Ranking Digital Rights
Índice de Responsabilidad Corporativa

Indicadores de la investigación 2015

Incluye definiciones y parámetros

Junio de 2015

Producido por

RANKING DIGITAL RIGHTS

www.rankingdigitalrights.org

SUSTAINALYTICS

www.sustainalytics.com

Reconocimientos

El trabajo de *Ranking Digital Rights* y *Sustainalytics* para elaborar los indicadores y la metodología de investigación descrita en este documento tuvo el apoyo de las siguientes organizaciones:

Fundación John S. y James L. Knight
Fundación John D. y Katherine T. MacArthur
Hivos People Unlimited
Fundación Ford
Fundaciones Open Society
Fundación William y Flora Hewlett
Universidad de Pensilvania
Annenberg COMPASS Fellowships

Para una lista completa de patrocinadores y socios, por favor ver https://rankingdigitalrights.org/who

Acerca de *Ranking Digital Rights*

Ranking Digital Rights es un proyecto presentado por Instituto Open Technology de *New America* dedicado a evaluar a las empresas de TIC más poderosas del mundo en políticas y prácticas que afectan la libre expresión y la privacidad de los usuarios. Para saber más del proyecto, por favor visitar rankingdigitalrights.org.

Para saber más acerca de *New America* por favor, visitar www.newamerica.org

Para saber más acerca del Instituto Open Technology, por favor visitar www.newamerica.org/oti

Acerca de *Sustainalytics*

Sustainalytics es una importante firma independiente de investigación y análisis ambiental, social y de gobernabilidad que apoya a inversionistas en todo el mundo en el desarrollo e implementación de estrategias responsables de inversión. Como socio de investigación del proyecto piloto de *Ranking Digital Rights*, *Sustainalytics* ayudó a diseñar la metodología de investigación para la iniciativa y clasificar a las importantes empresas globales de TIC sobre políticas y prácticas en libre expresión y privacidad con relación a parámetros de derechos humanos.

Con 13 oficinas a nivel mundial, *Sustainalytics* tiene un personal con más de 200 miembros, incluidos más de 100 analistas con amplia experiencia en industria y lenguaje. La empresa es el principal socio de investigación para el Índice de Acceso a la Medicina 2014, entre otras importantes calificaciones e índices. En los tres últimos años, *Sustainalytics* fue elegida como la mejor empresa independiente de investigación en la encuesta IRRI de Extel. Para más información sobre *Sustainalytics*, por favor visitar www.sustainalytics.com.

Índice

Acerca del Índice 2015 4

Las empresas 4

Proceso de investigación e información 5

C: Compromis 6
C1. Política y liderazgo 6
C2. Gobernabilidad y supervisión de gestión 6
C3. Implementación interna 7
C4. Evaluación de impacto..... 7
C5. Participación de los interesados 8
C6. Solución 8

F: Libertad de expresión 9
F1. Disponibilidad de los términos de servicio 9
F2. Términos de servicio, notificación y registro de cambios..... 9
F3. Razones para restringir contenido..... 9
F4. Razones para restringir una cuenta o servicio 10
F5. Notificación de restricciones a los usuarios: 10
F6. Proceso para responder a solicitudes de terceros 10
F7. Información sobre solicitudes gubernamentales 11
F8. Información sobre solicitudes privadas 11
F9. Información sobre aplicación de los términos de servicio 12
F10. Gestión de la red (empresas de telecomunicaciones)..... 12
F11. Política de identidad (empresas de internet) 13

P: Privacidad 14
P1. Disponibilidad de las políticas de privacidad..... 14
P2. Políticas de privacidad, notificación y registro de cambios 14
P3. Recopilación de información del usuario..... 14
P4. Intercambio de información del usuario..... 15
P5. Control del usuario de la recopilación e intercambio de información..... 15
P6. Acceso de los usuarios a su propia información 16
P7. Retención de información del usuario..... 16
P8. Recopilación de información del usuario por terceros (empresas de internet)..... 16
P9. Proceso para responder a solicitudes de terceros de información del usuario..... 17
P10. Notificación al usuario sobre solicitudes de terceros de información del usuario 17
P11. Datos de solicitudes de terceros sobre información del usuario..... 17
P12. Parámetros de seguridad..... 18
P13. Encriptación de contenido privado del usuario (empresas de internet) 19
P14. Información e instrucción a los usuarios sobre posibles amenazas 19

Apéndice 1 – Definiciones y referencias claves 20

Apéndice 2 – Guía de investigación 29

Acerca del Índice 2015

En noviembre de 2015, el proyecto *Ranking Digital Rights* lanzará su primer Índice de Responsabilidad Corporativa. Dieciséis empresas de internet y de telecomunicaciones serán evaluadas de acuerdo con 31 indicadores centrados en revelación corporativa de políticas y prácticas que afectan la libertad de expresión y la privacidad de los usuarios.

La información recogida por el Índice conformará el trabajo de defensores de derechos humanos, legisladores e inversionistas responsables. También ayudará a las empresas a mejorar sus propias políticas y prácticas.

Las empresas

En su primer año, el Índice evaluará a 16 empresas, divididas en partes iguales entre empresas de internet y de telecomunicaciones. Los investigadores examinarán políticas y prácticas integrales de empresas matrices, además de las políticas y prácticas reveladas políticas y prácticas de servicios seleccionados y/o empresas que funcionan localmente (dependiendo de la estructura de la empresa). Las empresas de 2015 son:

Empresas de telecomunicaciones:

(Nivel de empresa matriz, además de servicios de banda ancha fija y móviles en la jurisdicción local de cada empresa)

- **América Móvil**
- **AT&T**
- **Axiata**
- **Bharti Airtel**
- **Etisalat**
- **MTN**
- **Orange**
- **Vodafone**

Empresas de internet:

(Políticas a nivel de la empresa además de dos a tres servicios seleccionados como se especifica a continuación)

- **Daum Kakao** – Daum Search, Kakao Talk, Daum Mail
- **Facebook** – Facebook, WhatsApp, Instagram
- **Google** – Search, Gmail, YouTube
- **Mail.ru** – VKontakte, Mail, Mail.ru Agent
- **Microsoft** – Bing, Outlook.com, Skype
- **Tencent** – WeChat, Qzone, QQ
- **Twitter** – Twitter, Vine
- **Yahoo** – Mail, Flickr, Tumblr

Proceso de investigación e información

El proceso de investigación y evaluación para el Índice de Responsabilidad Corporativa 2015, llevado a cabo de manera conjunta por *Ranking Digital Rights*, *Sustainalytics* y un equipo de investigadores internacionales, incluye las siguientes etapas:

1. Investigación primaria – los investigadores evalúan a cada empresa por cada indicador (ver Apéndice 2 para más información sobre los parámetros de investigación);

2. Revisión a cargo de pares – un segundo grupo de investigadores revisa el trabajo de los investigadores primarios, plantean preguntas y sugieren cambios;

3. Conciliación – los investigadores principales de RDR y *Sustainalytics* resuelven las diferencias entre los resultados de la investigación primaria y la revisión a cargo de pares;

4. Revisión de la empresa – los resultados iniciales desde la etapa 3 se envían a las empresas para que formulen comentarios y observaciones;

5. Revisión y puntaje inicial – RDR y *Sustainalytics* procesan los comentarios de la empresa y toman decisiones sobre los resultados;

6. Análisis horizontal– *Sustainalytics* examina los resultados de las empresas a través de indicadores para garantizar consistencia y control de calidad;

7. Resultados finales – se toman las decisiones finales acerca de los resultados de las empresas.

Los resultados serán luego ponderados y convertidos a puntajes numéricos para cada empresa.

El Índice se dará a conocer en noviembre de 2015 en un sitio web interactivo y en versiones de un informe en versiones PDF descargables. La metodología de puntuación se dará a conocer conjuntamente con los resultados del Índice. Los puntajes estarán acompañados con un análisis narrativo integral sobre hallazgos y tendencias claves. Además, los perfiles de la empresa analizarán el desempeño de cada empresa e incluirán información destacada que ayude a brindar contexto y matices a los resultados. Esa información deberá incluir ejemplos específicos de práctica empresarial, u otras observaciones formuladas por los investigadores en asuntos que caen fuera del parámetro de investigación de los indicadores.

Nota sobre contextos nacionales que afectan el desempeño de las empresas: en la mayoría de países, algunas leyes, regulaciones o factores políticos realzarán o limitarán la capacidad de una empresa de desempeñarse bien en algunos indicadores. Nuestra metodología no compensa estos factores: en otras palabras, el Índice evalúa empresas en lo que hacen o no hacen, independientemente de la razón. Sin embargo, los perfiles narrativos de cada empresa incluirán un análisis de cómo la jurisdicción de origen de la empresa, el entorno legal, regulatorio y político afectó su puntaje.

Para más información de cómo se llevaron a cabo los indicadores y la metodología de investigación, además de los documentos que describen cómo se usaron los parámetros y definiciones de la investigación para guiar la investigación, por favor revise el sitio web del proyecto en https://rankingdigitalrights.org.

Los términos definidos en el Apéndice 1 aparecen en negrita en el texto del indicador que está debajo.

C: Compromiso

La empresa demuestra un claro compromiso en palabras y acciones de respeto a los derechos humanos de libertad de expresión y privacidad. Ambos derechos están consagrados en la Declaración Universal de Derechos Humanos y el Convenio Internacional sobre Derechos Civiles y Políticos, que se aplican en línea y fuera de línea por igual. Para que una empresa se desempeñe bien en este rubro, el compromiso de la empresa al menos debe seguir, y superar en el mejor de los casos, los Principios Rectores de Naciones Unidas para Negocios y Derechos Humanos y otros parámetros de derechos humanos específicos para el sector centrados en libertad de expresión y privacidad, tales como Global Network Initiative.

C1. Política y liderazgo

A. ¿La empresa hace un **compromiso explícito, destacado** y claramente articulado con los derechos humanos, incluidas libertad de expresión y privacidad?

Categorías de respuesta (elegir una):

1. Sí
2. No

B. ¿Los **altos ejecutivos** de la empresa **se comprometen significativamente** a fomentar la libertad de expresión y privacidad de los usuarios?

Categorías de respuesta (elegir una):

1. Comentario **a nivel ejecutivo**: un alto ejecutivo ha hecho declaraciones en un l**ugar destacado**.
2. Comentario **a nivel gerencial**: los gerentes o portavoces de la empresa han hecho declaraciones en un lugar destacado.
3. Ninguna/Sin evidencia: los representantes de la empresa no han hecho comentarios relacionados en un lugar destacado.

C2. Gobernabilidad y supervisión de gestión

¿Hay **supervisión** a nivel directivo, ejecutivo y gerencial sobre cómo las políticas y prácticas de la empresa afectan la libertad de expresión y la privacidad?

Lista de verificación (marque todas las que correspondan):

1. Supervisión **a nivel de la directiva**: un **comité** directivo tiene supervisión formal sobre cómo las prácticas de la empresa afectan la libertad de expresión y privacidad.
2. Responsabilidad **a nivel ejecutivo**: un comité, **equipo**, **programa** o **funcionario** a nivel ejecutivo supervisa cómo las prácticas de la empresa afectan la libertad de expresión y la privacidad.

3. Responsabilidad **a nivel gerencial**: un comité, equipo, programa o funcionario a nivel gerencial supervisa cómo las prácticas de la empresa afectan la libertad de expresión y la privacidad.

C3. Implementación interna

¿La empresa tiene mecanismos vigentes para implementar su compromiso con la libertad de expresión y privacidad?

Lista de verificación (marque todas las que correspondan):

1. La empresa brinda capacitación a los trabajadores sobre libertad de expresión y asuntos de privacidad.

2. La empresa mantiene un programa de **trabajador informante**.

C4. Evaluación de impacto

¿La empresa gestiona **evaluaciones de impacto en derechos humanos** con la diligencia debida, frecuente, extensa y creíblemente para identificar cómo todos los aspectos de su actividad impactan en la libertad de expresión y privacidad?

Lista de verificación (marque todas las que correspondan):

1. La empresa evalúa las leyes que afectan la privacidad y la libertad de expresión en jurisdicciones donde opera y usa este análisis para informar de las políticas y prácticas de la empresa.

2. La empresa evalúa con frecuencia la libre expresión y riesgos de privacidad asociados con productos y servicios existentes.

3. La empresa evalúa la libre expresión y riesgos de privacidad asociados con una actividad nueva, incluido el lanzamiento y/o adquisición de nuevos productos o servicios o entrada en nuevos mercados.

4. La empresa evalúa la libre expresión y riesgos de privacidad asociados con los procesos y mecanismos usados para aplicar sus términos de servicio.

5. La empresa se desenvuelve con la debida diligencia detallada donde las evaluaciones de riesgo de la empresa identifican problemas.

6. **Altos ejecutivos** y/o miembros de la junta directiva de la empresa revisan y toman en cuenta los resultados de las evaluaciones y la diligencia debida en toma de decisiones estratégica de la empresa.

7. La empresa lleva a cabo evaluaciones de manera frecuente.

8. La evaluación de la empresa cuenta con la garantía de un tercero externo.

9. El tercero externo que garantiza la evaluación está acreditado con un parámetro de derechos humanos relevante y respetable por parte de una organización confiable.

C5. Participación de los interesados

¿La empresa **interactúa** con varios **interesados** en libertad de expresión y asuntos de privacidad?

A. La empresa integra una **iniciativa de varios interesados** que incluye un compromiso de mantener la libertad de expresión y privacidad basado en principios internacionales de derechos humanos.

B. De no ser así, ¿la empresa cumple con alguno de los siguientes elementos?

   1. La empresa es miembro de una organización del sector que interactúa con interesados ajenos al sector y no gubernamentales en libertad de expresión y privacidad.

   2. La empresa inicia o participa en reuniones con interesados que representan, defienden o son personas afectadas directa y negativamente por los negocios de la empresa.

C6. Solución

¿Tiene la empresa mecanismos de **reclamo** y **solución**?

Lista de verificación (marque todas las que correspondan):

1. La empresa revela sus procesos de recepción de quejas o reclamos.

2. La empresa enumera las quejas que está preparada para responder.

3. La empresa detalla su proceso para responder a las quejas.

4. La empresa informa la cantidad de quejas que recibe.

5. La empresa brinda evidencia de que está respondiendo a las quejas, incluidos ejemplos de resultados.

F: Libertad de expresión

En las políticas y prácticas dadas a conocer, la empresa demuestra maneras concretas con las que respeta el derecho a la libertad de expresión de los usuarios, como lo establece la Declaración Universal de Derechos Humanos, el Convenio Internacional sobre Derechos Civiles y Políticos y otros instrumentos internacionales de derechos humanos. Las políticas y prácticas que la empresa ha dado a conocer muestran qué hace para evitar contribuir con acciones que pueden interferir con este derecho, salvo cuando esas acciones sean legítimas, proporcionadas y con un propósito justificado. Las empresas que se desempeñan bien en este indicador demuestran un fuerte compromiso público con la transparencia, no solamente en términos de cómo responden a las solicitudes gubernamentales, sino también cómo determinan, comunican y aplican reglas privadas y prácticas comerciales que afectan la libertad de expresión de los usuarios.

F1. Disponibilidad de los términos de servicio

¿Están **disponibles** los **términos de servicio** y son **fáciles de entender**?

Lista de verificación (marque todas las que correspondan):

1. Libres: los términos de servicio de la empresa son **fáciles de encontrar** y están **disponibles de manera libre** sin necesidad de registro o subscripción.

2. Idioma: los términos de servicio están disponibles en el idioma más usado por los usuarios de la empresa.

3. Fáciles de entender: los términos de servicio están presentados de **manera entendible**.

F2. Términos de servicio, notificación y registro de cambios

¿La empresa se compromete a proporcionar **notificación** y **documentación** significativa a los usuarios cuando cambia sus **términos de servicio**?

Lista de verificación (marque todas las que correspondan):

1. La empresa revela el método de notificación directa a los usuarios (por ejemplo, correo electrónico, mensajes de texto, etc.).

2. La empresa revela el periodo dentro del cual ofrece la notificación (por ejemplo, dos semanas antes de que se den los cambios).

3. La empresa mantiene un **archivo público** o **cambio de registrio**.

F3. Razones para restringir contenido

¿La empresa revela si prohíbe algún **contenido** o actividades?

Lista de verificación (marque todas las que correspondan):

1. La empresa explica qué contenido o actividades no permite.

2. La empresa explica el **proceso de aplicación de sus reglas**.

3. La empresa brinda ejemplos para ayudar al usuario a entender cuáles son las reglas y cómo se aplican.

F4. Razones para restringir una cuenta o servicio

¿La empresa explica las circunstancias bajo las cuales puede restringir o negar a los usuarios el acceso al servicio?

Lista de verificación (marque todas las que correspondan):

1. La empresa explica la razón o razones por las que **restringe la cuenta de un usuario**.
2. La empresa explica por qué podría **cerrar o restringir el servicio** a un área particular o un grupo de usuarios (donde sea aplicable).
3. La empresa brinda ejemplos específicos de situaciones que pueden desencadenar en restricción o negativa del servicio por parte de la empresa.

F5. Notificación de restricciones a los usuarios:

Si la empresa restringe **contenido** o acceso, ¿revela cómo lo **notifica** a los usuarios?

Lista de verificación (marque todas las que correspondan):

1. Si la empresa aloja contenido generado por el usuario, la empresa se compromete a notificar a los usuarios que generaron el contenido cuando lo restringe.
2. La empresa se compromete a notificar a los usuarios que tratan de acceder al contenido que ha sido restringido.
3. En su notificación, la empresa incluye una explicación del fundamento para la restricción del contenido (legal u otra).
4. La empresa se compromete a notificar a los usuarios cuando restringe acceso al servicio.

F6. Proceso para responder a solicitudes de terceros

¿La empresa publica información sobre su proceso de evaluación y respuesta de **solicitudes gubernamentales** y otros **terceros** para restringir **contenido** o servicio?

Lista de verificación (marque todas las que correspondan):

1. La empresa explica su proceso para recibir y responder a **solicitudes gubernamentales no judiciales**.
2. La empresa explica su proceso para responder a **órdenes judiciales**.
3. La empresa explica su proceso para responder a **solicitudes de privados**.
4. La empresa explica su proceso para responder a solicitudes de jurisdicciones extranjeras.
5. Las explicaciones de la empresa incluyen la base legal que debe cumplir.

6. La empresa se compromete a actuar con la debida diligencia con relación a las solicitudes antes de decidir cómo responder.

7. El proceso de la empresa se compromete a rechazar solicitudes que no se ajusten a la ley.

8. La empresa brinda orientación o ejemplos de implementación de políticas.

F7. Información sobre solicitudes gubernamentales

¿La empresa publica con frecuencia información sobre **solicitudes gubernamentales** (incluidas órdenes judiciales) para retirar, filtrar o restringir **contenido** o acceso a servicios, además de información sobre hasta qué punto la empresa cumple con esas solicitudes?

Lista de verificación (marque todas las que correspondan):

1. La empresa disgrega la cantidad de solicitudes que recibe por país.

2. La empresa enumera la cantidad de cuentas afectadas.

3. La empresa enumera la cantidad de contenido o las URL afectadas.

4. La empresa enumera los asuntos asociados con las solicitudes que recibe.

5. La empresa identifica la autoridad legal específica que hace la solicitud.

6. La empresa enumera la cantidad de solicitudes que ha acatado.

7. La empresa publica solicitudes originales o proporciona copias para el archivo de un tercero, tal como *Chilling Effects* u organización similar.

8. La empresa da cuenta de esta información al menos una vez al año.

9. La información de la que se da cuenta puede exportarse como un **archivo de datos estructurado**.

F8. Información sobre solicitudes privadas

¿La empresa publica con frecuencia información sobre **solicitudes de entes no gubernamentales** (y **no judiciales**) para retirar, filtrar o restringir acceso a contenido, e información de hasta qué punto la empresa cumple con esas solicitudes

Lista de verificación (marque todas las que correspondan):

1. La empresa disgrega la cantidad de solicitudes que recibe por país.

2. La empresa enumera la cantidad de cuentas afectadas.

3. La empresa enumera la cantidad de contenido o las URL afectadas.

4. La empresa enumera las razones de retiro asociadas con las solicitudes recibidas (por ejemplo, infracciones a derechos de autor, discurso de odio, incitación a la violencia, imágenes de abuso infantil, etc.).

5. La empresa describe a las partes de las que recibe solicitudes (por ejemplo, solicitudes hechas bajo un sistema de notificación y retiro, solicitudes de una organización no gubernamental, solicitudes de un ente autorregulador voluntario del sector, etc.).

6. La empresa enumera la cantidad de solicitudes que ha acatado.

7. La empresa publica la solicitud original o bien proporciona copias para el archivo de un tercero, como *Chilling Effects* o una organización similar.

8. La empresa da cuenta de esta información al menos una vez al año.

9. La información de la que se da cuenta puede exportarse como un **archivo de datos estructurado**.

F9. Información sobre aplicación de los términos de servicio

¿La empresa publica con frecuencia información sobre el volumen y naturaleza de acciones tomadas para aplicar sus propios **términos de servicio**?

Lista de verificación (marque todas las que correspondan):

1. La empresa enumera la cantidad de cuentas afectadas.

2. La empresa enumera la cantidad de contenido o las URL restringidas.

3. La empresa enumera el contenido restringido durante el periodo informado (por ejemplo, discurso de odio, acoso, incitación a la violencia, contenido sexualmente explícito, etc.).

4. La empresa brinda ejemplos de las razones por las que actuó en diferentes casos.

5. La empresa da cuenta de esta información al menos una vez al año.

6. La información de la que se da cuenta puede exportarse como un **archivo de datos estructurado**.

F10. Gestión de la red (empresas de telecomunicaciones)

¿La empresa revela si **prioriza** o degrada la **transmisión** o **envío** de **contenido** diferente (por ejemplo, **formación** o **regulación de tráfico**), y de ser así, con qué propósito?

Categorías de respuesta (elegir una):

1. La empresa revela que no prioriza ni degrada la distribución de contenido.

2. La empresa revela que prioriza o degrada la distribución de contenido y el propósito con que lo hace.

3. La empresa revela que prioriza o degrada la distribución de contenido pero no explica con qué propósito lo hace.

4. La empresa no revela información sobre si prioriza o degrada la distribución de contenido.

F11. Política de identidad (empresas de internet)

¿La empresa solicita a los usuarios que confirmen su identidad con identificaciones expedidas por el gobierno, o con otras formas de identificación relacionadas con su actividad fuera de línea?

Categorías de respuesta (elegir una):

1. No
2. Sí

P: Privacidad

En las políticas y prácticas dadas a conocer, la empresa muestra maneras concretas con las que respeta el derecho a la privacidad de los usuarios, como está establecido en la Declaración Universal de Derechos Humanos y el Convenio Internacional sobre Derechos Civiles y Políticos y otros instrumentos internacionales de derechos humanos. Las políticas y prácticas que la empresa revela muestran cómo trabaja para evitar contribuir con acciones que podrían interferir con la privacidad de los usuarios, salvo cuando esas acciones sean legales, proporcionadas y tengan un propósito justificado. También mostrarán un fuerte compromiso de proteger y defender la seguridad digital de los usuarios. Las empresas que se desempeñan bien en este indicador muestran un fuerte compromiso público con la transparencia en términos de cómo responden a solicitudes gubernamentales y también cómo determinan, comunican y aplican reglas privadas y prácticas comerciales que afectan la privacidad de los usuarios.

P1. Disponibilidad de las políticas de privacidad

¿Las **políticas de privacidad** de la empresa están **disponibles libremente** y son **fáciles de entender**?

Lista de verificación (marque todas las que correspondan):

1. Libre: Las políticas de privacidad de la empresa son **fáciles de encontrar** y están disponibles libremente sin necesidad de registro o subscripción.

2. Idioma: las políticas de privacidad están disponibles en el idioma más usado por los usuarios de la empresa.

3. Fáciles de entender: las políticas están presentadas de manera entendible.

P2. Políticas de privacidad, notificación y registro de cambios

¿La empresa se compromete a proporcionar **notificación** y **documentación** significativa a los usuarios cuando cambia sus **políticas de privacidad**?

Lista de verificación (marque todas las que correspondan):

1. La empresa revela el método de notificación directa a los usuarios (por ejemplo, correo electrónico, mensajes de texto etc.).

2. La empresa revela el periodo dentro del cual ofrece la notificación (por ejemplo, dos semanas antes de que se den los cambios).

3. La empresa mantiene un **archivo público** o **cambio de registro**.

P3. Recopilación de información del usuario

¿La empresa revela qué **información del usuario recopila**, cómo recopila esta información y por qué?

B. La empresa revela que no recopila información del usuario.

C. De no ser así, ¿la empresa cumple con alguno de los siguientes elementos?

1. **Minimización de información**: la empresa se compromete a limitar la recopilación de información del usuario a lo directamente pertinente y necesario para cumplir con el propósito de su servicio.

2. La empresa revela claramente qué información del usuario recopila.

3. La empresa revela claramente cómo recopila la información del usuario.

4. La empresa revela claramente por qué recopila información del usuario.

P4. Intercambio de información del usuario

¿La empresa revela si **intercambia** o **comparte información del usuario** con **terceros** y por qué?

A. La empresa revela que no intercambia ni comparte información del usuario.

B. De no ser así, ¿la empresa cumple con algunos de los siguientes elementos?

   1. La empresa revela claramente qué información del usuario intercambia o comparte.

   2. La empresa revela claramente por qué intercambia o comparte información del usuario.

   3. La empresa ofrece una descripción detallada de los terceros con los que intercambia o comparte información del usuario.

   4. La empresa revela los nombres de todos los terceros con los que intercambia o comparte información del usuario y explica qué información intercambia o comparte con cada uno de esos terceros.

   5. Si la empresa ofrece múltiples servicios, revela claramente si intercambia o comparte información del usuario entre los diferentes servicios y cómo los intercambiará o compartirá.

P5. Control del usuario de la recopilación e intercambio de información

¿La empresa brinda **opciones** a los usuarios **para controlar** la **recopilación** e **intercambio** de su información?

Lista de verificación (marque todas las que correspondan):

1. La empresa brinda opciones a los usuarios para controlar la recopilación de su información.

2. La empresa brinda opciones a los usuarios para controlar el intercambio que la empresa hace de su información.

P6. Acceso de los usuarios a su propia información

¿Los usuarios pueden ver, descargar u obtener de alguna manera, en **formatos de datos estructurados**, toda la información que la empresa tiene sobre ellos?

Lista de verificación (marque todas las que correspondan):

1. La empresa permite a los usuarios ver su información.
2. La empresa permite a los usuarios recibir una copia de su información.
3. La información se puede descargar en un archivo de datos estructurado.
4. Esta información incluye toda la información que ve el público y la información privada que una empresa tiene sobre un usuario.

P7. Retención de información del usuario

¿La empresa revela cuánto tiempo **retiene la información del usuario**?

A. La empresa revela que no retiene información del usuario.

B. De no ser así, ¿la empresa cumple alguno de los siguientes elementos?

1. La empresa revela que retiene información del usuario (que no ha sido remitida activamente por el usuario con el propósito de almacenamiento o publicación) de manera **anónima**.
2. La empresa revela la información del usuario que retiene.
3. La empresa revela cuánto tiempo retiene la información del usuario.
4. La empresa revela que elimina toda la información del usuario después de que el usuario pone fin a su cuenta.

P8. Recopilación de información del usuario por terceros (empresas de internet)

¿La empresa publica información clara sobre si **recopila información del usuario** de **terceros**?

A. La empresa revela que no recopila información del usuario de terceros.

B. De no ser así, ¿la empresa cumple con alguno de los siguientes elementos?

1. La empresa explica claramente cómo recopilaría de terceros la información del usuario (por ejemplo, el uso de una aplicación o servicio de publicidad).
2. La empresa declara claramente cómo usa la información que recopila.
3. La empresa declara claramente cuánto tiempo retiene la información que recopila.
4. La empresa respeta las **señales generadas por el usuario** (por ejemplo, encabezados de "**No Rastrear**") para no participar en la recopilación de información.

P9. Proceso para responder a solicitudes de terceros de información del usuario

¿La empresa publica información sobre su proceso de evaluación y respuesta a solicitudes gubernamentales y otros **terceros** de **información de usuario** guardada y/o **comunicaciones en tiempo real**, incluida la base legal para cumplir con esas solicitudes?

Lista de verificación (marque todas las que correspondan):

1. La empresa explica su proceso para recibir y responder a **solicitudes gubernamentales no judiciales**.
2. La empresa explica su proceso para responder a **órdenes judiciales**.
3. La empresa explica su proceso para responder **solicitudes hechas por terceros privados**.
4. La empresa explica su proceso para responder a solicitudes de jurisdicciones extranjeras.
5. Las explicaciones de la empresa incluyen la base legal según la cual pueden cumplir.
6. La empresa se compromete a manejar con la debida diligencia las solicitudes antes de decidir cómo responder.
7. El proceso de la empresa se compromete a rechazar solicitudes ilegales.
8. La empresa ofrece orientación o ejemplos de implementación de políticas.

P10. Notificación al usuario sobre solicitudes de terceros de información del usuario

¿La empresa se compromete a **notificar** a los usuarios hasta donde sea legalmente posible cuando **su información** ha sido solicitada por gobiernos y otros **terceros**?

Lista de verificación (marque todas las que correspondan):

1. La empresa se compromete a notificar a los usuarios cuando las **entidades gubernamentale**s (incluidos juzgados y otros entes judiciales) solicitan la **información de sus usuarios**.
2. La empresa se compromete a notificar a los usuarios cuando entidades no gubernamentales solicitan la información de sus usuarios.
3. La empresa revela situaciones en que podría no notificar a los usuarios, incluida una descripción de las **solicitudes gubernamentales** que por ley está prohibida de revelar a los usuarios.

P11. Datos de solicitudes de terceros sobre información del usuario

¿La empresa publica con frecuencia datos sobre solicitudes gubernamentales y de terceros para **información del usuario**, además de información sobre hasta qué punto la empresa cumple con esas solicitudes?

Lista de verificación (marque todas las que correspondan):

1. La empresa disgrega la **información del usuario** y los pedidos de acceso a comunicaciones en tiempo real que recibe por país.

2. La empresa enumera la cantidad de cuentas afectadas.

3. La empresa enumera si una solicitud buscaba comunicaciones con **contenido** o **sin contenido** (por ejemplo, metadata, información básica del abonado, o información transaccional sin contenido) o ambos.

4. La empresa identifica la autoridad legal específica o el proceso legal a través del cual se realizan las solicitudes de las autoridades y de seguridad nacional.

5. La empresa incluye solicitudes provenientes de **órdenes judiciales** o citatorios (incluidos procesos civiles).

6. La empresa incluye otras solicitudes no gubernamentales.

7. La empresa enumera la cantidad de solicitudes con las que cumplió, disgregadas por categoría de solicitud.

8. La empresa enumera qué **solicitudes gubernamentales** está impedida de revelar por disposición legal.

9. La empresa da cuenta de esta información al menos una vez al año.

10. La información de la que se da cuenta puede exportarse como un **archivo de datos estructurado**.

P12. Parámetros de seguridad

¿La empresa utiliza estándares del sector para **encriptación** y seguridad para sus productos y servicios?

Lista de verificación (marque todas las que correspondan):

1. La empresa se compromete a estar al día con los últimos estándares de encriptación y seguridad y publica evidencia de eso.

2. La empresa se compromete a abordar los puntos débiles de seguridad cuando se detecten y publica información general de cómo lo hace.

3. La empresa revela que tiene sistemas vigentes para limitar y dar seguimiento al acceso de los trabajadores a información del usuario.

4. La empresa revela que con frecuencia realiza auditorías de seguridad sobre sus tecnologías y prácticas que afectan la información del usuario.

5. La empresa revela que la transmisión de las comunicaciones del usuario está encriptada por defecto.

6. La empresa revela que utiliza métodos avanzados de autenticación para evitar acceso fraudulento.

P13. Encriptación de contenido privado del usuario (empresas de internet)

¿Pueden los usuarios **encriptar** su propio **contenido** y, por tanto, controlar quién tiene acceso a ese contenido?

Categorías de respuesta (elegir una):

1. El contenido privado del usuario está encriptado por defecto; la propia empresa no tiene acceso.
2. La empresa brinda una opción incorporada para encriptar contenido privado.
3. Los términos u otras políticas de la empresa explican que el usuario puede utilizar tecnologías de encriptado de terceros.
4. No hay revelación.
5. Los términos u otras políticas de la empresa prohíben el encriptado.

P14. Información e instrucción a los usuarios sobre posibles amenazas

¿La empresa publica información para ayudar a los usuarios a defenderse contra las **ciberamenazas**?

Lista de verificación (marque todas las que correspondan):

1. La empresa se compromete a notificar a los usuarios sobre actividad no habitual de la cuenta, la actividad más reciente de la cuenta y posible acceso no autorizado.
2. La empresa publica materiales prácticos que instruyen a los usuarios sobre cómo protegerse de ciberamenazas relacionadas con sus servicios.

Apéndice 1 – Definiciones y referencias claves

Nota: este no es un glosario general. Las definiciones y explicaciones que aparecen a continuación fueron escritas específicamente para guiar a los investigadores para evaluar empresas de internet y telecomunicaciones en los indicadores de investigación del proyecto.

Acceso a comunicaciones en tiempo real – La vigilancia de una conversación u otra comunicación electrónica en "tiempo real" mientras la conversación está ocurriendo, la interceptación de información en el preciso momento en que se está transmitiendo. A veces también se le llama "escucha telefónica". Consideremos la diferencia entre la solicitud de una escucha telefónica y una solicitud de información almacenada. Una escucha telefónica da a las autoridades potestad de acceder a futuras comunicaciones, mientras que una solicitud de información almacenada da a las autoridades acceso a los registros de comunicaciones que se dieron en el pasado. El gobierno de Estados Unidos puede tener acceso a comunicaciones en tiempo real con la Ley de Escuchas Telefónica y la Ley de Registro de Bolígrafo, ambas como parte de la Ley de Privacidad en las Comunicaciones Electrónicas (ECPA, por su nombre en inglés); el gobierno ruso puede hacerlo a través del "Sistema para Actividades Operativas de Investigación" (SORM).

Para mayor información sobre cómo las escuchas telefónicas y registros de bolígrafo afectaron las comunicaciones en línea de acuerdo con la Ley Patriota de Estados Unidos (en mayo de 2015), ver las siguientes secciones de la página web de ACLU "Vigilancia de acuerdo con la Ley Patriota de Estados Unidos":

- Expansión de la excepción de "registro de bolígrafo" en la ley de escuchas telefónicas
- Órdenes de registro de bolígrafo "a nivel nacional"
- Búsquedas de registro de bolígrafo aplicadas a internet

Fuente: https://www.aclu.org/surveillance-under-usa-patriot-act?redirect=national-security/surveillance-under-usa-patriot-act

Altos ejecutivos – Presidentes ejecutivos y otros miembros del equipo directivo tal como aparecen enumerados por la empresa en su sitio web u otros documentos oficiales, como un informe anual. A falta de una lista definida por la empresa, otros cargos con categoría de jefe y quienes estén al más alto nivel de gerencia (por ejemplo, vicepresidente ejecutivo/vicepresidente principal, dependiendo de la empresa).

Archivo público – Una fuente públicamente disponible que contiene las versiones anteriores de los términos de servicio o que explica exhaustivamente cada ronda de cambios que la empresa hace a sus términos de servicio.

Aviso / Notificación — La empresa se comunica con los usuarios o informa a los usuarios sobre algo relacionado con la empresa o servicio.

Cambio de registro — Un registro que describe los cambios específicos en un documento, en este caso, un documento de términos de servicio.

Ciberamenaza — El proceso por el cual un acto malicioso (que incluyen pero no se limitan a criminales, informantes o estados nacionales) puede obtener acceso no autorizado a la información del usuario por medio de ataque informático, phishing u otras técnicas engañosas.

Comentario a nivel de gerencia — Comentario de trabajadores de la empresa con roles y títulos gerenciales que no son parte del equipo directivo.

Comité a nivel directivo — Un comité del directorio de la empresa (o ente de gobierno similar).

Compromiso político — El compromiso de la empresa debe ser parte de un documento de política de derechos humanos. Esto representa una declaración formal que ha pasado por un proceso de evaluación y ha recibido aprobación en los niveles más altos de la empresa. Los compromisos o declaraciones generales hechos en documentos que no son de políticas (por ejemplo, informes de responsabilidad social corporativa, páginas web, entradas en blogs, comunicados de prensa) no cuentan.

Compromiso significativo — La empresa analiza libertad de expresión y privacidad en sus propios materiales así como en presentaciones externas (por ejemplo, presentaciones, medios, etc.). La empresa ha analizado libertad de expresión y privacidad varias veces, no solamente una vez. La empresa responde reacciona a problemas de libre expresión y privacidad (por ejemplo, haciendo declaraciones públicas, interponiendo demandas, etc.).

Contenido — La información contenida dentro de comunicaciones de telefonía, oral o electrónica (por ejemplo, una conversación que se realiza por teléfono o cara a cara, el texto escrito y transmitido en un SMS o por correo electrónico).

Datos del usuario — La información de contenido o sin contenido de los usuarios y sus comunicaciones (ver definiciones de "contenido" y "sin contenido" para más detalles). Nótese que los indicadores P9-P11 usan el término "información del usuario" para igualar el lenguaje usado en los "informes de transparencia" de las empresas con respecto a solicitudes de terceros de información sobre los usuarios. El resto de esta metodología usa el término "información del usuario" como se define más abajo, cuando se refiere a información que una empresa tiene con respecto a un usuario específico.

Destacado — La revelación de la empresa es fácil de encontrar en el sitio web de la empresa.

Documentación — La empresa proporciona registros que los usuarios pueden consultar.

Encriptación — Esencialmente, oculta el contenido de las comunicaciones para que solamente el destinatario previsto pueda verlo. El proceso usa un algoritmo para convertir el mensaje (texto sin formato) a un formato codificado (texto cifrado) para que el mensaje parezca una serie aleatoria de caracteres para quien lo vea. Solamente alguien con la clave de encriptación apropiada, que revierta el texto cifrado de nuevo a texto sin formato. La información se puede encriptar cuando se guarda y cuando está en transmisión.

Por ejemplo, los usuarios pueden encriptar la información en su disco duro para que solamente el destinatario previsto con la clave de encriptación pueda descifrar los contenidos de la unidad. Además, los usuarios pueden enviar un mensaje de correo electrónico encriptado, que evitaría que nadie viera el contenido de los correos electrónicos mientras un mensaje está moviéndose a través de la red para llegar al destinatario previsto. Con una encriptación en tránsito (por ejemplo, visible cuando un sitio web usa HTTPS), la comunicación entre un usuario y un sitio web está encriptada, para que personas externas, como el proveedor de servicios de internet del usuario, solamente pueda ver la visita inicial al sitio web, pero no lo que el usuario comunica en ese sitio web, o las subpáginas que el usuario visita.

Para más información, ver este recurso: http://www.explainthatstuff.com/encryption.html.

Entrega — Cuando paquetes de datos llegan a un usuario final.

Evaluaciones de impacto de derechos humanos (HRIA, por su nombre en inglés) — Para los fines de esta metodología, los HRIA son un enfoque sistemático de la debida diligencia. Una empresa realiza estas evaluaciones o revisiones para ver cómo sus productos, servicios y prácticas empresariales afectan la libertad de expresión y privacidad de sus usuarios.

Para más información sobre evaluaciones de impacto de derechos humanos y mejores prácticas para llevarlas a cabo, ver esta página especial presentada por el Centro de Recursos de Negocios y Derechos Humanos: http://www.business-humanrights.org/UNGuidingPrinciplesPortal/ToolsHub/Empresas/StepTaken/ImpactAssessment

El Instituto Danés para Derechos Humanos ha elaborado una herramienta relacionada para Cumplimiento de Evaluación de Derechos Humanos (https://hrca2.humanrightsbusiness.org), y BSR ha elaborado una útil guía para realizar una HRIA: http://www.bsr.org/en/our-insights/bsr-insight-article/how-to-conduct-an-effective-human-rights-impact-assessment

Para una guía específica para el sector de TIC, ver el capítulo extraído del libro ("Negocios, derechos humanos e internet: Marco de trabajo para implementación") de Michael Samway en el sitio web del proyecto: http://rankingdigitalrights.org/resources/readings/samway_hria

Ver también la Parte 3 Sección 2 sobre evaluación en la Guía del Sector de TIC de la Comisión Europea sobre Implementación de Principios Rectores de Naciones Unidas sobre Negocios y Derechos Humanos: http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf

Explícito — La empresa afirma específicamente su apoyo a la libertad de expresión y privacidad.

Fácil de encontrar — La información o documento se ubica en la página de inicio de la empresa o servicio, o como mucho, en una página que está a un clic de distancia de la página de inicio.

Fácil de entender y manera comprensible — La empresa ha tomado medidas para ayudar a los usuarios a realmente entender la información. Esto incluye, pero no se limita a, ofrecer resúmenes, consejos o asesoría que explican lo que significan los términos, usando encabezados de las secciones, fuentes en tamaños legibles u otros rasgos gráficos que ayude a los usuarios a entender el documento, o escribir los términos usando una sintaxis legible.

Formación de tráfico — Ajustar el flujo de tráfico a través de una red. Esto puede implicar condicionalmente el retraso de algunos tipos de tráfico. La formación de tráfico se puede usar con fines de gestión de red (por ejemplo, priorizar tráfico de VoIP antes de tráfico web normal para facilitar comunicación en tiempo real) o por razones que contrarrestan principios de neutralidad en la red (por ejemplo, retrasar intencionalmente tráfico de video para persuadir a los usuarios de no usar aplicaciones de gran ancho de banda) (actualizado el 10 de julio de 2015).

Funcionario — Un trabajador con rango superior responsable por un grupo explícito de riesgos e impactos, en este caso, privacidad y libertad de expresión.

Información anónima — La información no está conectada de ninguna manera con otra información que podría permitir que se identifique a un usuario. La naturaleza amplia de esta definición usada por el proyecto de *Ranking Digital Rights* es necesaria para reflexionar sobre varios datos. Primero, los analistas especializados pueden quitarle el anonimato a grandes conjuntos de datos. Esto hace que casi todas las promesas de anonimato sean inalcanzables. En esencia, cualquier información vinculada a un 'identificador anónimo' no es anónima; más bien, a menudo es información pseudónima que puede ser vinculada a la identidad fuera de línea del usuario. Segundo, la metadata puede revelar más de las asociaciones e intereses del usuario que el contenido de la información, así pues, esta información es de vital interés. Tercero, las entidades que tienen acceso a muchas fuentes de datos, como corredores de datos y gobiernos, pueden emparejar dos o más fuentes de datos para revelar información sobre los usuarios. Así, agentes sofisticados pueden usar datos que parecen anónimos para elaborar una imagen mayor de un usuario.

Información del usuario — Toda información que está conectada a una persona identificable, o puede estar conectada a esa persona por medio de combinación de conjuntos de datos o utilizando técnicas de minería de datos. Como explicación adicional, la información del usuario es toda información que documenta las características y/o actividades de un usuario. Esta información puede o no estar vinculada a la cuenta de un usuario específico. Esta información incluye, pero no se limita a, correspondencia personal, contenido generado por el usuario, preferencias y configuraciones de cuenta, datos de registro y acceso, información sobre las actividades o preferencia de un usuario recopilada de terceros ya sea a través de rastreo de comportamiento o de adquisición de información, y todas las formas de metadata. La información del usuario nunca se considera anónima, excepto cuando se incluye solamente como una base para generar mediciones globales (por ejemplo, número de usuarios activos mensuales). Por ejemplo, la declaración 'Nuestro servicio tiene un millón de usuarios activos mensualmente' contiene información anónima, pues no brinda suficiente información para saber quiénes son ese millón de usuarios.

Información estructurada — "Información que yace en campos fijos dentro de un registro o archivo. Las bases de datos relacionales y hojas de cálculo son ejemplos de información estructurada. Aunque la información en archivos XML no están fijos en una ubicación como los registros de bases de datos tradicionales, están estructurados porque la información está etiquetada y puede identificarse correctamente". En cambio, la información no estructurada es información que "no yace en ubicaciones fijas. El término generalmente se refiere a texto espontáneo, que es ubicuo. Los ejemplos son documentos de procesadores de palabras, archivos PDF, mensajes de correo electrónico, blogs, páginas web y sitios sociales".

Fuente: Enciclopedia PC Mag de "información estructurada"
http://www.pcmag.com/encyclopedia/term/52162/structured-data
"información no estructurada"
http://www.pcmag.com/encyclopedia/term/53486/unstructured-data

Iniciativa multipartidaria — Una organización multipartidaria y confiable incluye y está dirigida por miembros de al menos otros tres grupos interesados, aparte del sector: sociedad civil, inversionistas, académicos, usuarios o consumidores en general, comunidad técnica y/o gobierno. Su modelo de financiación se deriva de más de una fuente (corporaciones, gobiernos, fundaciones, donaciones públicas, etc.). Su

independencia, rigor y profesionalismo son de alto nivel, con fuerte participación de organizaciones de derechos humanos que tienen por sí mismas un sólido historial de independencia del control corporativo y/o gubernamental. *Global Network Initiative* es un ejemplo de una iniciativa multipartidaria dedicada a la libertad de expresión y privacidad.

Intercambiar / Compartir — La empresa permite que un tercero tenga acceso a la información del usuario, ya sea entregando libremente la información a un tercero (o el público, u otros usuarios) o vendiéndola a un tercero.

Interesados — Personas que tienen un "interés" porque están afectados de alguna manera por las acciones o decisiones de una empresa. Nótese que los interesados no son los mismos que los "titulares de derechos" y que hay diferentes tipos de interesados: los que están directamente afectados, y los "interesados intermediarios" cuyo rol es defender los derechos de los interesados directos.
• Titulares de derechos son las personas cuyos derechos humanos podrían verse impactados directamente. Interactúan con la empresa y sus productos y servicios a diario, por lo general como trabajadores, clientes o usuarios.
• Interesados intermediarios incluyen a personas y organizaciones informadas que pueden hablar en nombre de los titulares de derechos, como organizaciones de la sociedad civil, grupos activistas, académicos, líderes de opinión y legisladores" (p. 10 de 28).

Fuente: Compromiso de los interesados en diligencia debida en derechos humanos: Desafíos y soluciones para empresas TIC de BSR, septiembre de 2014
http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf

Libremente disponible — Una persona puede ver la información sin tener que iniciar sesión, hacer una compra, descargar software, agregar una conexión o cookie, ni brindar información alguna ni tomar acción a cambio de ver la información.

Minimización de datos — Según el Supervisor Europeo de Protección de Datos (EDPS, por su nombre en inglés), "el principio de 'minimización de datos' significa que un controlador de datos ["la institución o entidad que determina el propósito y medios del procesamiento de datos personales"] debería limitar la recopilación de información personal a lo directamente relevante y necesario para lograr un propósito específico. Además, debe retener la información solamente por el tiempo que sea necesario para lograr ese propósito. En otras palabras, los controladores de datos deberían recopilar solamente la información personal que realmente necesitan, y solamente la deben conservar durante en el tiempo que la necesiten".

Fuente: Supervisor Europeo de Protección de Datos, Glosario de Protección de Datos, https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74

Nivel de gerencia — Un comité, programa, equipo o funcionario que no es parte del directorio de la empresa ni del equipo directivo.

No Rastrear — También conocido por el acrónimo "DNT" por su nombre en inglés, se refiere a una configuración en las preferencias del navegador de un usuario que dice a las entidades que no los "rastree". En otras palabras, cada vez que un usuario carga un sitio web, a todas las partes involucradas en enviar la página (que a menudo son muchas, principalmente anunciantes) se les dice que no recopilen ni guarden ninguna información sobre la visita del usuario a la página. Sin embargo, esta es una solicitud de mera educación - una empresa puede ignorar una solicitud de no rastrear, y la amplia mayoría lo hace.

Opciones para controlar — La empresa proporciona al usuario un mecanismo directo y fácil de entender para incluirse o excluirse de recopilación de información, uso o intercambio. "Incluirse" significa que la empresa no recopila, usa ni intercambia información con un fin determinado hasta que los usuarios señalan explícitamente que quieren que sea así. "Excluirse" significa que la empresa usa la información para un propósito específico por defecto, pero que dejará de hacerlo una vez que el usuario le diga a la empresa que deje de hacerlo. Nótese que esta definición es potencialmente polémica pues muchos defensores de la privacidad creen que solamente "incluirse" constituye control aceptable. Sin embargo, para los fines de RDR, hemos elegido contar "excluirse" como una forma de control.

Órdenes judiciales — Órdenes emitidas por un tribunal o un juzgado. Incluyen órdenes judiciales en casos penales y civiles.

Participación de interesados — Interacciones entre la empresa y los interesados. Las empresas o los interesados pueden iniciar estas interacciones, y pueden tomar diversos formatos, incluidas reuniones, otra comunicación, etc.

Políticas de privacidad — Los documentos que resumen las prácticas de una empresa que tienen que ver con la recopilación y uso de información, sobre todo información sobre los usuarios.

Fuente: "Protegiendo la privacidad del consumidor en un era de cambios rápidos: Recomendaciones para empresas y legisladores", Comisión Federal de Comercio de los Estados Unidos, marzo de 2012, p. 77.
https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Priorización — La priorización ocurre cuando el operador de una red "maneja su trabajo de una manera que beneficia contenido, aplicaciones, servicios o dispositivos en particular". Para los fines de RDR, esta definición de priorización incluye la decisión de una empresa de bloquear acceso a una aplicación, servicio o dispositivo particular.

Fuente: Reglas Abiertas de Internet 2015 de la Comisión Federal de Comunicaciones de Estados Unidos, p. 7 de 400,
https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

Proceso para aplicación de reglas — Esto incluye casos en que una empresa bloquea, filtra, retira o vuelve de alguna manera inaccesible un contenido. También incluye casos en que una empresa cierra, bloquea o niega el servicio de alguna manera (ya sea borrando cuentas de usuarios o cerrando el servicio) a una persona o grupo de personas debido a algo que el usuario ha hecho en el servicio.

Programa / Equipo — Una unidad definida dentro de una empresa que tiene la responsabilidad de cómo se cruzan los productos o servicios de la empresa, este caso, con libertad de expresión y/o privacidad.

Programa de informantes — Este es un programa a través del cual los trabajadores de la empresa pueden informar de cualquier supuesta actividad ilícita que vean dentro de la empresa, incluyendo asuntos relacionados con derechos humanos. Típicamente, toma la forma de una línea directa anónima y a menudo es responsabilidad de un jefe de conformidad o jefe de ética.

Reclamo — "[Una] injusticia detectada que suscita la sensación de una persona o grupo de tener derecho, que se puede basar en la ley, contrato, promesas explícitas o implícitas, prácticas habituales o nociones generales de justicia de comunidades agraviadas" (p. 32 de 42).

Fuente: "Principios rectores de negocios y derechos humanos: Implementando el 'Marco de trabajo de protección, respeto y solución" de Naciones Unidas, 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Recinto destacado — Esto puede incluir declaraciones públicas o hechas delante de una audiencia pública significativa, incluida una importante conferencia pública, una entrevista en la prensa, en una entrada del blog de la empresa, en archivos de valores públicos, etc. Esto no incluye los comunicados de prensa de la empresa.

Recopilar / Recopilación — Todos los medios por los cuales una empresa puede reunir información sobre los usuarios. Una empresa puede recopilar esta información directamente de los usuarios, por ejemplo, cuando los usuarios envían contenido generado por el usuario a la empresa. Una empresa también puede recopilar esta información indirectamente, por ejemplo, registrando datos de registro, información de cuenta, metadata y otra información relacionada que describa a los usuarios y/o documente sus actividades.

Regulación — Una manera directa de formación de tráfico en que el operador de una red retrasa el flujo de paquetes a través de una red. Los operadores móviles pueden regular el tráfico para aplicar límites de datos (actualizado el 10 de julio de 2015).

Para más información, ver: Open Signal, "Regulación de datos: Por qué los operadores retrasan tu velocidad de conexión". http://opensignal.com/blog/2015/06/16/data-throttling-operators-slow-connection-speed

Restricción de cuenta / restringir la cuenta de un usuario — Limitación, suspensión, desactivación, supresión o retiro de la cuenta de un usuario específico o de permisos en la cuenta de un usuario.

Restricción de servicio — La empresa bloquea, cancela o evita de alguna otra manera el acceso al servicio. La restricción del servicio puede darse con un usuario específico, un grupo de usuarios o usuarios en una zona en particular.

Retención de información del usuario — Una empresa puede recopilar información y luego borrarla. Si la empresa no la borra, la información está "retenida". El tiempo entre recopilación y eliminación es el 'periodo de retención'. Esa información puede caer dentro de nuestra definición de 'información del usuario', o puede ser anónima. Hay que tener en cuenta que la información verdaderamente anónima de ninguna manera puede ser vinculada a un usuario, a la identidad, comportamiento o preferencia de un usuario, lo que es muy raro.

Un asunto relacionado es el 'periodo de retención'. Por ejemplo, la empresa puede recopilar información de registro de manera continua, pero purgar (borrar) la información una vez por semana. En este caso, el periodo de retención de información es de una semana. Sin embargo, si no se especifica un periodo de retención, se asume por defecto que la información no se borra nunca, y que por tanto el periodo de retención es infinito. En muchos casos, los usuarios pueden querer que se retenga su información mientras usan

el servicio activamente, pero les gustaría que se eliminara (y por lo tanto, que no se retuviera) si y cuando dejaran de usar el servicio. Por ejemplo, los usuarios pueden querer que el servicio de una red social conserve todos sus mensajes privados, pero cuando el usuario deja la red, podría querer que todos sus mensajes privados se borren.

Señales generadas por el usuario — Muchas empresas permiten a los usuarios que "se excluyan" del rastreo configurando una variedad de cookies específicas para la empresa. Si un usuario borra cookies para proteger la privacidad, entonces se le rastrea hasta que reconfigure la cookie de "excluirse". Además, algunas empresas pueden requerir que un usuario instale un navegador adicional para evitar el rastreo. Esos dos escenarios comunes son ejemplos de usuarios a los que se obligue a usar señales que son específicas para la empresa; y por lo tanto no cuentan. En cambio, una señal generada por el usuario viene del usuario y es un mensaje universal de que el usuario no debe ser rastreado. La opción principal para la señal generada por el usuario hoy es el encabezado "No Rastrear" (cubierto arriba), pero esta redacción deja la puerta abierta a futuros medios para que los usuarios señalen que no quieren ser rastreados.

Sin contenido — Información sobre una instancia de comunicación o sobre un usuario. Las empresas pueden usar diferentes términos para referirse a esta información, incluyendo metadata, información básica del abonado, datos transaccionales sin contenido, información de la cuenta o información del cliente. *The Guardian* tiene un guía útil con ejemplos de qué es lo que cuenta como metadata en diversos servicios.

En Estados Unidos, la ley de Comunicaciones Almacenadas define las comunicaciones o registros de clientes sin contenido como, "nombre; dirección, registros de conexión telefónico local y de larga distancia, o registros de la hora y duración de las sesiones; extensión del servicio (incluida fecha de inicio) y tipo de servicios utilizados; número de teléfono o de instrumento u otro número de abonado o identidad (incluida la dirección de cualquier red asignada temporalmente); y medio y fuente de pago por ese servicio (incluido cualquier tarjeta de crédito o número de cuenta bancaria)". El Manual de la Unión Europea sobre la Ley Europea de Protección de Datos establece: "La confidencialidad de comunicaciones electrónicas compete solamente al contenido de una comunicación sino también a la información de tráfico, como información sobre quién se comunicó con quién, cuándo y por cuánto tiempo, y datos de ubicación, como desde dónde se comunicaron los datos".

http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1100110

Solicitudes privadas — Solicitudes hechas por cualquier persona o entidad que no actúa bajo autoridad gubernamental directa o judicial. Estas solicitudes pueden venir de un organismo de autorregulación, como *Internet Watch Foundation*, o un sistema de notificación y retiro, como la Ley Digital del Milenio para los Derechos de Autor. Para más información sobre notificación y retiro, así como sobre la Ley Digital del Milenio para los Derechos de Autor específicamente, ver el reciente informe de UNESCO: "Fomentar la libertad en línea: El rol de los Intermediarios de internet" en http://unesdoc.unesco.org/images/0023/002311/231162e.pdf (p. 40-52 de 211).

Solicitudes gubernamentales — Incluye solicitudes de ministerios del gobierno o agencias, autoridades y órdenes judiciales en casos penales y civiles.

Solicitudes gubernamentales no judiciales — Estas son solicitudes que vienen de entidades no gubernamentales que no son entes judiciales, jueces ni tribunales. Pueden

incluir solicitudes de ministerios del gobierno, agencias, departamentos de policía, funcionarios de policía (actuando con carácter oficial) y otras oficinas, autoridades o entidades gubernamentales no judiciales.

Solución — "La solución puede incluir disculpas, restitución, rehabilitación, compensación financiera o no financiera y sanciones punitivas (ya sean penales o administrativas, como multas), así como la prevención de perjuicio, por ejemplo, requerimientos o garantías de no repetición. Los procedimientos para la provisión de soluciones debe ser imparcial, protegidos de corrupción y libres de intentos políticos u otros para influenciar en el resultado" (p. 22 of 27).

Fuente: "Informe del Representante Especial del Secretario General en el asunto de derechos humanos y corporaciones transnacionales y otras empresas comerciales, John Ruggie. Principios rectores en negocios y derechos humanos: Implementando el marco de trabajo del proyecto de Naciones Unidas 'Protección, Respeto y Solución" 2011. http://businesshumanrights.org/sites/default/files/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf

Ver también: el Plan de Solución de Telco por Acceso: https://s3.amazonaws.com/access.3cdn.net/fd15c4d607cc2cbe39_onm6ii982.pdf

Supervisar / Vigilar — Los documentos que dirigen la empresa o los procesos de toma de decisiones asignan un comité, programa, equipo o funcionario con autoridad supervisora formal para una función en particular. Este grupo o personas tienen responsabilidad por su función y se evalúa en base al grado en que cumple con esa responsabilidad.

Supervisión a nivel ejecutivo — El comité ejecutivo o un miembro del equipo directivo de la empresa supervisa directamente asuntos relacionados con la libertad de expresión y privacidad.

Términos de Servicio — Este documento también se puede llamar Términos de uso, Términos y condiciones, etc. Los términos de servicio "a menudo ofrecen normas básicas necesarias de cómo se deben usar diversos servicios en línea", como lo establece EFF, y representan un acuerdo legal entre la empresa y el usuario. Las empresas pueden tomar acción contra los usuarios y su contenido basándose en la información en los términos de servicio.

Fuente: Electronic Frontier Foundation, "Términos de (Ab)uso" https://www.eff.org/issues/terms-of-abuse

Tercero — Una "parte" o entidad que no es más que el usuario o la empresa. Para los propósitos de esta metodología, los terceros pueden incluir organizaciones gubernamentales, juzgados u otros privados (por ejemplo, una empresa, una ONG, una persona) (nótese que esta es una definición intencionalmente amplia e inclusiva).

Transmisión — El movimiento de paquetes de datos a través de una red.

Usuarios — Incluye a las personas que publican o transmiten el contenido en línea así como quienes tratan de acceder o recibir el contenido.

Apéndice 2 – Guía de investigación

A continuación, mayores detalles que explican cómo se evalúa cada indicador, extraídos de una Guía del Investigador más extensa y que todos los investigadores de RDR están obligados a seguir.

C1

Este indicador busca evidencia de que la empresa y las personas que dirigen las empresas han hecho compromisos públicos sobre la importancia de la libertad de expresión y privacidad.

Evaluación: Este indicador se evalúa en dos partes. Una empresa solamente puede recibir crédito total por este indicador si recibe un "Sí" en la parte A y "comentarios a nivel ejecutivo" para la parte B. Esperamos ver compromisos de la empresa que se relacionen con la libertad de expresión y la privacidad.

Posibles fuentes:

- Política de derechos humanos de la empresa
- Un listado de la empresa de su equipo administrativo que identifique a quién define la empresa como nivel ejecutivo (para el elemento B1). Organigrama, informes anuales o declaraciones de poder de la empresa también podrían identificar quién es parte del equipo administrativo de la empresa.
- Principales medios de comunicación
- Grabaciones o transcripciones de conferencias públicas
- Respuestas públicas, cartas u otras comunicaciones con legisladores o agencias del gobierno
- Comunicaciones públicas con organizaciones de la sociedad civil
- Artículos de blog de la empresa (con el autor claramente nombrado)

C2

Este indicador busca revelación de la empresa de que la dirigencia de la empresa y las estructuras internas de gestión incluyen consideraciones a la libertad de expresión y la privacidad. Las decisiones tomadas por ejecutivos y gerentes de las empresas de internet y telecomunicaciones afectan significativamente la capacidad de las personas de experimentar la libertad de expresión y privacidad. Esperamos que estos procesos de toma de decisión y la cadena de responsabilidad dentro de la empresa consideren explícitamente estos derechos humanos.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si revelan información sobre cómo toman en cuenta estos asuntos a nivel directivo, ejecutivo y gerencial. A nivel directivo, sería un comité. Por debajo del nivel directivo, puede incluir una unidad o personas de la empresa que reporta a la instancia ejecutiva o gerencial. El comité, programa, equipo, funcionario, etc. deberá identificar específicamente libertad de expresión y privacidad en su descripción de responsabilidades.

Posibles fuentes:

- Lista de comités del directorio
- Documentos que rigen a la empresa
- Informe de responsabilidad social corporativa de la empresa
- Organigrama de la empresa
- Política de derechos humanos de la empresa

C3

Los Indicadores C1 y C2 se centran en los dirigentes de la empresa y quienes toman las decisiones. Este indicador busca revelación de la empresa de cómo también ayuda al resto de sus trabajadores

a entender la importancia de la libertad de expresión y privacidad. Cuando los empleados escriben un código para un nuevo producto, revisan la solicitud de información del usuario o responden preguntas de clientes sobre cómo usar un servicio, actúan de manera que puede afectar directamente la libertad de expresión y privacidad de la gente. Esperamos que las empresas revelen información sobre si ofrecen capacitación que informe a los trabajadores de su rol en el respeto de derechos humanos y que proporciona a los trabajadores un medio para expresar las preocupaciones que tienen con respecto a derechos humanos.

Evaluación: Este indicador se evalúa usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si revelan información sobre capacitación de los trabajadores en libertad de expresión y privacidad y si revelan la existencia de un programa de informantes que abarca esos asuntos. La revelación en torno a la capacitación de los trabajadores deberá especificar que la capacitación abarca libertad de expresión, privacidad o ambas.

Posibles fuentes:

- Código de conducta de la empresa
- Manual del trabajador
- Organigrama de la empresa
- Informe de responsabilidad social corporativa de la empresa
- Entradas en el blog de la empresa

C4

Este indicador examina si las empresas revelan la existencia de cualquier proceso de evaluaciones de impacto de derechos humanos (HRIA), incluyendo libertad de expresión y privacidad (ver definición y referencias en el Apéndice 1).

Nótese que este indicador no espera que las empresas publiquen resultados detallados de sus evaluaciones de impacto de derechos humanos, pues una evaluación minuciosa incluye información delicada. En cambio, espera que las empresas revelen que llevan a cabo evaluaciones de impacto de derechos humanos y brinden información sobre qué abarca su proceso de evaluaciones de impacto de derechos humanos.

Aunque este indicador usa el lenguaje de evaluaciones de impacto de derechos humanos, las empresas pueden usar diferentes nombres para este proceso de revisión. Lo que las empresas llaman proceso es menos importante que lo que el proceso abarca o consigue. Este indicador incluirá una revisión de Evaluaciones de Impacto en la Privacidad y otros procesos de evaluación que contiene características o componentes enumerados en este indicador, pero no necesariamente se llaman “evaluaciones de impacto de derechos humanos”.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente reciben crédito total si demuestran que su proceso de evaluación aborda todos los elementos de la lista de verificación. Si una empresa lleva a cabo evaluaciones de impacto de derechos humanos pero no hay revelación pública del hecho de que las lleva a cabo, la empresa no recibirá crédito.

Posibles fuentes:

- Informes de responsabilidad social corporativa de la empresa
- Política de derechos humanos de la empresa
- Documentos regulatorios (por ejemplo, Comisión Federal de Comercio de Estados Unidos)
- Informes de terceros asesores u organismos acreditadores
- Informes de evaluación de *Global Network Initiative*

C5

Este indicador busca evidencia de que la empresa interactúa con sus interesados, particularmente los que enfrentan riesgos en derechos humanos en relación con sus actividades en línea.

Interactuar con los interesados, sobre todo los que operan en ambientes de alto riesgo, puede ser delicado. Una empresa puede no sentirse cómoda de revelar públicamente detalles específicos acerca de qué interesados consulta, dónde o cuándo se reúnen y qué discuten. Aunque exhortamos a las empresas a ofrecer detalles que no sean delicados sobre participación de los interesados, buscamos como mínimo, revelación pública de que una empresa interactúa con los interesados que son o representan a usuarios cuyos derechos de libertad de expresión y privacidad están en riesgo. Una manera en que el público sabe que una empresa participa en este tipo de interacción es a través de su participación en una iniciativa multipartidaria que pone en contacto a la empresa con representantes de diversos grupos de interesados, incluidas organizaciones de derechos humanos y otros que defienden los derechos de grupos en riesgo.

Evaluación: Una empresa solamente recibirá crédito total para este indicador si cumple con el elemento A. Una empresa recibirá crédito parcial si cumple uno o dos elementos de B.

Posibles fuentes:

- Informe de responsabilidad social corporativa de la empresa
- Informe anual de la empresa
- Blog de la empresa
- Listas de membrecías de los sitios web de *Global Network Initiative* e *Industry Dialogue*
- Preguntas frecuentes de la empresa o centro de ayuda

C6

Este indicador examina si las empresas ofrecen mecanismos de solución y si tienen un proceso dado a conocer públicamente para responder a informes de reclamos o reclamos de personas que creen que la empresa ha violado o facilitado directamente la violación de su derecho de libertad de expresión o privacidad.

Evaluación: Este indicador se evalúa usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si pueden demostrar que sus mecanismos de solución y reclamo incluyen todos los elementos de la lista de verificación.

Posibles fuentes:

- Términos de servicios de la empresa o acuerdos de usuario equivalentes
- Políticas de contenido de la empresa
- Políticas privadas de la empresa, guías de privacidad o sitio de recursos de privacidad
- Informe de responsabilidad social corporativa de la empresa
- Centro de ayuda o guía del usuario de la empresa
- Informe de transparencia de la empresa (por el número de quejas recibidas).

F1

Los términos de servicio resumen la relación entre el usuario y la empresa, y las empresas pueden tomar acción contra los usuarios de acuerdo con las condiciones descritas en los términos. Dado esto, esperamos que las empresas proporcionen libremente estos términos y que hagan un esfuerzo para ayudar a los usuarios a entender qué quieren decir.

Evaluación: Este indicador se evalúa usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación cumple con todos los elementos de la lista de verificación. Este indicador incluye un resumen de otros documentos como “guías de la comunidad” o reglas específicas para el servicio que explican más a los usuarios qué significan

los términos. Las políticas de privacidad NO están incluidas en este indicador pues están cubiertas en indicadores separados en la sección "Privacidad".

Posibles fuentes:

- Términos de servicio de la empresa, términos de uso, términos y condiciones, etc.
- Política de uso aceptable de la empresa, guías de la comunidad, reglas, etc.

F2

Es común que las empresas cambien sus términos de servicio a medida que su negocio evoluciona. Esperamos que las empresas se comprometan a notificar a los usuarios cuando cambien estos términos y que brinden información a los usuarios para que entiendan qué significan estos cambios. Este indicador busca revelación de la empresa sobre el método y periodo en el que las empresas se comprometen a notificar a los usuarios acerca de cambios en los términos de servicio. También busca evidencia de que una empresa proporciona registros disponibles de términos anteriores para que la gente pueda entender cómo han evolucionado con el tiempo los términos de la empresa.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación cumple con todos los elementos de la lista de verificación.

Posibles fuentes:

- Términos de servicio de la empresa

F3

A menudo, las empresas fijan límites sobre el contenido que los usuarios pueden publicar sobre un servicio así como con qué actividades los usuarios pueden participar en el servicio. Esperamos que las empresas revelen a sus usuarios qué son estas reglas y cómo las aplican las empresas. Esto incluye requisitos legales para bloquear algunos tipos de contenido así como restricciones relacionadas con la propiedad intelectual (por ejemplo, infracción a los derechos de autor). En esta revelación, la empresa también debería ofrecer ejemplos para ayudar a los usuarios a entender qué significan estas reglas.

Evaluación: Este indicador se evalúa usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementes en la lista de verificación.

Posibles fuentes:

- Términos de servicio de la empresa, contrato de usuario, política de uso aceptable, parámetros de la comunidad, guías de contenido, comportamiento abusivo o documento similar que explique las reglas que los usuarios deben seguir.
- Respaldo de la empresa, centro de ayuda o preguntas frecuentes (por ejemplo, pregunta en torno a por qué se retira contenido, por qué se suspende una cuenta, etc.).

F4

El Indicador F3 examina la revelación de restricciones de la empresa sobre lo que los usuarios pueden publicar o hacer en un servicio, mientras que este indicador observa la revelación de restricciones de la empresa en la capacidad de un usuario para acceder a un servicio. Las empresas pueden restringir el acceso a un servicio borrando la cuenta de un usuario o cerrando un servicio por completo. Esperamos que las empresas expliquen a sus usuarios las circunstancias bajo las cuales pueden emprender esa acción.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación tiene todos los elementos de la

lista de verificación. El elemento 2 solamente es aplicable a empresas de telecomunicación; las empresas de internet recibirán una puntación de N/A (no aplicable) para el elemento 2. Las empresas de internet deben cumplir con los elementos 1 y 3 para recibir crédito total para este indicador.

Posibles fuentes:

- Términos de servicio de la empresa, contrato de usuario, política de uso aceptable, parámetros de la comunidad, guías de contenido, política de comportamiento abusivo o documento similar que explique las reglas que los usuarios deben seguir.
- Respaldo de la empresa, centro de ayuda o preguntas frecuentes (por ejemplo, pregunta sobre por qué se retira contenido, por qué se suspende una cuenta, etc.).

F5

El Indicador F3 examina la revelación de la empresa de restricciones sobre lo que los usuarios pueden publicar sobre un servicio, y el indicador F4 analiza la revelación de restricciones de la empresa a la capacidad de un usuario de acceder a un servicio. Este indicador, F5, se centra en si las empresas revelan que notifican a los usuarios cuando toman este tipo de acciones. Esperamos que las empresas revelen un compromiso para notificar a los usuarios cuando han retirado contenido, restringido la cuenta de un usuario o han restringido de alguna manera la capacidad de un usuario de acceder a un servicio. Esta revelación debería ser parte de las explicaciones de las empresas de prácticas de restricción de contenido y acceso.

Evaluación: Este indicador se evalúa usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación.

Posibles fuentes:

- Términos de servicio de la empresa, política de uso aceptable, parámetros de la comunidad, guías de contenido, política de comportamiento abusivo o documento similar que explique las reglas que los usuarios deben seguir.
- Respaldo de la empresa, centro de ayuda o preguntas frecuentes (por ejemplo, pregunta en torno a por qué se retira contenido, por qué se suspende una cuenta, etc.)
- Política de derechos humanos de la empresa

F6

Cada vez más, las empresas reciben solicitudes de retirar, filtrar o restringir acceso a contenido. También pueden recibir solicitudes de restringir acceso a usuarios o, en casos raros, cerrar una red. Estas solicitudes pueden venir de agencias gubernamentales, juzgados o privados. Esperamos que las empresas revelen públicamente su proceso explicando cómo responden a solicitudes de cada tipo de tercero.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación.

Posibles fuentes:

- Informe de transparencia de la empresa
- Guías de aplicación de la ley de la empresa
- Términos de servicio de la empresa
- Política de la empresa sobre derechos de autor o propiedad intelectual
- Centro de ayuda o de respaldo de la empresa
- Entadas de blog de la empresa

F7

Este indicador examina la revelación de información de la empresa sobre las solicitudes que recibe de los gobiernos para retirar contenido. Hacer pública esta información ayuda a tener una mayor comprensión de cómo la libertad de expresión opera en línea, y ayuda a al público a que empresas y gobiernos rindan cuentas por sus respectivos roles en el respeto y protección a la libertad de expresión. Por estas razones, esperamos que las empresas publiquen frecuentemente información sobre las solicitudes gubernamentales que reciben para retirar contenido.

En algunos casos, la ley puede impedir que una empresa revele información citada en los elementos de este indicador. Por ejemplo, esperamos que las empresas publiquen números exactos en vez de rangos de números. Reconocemos que las leyes a veces impiden que las empresas lo hagan, y los investigadores documentarán las situaciones cuando sea ese el caso. Pero una empresa perderá puntos si no contiene todos los elementos. Esto representa una situación donde la ley hace que las empresas no sean competitivas, y exhortamos a las empresas a que aboguen por leyes que les permitan respetar plenamente los derechos de los usuarios a la libertad de expresión y privacidad.

Evaluación:

Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación.

Posibles fuentes:

- Informa de transparencia de la empresa

F8

Este indicador examina la revelación de información de la empresa debido a las solicitudes que recibe de privados (no gubernamentales y no judiciales) para retirar contenido. Esperamos que las empresas publiquen con frecuencia información acerca las solicitudes privadas que reciben para retirar contenido (ver definición de “solicitudes privadas” en el Apéndice 1).

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación.

Posibles fuentes:

- Informe de transparencia de la empresa

F9

Las empresas pueden emplear personal para revisar contenido y/o actividad del usuario o pueden depender de mecanismos de aviso de la comunidad a través de los cuales otros usuarios marcan contenido y/o actividad para que la empresa revise. Este indicador busca que la empresa revele información sobre el número de casos en que una empresa ha retirado contenido o restringido acceso de un usuario debido a infracciones a los términos de servicios de la empresa. Hacer pública esta información proporcionará al público una visión más precisa del ecosistema de retiro de contenido así como el propio rol de las empresas en el retiro de contenido. Esperamos que las empresas publiquen con frecuencia información a sobre sus propias decisiones para retirar contenido.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación.

Posibles fuentes:

- Informe de transparencia de la empresa

F10

Este indicador solamente es aplicable a las empresas de telecomunicaciones. Busca revelaciones sobre si las empresas participan en prácticas que afectan el flujo de contenido a través de sus redes. Esperamos que las empresas se comprometan a evitar que priorice o degrade contenido. Si las empresas se comprometen a estas acciones, esperamos que revelen públicamente y expliquen su propósito al hacerlo. Nótese que este indicador no aborda el bloqueo de contenido, que se aborda en el indicador F3. Este indicador incluye revelación de la empresa relacionada con el bloqueo de servicios, aplicaciones o dispositivos, que se consideran un tipo de priorización.

Evaluación: A los investigadores se les da instrucciones de elegir una de cuatro posibles categorías de respuesta. Solamente las empresas que cumplen con los requisitos para la primera categoría de respuesta "La empresa revela que no prioriza ni degrada la entrega de contenido" recibirán crédito total para este indicador. Otras categorías de respuesta reciben progresivamente menos crédito.

Posibles fuentes:

- Explicación de la empresa de gestión de red o prácticas de gestión de tráfico

F11

Este indicador solamente es para empresas de internet. Esperamos que las empresas revelen si piden a los usuarios que confirmen su identidad usando identificaciones emitidas por el gobierno u otras formas de identificación que deberá estar conectada con su identidad fuera de línea.

Evaluación: Este indicador tiene dos respuestas posibles. Una empresa recibirá crédito total si su respuesta es "No", y una empresa no recibirá crédito si su respuesta es "Sí".

Posibles fuentes:

- Términos de servicio de la empresa o documento equivalente
- Centro de asistencia de la empresa
- Página de registro de la empresa

P1

Las políticas de privacidad tratan sobre cómo las empresas recopilan, gestionan, usan y aseguran la información sobre los usuarios así como la información proporcionada por los usuarios. Esperamos que las empresas proporcionen estas políticas libremente y que hagan un esfuerzo para ayudar a los usuarios a entender lo que quieren decir.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación. Los términos de servicio NO están incluidos en este indicador pues están incluidos en indicadores separados en la sección "Libertad de Expresión".

Posibles fuentes:

- Política de privacidad de la empresa, política de uso información

P2

Es común que las empresas cambien sus políticas de privacidad a medida que su negocio evoluciona. Esperamos que las empresas se comprometan a notificar a los usuarios cuando cambien esas políticas y que brinden información a los usuarios para que entiendan qué significan esos cambios. Este indicador busca que la empresa revele el método y periodo en el cual las empresas se comprometen a notificar a los usuarios sobre cambios en las políticas de privacidad.

También busca evidencia de que una empresa proporcione registros disponibles públicamente de políticas anteriores para que las personas puedan entender cómo las políticas de la empresa han evolucionado con el tiempo.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación.

Posibles fuentes:

- Política de privacidad de la empresa, política de uso información

P3

Esperamos que las empresas revelen claramente si recopilan información del usuario (tal como la definimos) y, de ser así, que proporcionen suficiente detalles para que los usuarios puedan entender qué información recopila la empresa, cómo lo hace y su razón para hacerlo.

El término "información del usuario" aparece en muchos indicadores a lo largo de esta sección. RDR hace una interpretación amplia de lo que constituye información del usuario. Nuestra definición es:

"Información del usuario es toda información que está conectada con una persona identificable, o que puede estar conectada a esa persona combinando grupos de datos o utilizando técnicas de minería de datos".

Como explicación adicional, información del usuario es toda información que documenta las características y/o actividades de un usuario. Esta información puede estar vinculada o no a la cuenta de un usuario específico. Esta información incluye, pero no se limita a, correspondencia personal, contenido generado por el usuario, preferencias y configuración de cuentas, datos de registro y acceso, datos sobre las actividades o preferencias de un usuario recopiladas de terceros, ya sea a través de rastreo de comportamiento o compra de datos, y todas las formas de metadata. La información nunca se considera anónima, excepto cuando se incluye únicamente como una base para generar medidas globales (por ejemplo, el número de usuarios activos mensuales). Por ejemplo, la afirmación 'Nuestro servicio tiene un millón de usuarios activos mensuales', contiene información anónima, pues no da suficiente información para saber quiénes son ese millón de usuarios. Nuestra definición es:

"Información anónima es información que no está conectada de ninguna manera a otra información que podría permitir que se identifique a un usuario".

La naturaleza amplia de esta opinión es necesaria para reflejar varios hechos. Primero, analistas calificados pueden hacer que grandes grupos de datos dejen de ser anónimos. Esto hace que casi todas las promesas de anonimato sean inalcanzables. En esencia, toda la información vinculada a un 'identificador anónimo' no es anónima; más bien, a menudo esto es información pseudónima que puede ser vinculada a la identidad fuera de línea de un usuario. Segundo, la metadata puede revelar tanto o más de las asociaciones e intereses de un usuario que la información de contenido, así pues esta información es de vital interés. Tercero, las entidades que tienen acceso a muchas fuentes de datos, como corredores de datos y gobiernos, pueden emparejar dos o más fuentes de datos para revelar información sobre los usuarios. Así, agentes sofisticados pueden usar datos que parecen anónimos para elaborar una imagen mayor de un usuario.

Evaluación: Si la revelación de una empresa afirma que no recopila información del usuario, al cumplir con el elemento A la empresa recibe crédito total para el indicador. Si una empresa no cumple con el elemento A, el investigador buscará que la revelación de la empresa contenga los

elementos de la lista de verificación de B. Una empresa puede recibir crédito parcial si su revelación contiene todos los elementos en la lista de verificación B.

En algunos casos, las leyes o regulaciones pueden requerir que las empresas recopilen alguna información o pueden prohibir o disuadir a la empresa a que revele qué información del usuario recopila. Los investigadores documentarían las situaciones en que este fuera el caso, pero de todas maneras una empresa perderá puntos si no logra cumplir con todos los elementos. Esto representa una situación donde la ley causa que las empresas no sean competitivas, y exhortamos a las empresas a abogar por leyes que les permitan respetar totalmente el derechos de los usuarios a la libertad de expresión y privacidad.

Posibles fuentes:

- Política de privacidad de la empresa (fuente principal)
- Sección sobre protección de información o de recopilación de información de la empresa (fuente secundaria)

P4

Esperamos que las empresas revelen claramente si intercambian información del usuario, tal como la definimos, y de ser así, que brinden suficiente detalle para que los usuarios puedan entender el alcance de este intercambio. Esperamos que la revelación de la empresa aborde el intercambio de la empresa de información del usuario con gobiernos y con entidades comerciales. El término "información del usuario" aparece en muchos indicadores a lo largo de esta sección. RDR toma una interpretación amplia de lo que constituye información del usuario:

"Información del usuario es toda información que está conectada a una persona identificable, o que puede estar conectada a esa persona por medio de combinación de conjuntos de datos o utilizando técnicas de minería de datos".

Como explicación adicional, la información del usuario es toda información que documenta las características y/o actividades de un usuario. Esta información puede o no estar vinculada a la cuenta de un usuario específico. Esta información incluye, pero no se limita a, correspondencia personal, contenido generado por el usuario, preferencias y configuraciones de cuenta, datos de registro y acceso, información sobre las actividades o preferencia de un usuario recopilada de terceros ya sea a través de rastreo de comportamiento o de adquisición de información, y todas las formas de metadata. La información del usuario nunca se considera anónima, excepto cuando se incluye solamente como una base para generar mediciones globales (por ejemplo, número de usuarios activos mensuales). Por ejemplo, la declaración 'Nuestro servicio tiene un millón de usuarios activos mensualmente' contiene información anónima, pues no brinda suficiente información para saber quiénes son ese millón de usuarios. Nuestra definición es:

"Información anónima es información que de ninguna manera está conectada con otra información que podría permitir que se identificara a un usuario".

La naturaleza amplia de esta visión es necesaria para reflexionar sobre varios datos. Primero, los analistas especializados pueden quitarle el anonimato a grandes conjuntos de datos. Esto hace que casi todas las promesas de anonimato sean inalcanzables. En esencia, cualquier información vinculada a un 'identificador anónimo' no es anónima; más bien, a menudo es información pseudónima que puede ser vinculada con la identidad fuera de línea del usuario. Segundo, la metadata puede ser más reveladora de las asociaciones e intereses del usuario que el contenido de la información, así pues, esta información es de vital interés. Tercero, las entidades que tienen acceso a muchas fuentes de datos, como corredores de datos y gobiernos, pueden emparejar dos o más fuentes de datos para revelar información sobre los usuarios. Así, agentes sofisticados pueden usar datos que parecen anónimos para elaborar una imagen mayor de un usuario.

Evaluación: Si la revelación de una empresa afirma que no hace ningún intercambio de información del usuario, al cumplir con el elemento A, la empresa recibe crédito total para el indicador. Si una empresa no cumple con el elemento A, el investigador buscará que la revelación de la empresa cumpla con los elementos de la lista de verificación de B. Una empresa solamente puede recibir crédito parcial si su revelación cumple contiene todos los elementos en la lista de verificación de B.

Posibles fuentes:

- Política de privacidad de la empresa (fuente principal)
- Políticas de la empresa relacionadas con intercambio de información, interacción con terceros (fuente secundaria)

P5

Esperamos que las empresas proporcionen proactivamente a los usuarios opciones para controlar qué información del usuario recopila e intercambia la empresa. Los usuarios deberán poder acceder a estas opciones después de suscribirse al servicio, no simplemente al momento de la suscripción. El simple registro en el servicio no representa consentimiento.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación. Esperamos que las empresas revelen cuáles son las opciones para controlar, y no que simplemente revelen que los usuarios tienen opciones.

Posibles fuentes:

- Política de privacidad de la empresa
- Configuraciones de cuenta de la empresa

P6

Esperamos que las empresas brinden a los usuarios la capacidad de ver y obtener copias de su información que la empresa tiene. La revelación de la empresa debería explicar qué información contiene este registro y qué formatos pueden obtener los usuarios en el registro.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación.

Posibles fuentes:

- Política de privacidad de la empresa
- Configuraciones de cuenta de la empresa
- Centro de asistencia de la empresa
- Entradas de blog de la empresa

P7

Esperamos que las empresas revelen información referente a retención de información. Al considerar la información del usuario, las empresas deberían ser específicas acerca del propósito por el cual recopilