso desde la perspectiva de *terceros*, la distribución y el uso de dichos alias de contacto podrían ser considerados como tratamiento de datos personales.

74. Desde la perspectiva de una parte contratada que conoce qué alias de contacto se asignó a un registratario / contacto nominado por el registratario, la creación y el alojamiento de dichas direcciones y su disponibilidad para uso por parte de otros, constituiría casi seguramente un tratamiento de datos personales (cuando las personas de contacto son personas físicas).

Riesgo de las opciones respectivas presentadas

75. Después de haber explicado nuestro punto de vista de que, para cualquiera de las opciones, el GDPR sigue siendo relevante, ahora nos dirigimos a su solicitud de que comparemos los riesgos asociados con la (a) publicación en la Web o (b) divulgación automática de (i) un contacto de correo electrónico basado en el registratario, por un lado, y (ii) un contacto de correo electrónico basado en la registración, por el otro.

76. Nuestro resumen (que refleja los supuestos importantes y las advertencias presentadas con posterioridad en esta respuesta) es el siguiente:

	Contacto de correo electrónico basado en el registratario	**Contacto de correo electrónico basado en la registración**
Publicación en la Web	Media	Baja
Divulgación automática	Baja	Más baja

77. En función de una aplicación de los principios del GDPR, el hecho de compartir (ya sea a través de una publicación en la Web o una divulgación automática) alias de correo electrónico basados en la registración conlleva menos riesgo que los alias de correo electrónico basados en el registratario.

78. Esto se debe a que alguien que tiene una dirección de correo electrónico basado en el registratario puede conocer más información sobre el titular de los datos, en particular, qué otros nombres de dominio están asociados a ese titular de los datos. El motivo de esto es que, a menos que se proporcionase una dirección de contacto *real* diferente para el titular de los datos para cada dominio que registre, cada registración tendría el mismo alias de correo electrónico.

79. La publicación en la Web de dichos detalles podría facilitar crear dichos perfiles y posiblemente incluso crear una herramienta de búsqueda inversa ('para un contacto de correo electrónico basado en la registración en particular, ¿qué nombres de dominio se asocian con este contacto?').

80. La divulgación automática, por sí sola, supuestamente dificultaría esto un poco más, ya que, a menos que las herramientas de divulgación automática *específicamente* proporcionen una función de búsqueda inversa,[107] es de suponer que los solicitantes necesitarían consultar cantidades más grandes

[107] Dichas funciones, antes de ser implementadas, deberían ser consideradas en forma exhaustiva. Para conocer asesoramientos anteriores sobre esta cuestión, consulte la opinión 5/2000 del Grupo de Trabajo sobre el Artículo 29 sobre el uso de directorios públicos para servicios de búsqueda inversa o con múltiples criterios (Directorios inversos) ("WP 33"), disponible en línea en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp33_en.pdf

de nombres de dominio para recopilar suficiente información para poder obtener coincidencias y empezar a crear una función de búsqueda inversa (incompleta). Dicho esto, los solicitantes que tienen una lista preestablecida de nombres de dominio específicos (por ejemplo, "espejos" sospechosos de un sitio web que aloja contenido ilegal) podrían determinar si se proporcionó la misma dirección de correo electrónico para algunos de dichos sitos o para todos ellos. Por ende, incluso en el caso de una divulgación automática, el uso del esquema de contacto de correo electrónico basado en el registratario conlleva riesgos adicionales a la privacidad, en relación con el esquema de contacto de correo electrónico basado en la registración.

81. En consecuencia, teniendo en cuenta las siguientes consideraciones:

81.1 La necesidad de cumplir con la regla de minimización de datos;

81.2 La necesidad de cumplir con una regla de "protección de datos desde el diseño y por defecto";

81.3 Esa dependencia en el artículo 6(1)(f) del GDPR (el fundamento legal de intereses legítimos) es más sólida cuando el diseño del sistema minimiza el prejuicio a "los intereses o derechos fundamentales y libertades del titular de los datos que exigen la protección de los datos personales"; y

81.4 Que, al evaluar si se deberían imponer multas (y de ser así, en qué medida) en contra de un responsable del tratamiento de datos, las autoridades deben considerar *inter alia* la "gravedad" de una infracción, el "alcance" del tratamiento de datos, el "nivel de daños sufrido por" los titulares de los datos, "cualquier acción realizada por el encargado o responsable del tratamiento de datos para mitigar el daño sufrido por los titulares de los datos" y "el grado de responsabilidad del encargado o responsable del tratamiento de datos en consideración de las medidas técnicas y organizacionales implementadas por él en virtud de los artículos 25 y 32" (consulte el artículo 83 del GDPR),

por lo tanto, consideramos que un esquema de contacto de correo electrónico basado en la registración conlleva un riesgo menor que un esquema de contacto de correo electrónico basado en el registratario.

82. Después de haber explicado el equilibrio que conlleva el eje del "esquema basado en la registración en comparación con aquel basado en el registratario", ahora trataremos los diferentes riesgos de la publicación basada en la Web en comparación con la divulgación automática.

83. Un riesgo común tanto en el esquema de correo electrónico basado en la registración como en aquel basado en el registratario es el spam u otros correos electrónicos no deseados; esta "capacidad de direccionamiento" es, posiblemente, un aspecto de la privacidad.[108] El spam es una preocupación de larga data para los sistemas de WHOIS; fue el tema de un estudio del Comité Asesor de Seguridad y Estabilidad de la ICANN en el año 2007, que concluyó que "la aparición de direcciones de correo electrónico en respuesta a consultas en el WHOIS contribuye realmente a la recepción de spam, aunque es solo un factor entre tantos.[109]

[108] La cláusula 40 de la Directiva 2002/58/EC ("Directiva de privacidad electrónica" de la UE) manifiesta lo siguiente: "Se deberían proporcionar medidas de protección para los suscriptores contra la intrusión a su privacidad por comunicaciones no deseadas con fines directos de marketing, en particular, por medio de máquinas de llamadas automatizadas, faxes y correos electrónicos, incluidos los mensajes SMS".

[109] *SAC 023: ¿Es el servicio de WHOIS una fuente de direcciones de correo electrónico para los remitentes de correo electrónico no deseado?* , Resumen Ejecutivo. Disponible en línea en https://www.icann.org/en/system/files/files/sac-023-en.pdf

84. En consecuencia, si se emplea un sistema de contacto de correo electrónico basado en el registratario o en la registración, se deberían tomar medidas eficaces para abordar la disponibilidad de las direcciones a los spammers (por ejemplo, el uso de funciones técnicas para impedir la "recolección" de dichas direcciones; o el filtrado de comunicaciones inadecuadas antes de ser entregadas al destinatario deseado).

85. En comparación con la publicación basada en la Web, suponemos que la divulgación automática permite un mayor alcance para evaluar los motivos de una solicitud, las fuentes de dicha solicitud, y para supervisar/auditar y aplicar medidas de protección (por ejemplo, límites de índices) sobre dichas solicitudes – es decir mayor alcance para implementar las clases de mitigaciones que reducirán la responsabilidad en función de los factores establecidos en el párrafo 81 más atrás arriba. Por ende, parecería que la divulgación automática presenta un riesgo inherentemente menor sobre este frente, en comparación con la publicación basada en la Web.

86. Esas posibles ventajas de la divulgación automática en comparación con la publicación basada en la Web también, en principio, están presentes en las ventajas del Artículo 25 del GDPR (protección de datos desde el diseño y por defecto). En particular, se debería pensar un poco a fin de garantizar que la publicación basada en la Web esté diseñada de manera tal de cumplir con el artículo 25(2) del GDPR, "dichas medidas garantizarán, por defecto, que los datos personales no estén accesibles sin la intervención de la persona a una cantidad indefinida de personas físicas".[110]

87. Dicho esto, si se emplean medidas eficaces contra el spam, y si se toma un enfoque basado en la registración (debido a sus ventajas expuestas anteriormente), debido a la baja utilidad resultante de los datos, resulta difícil ver cómo la publicación basada en la Web presentaría riesgos considerables a la privacidad o seguridad de los datos.

* * *

[110] En *sus pautas 4/2019 en el artículo 25, Protección de datos desde el diseño y por defecto, v2.0*, en el párrafo 56, el EDPB explica que esto significa que"[e]l responsable del tratamiento de datos, por defecto, deberá limitar la accesibilidad y otorgar al titular de los datos la posibilidad de intervenir antes de publicar o hacer que de algún otro modo estén disponibles los datos personales sobre el titular de los datos a una cantidad indefinida de personas físicas". Disponible en línea en https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf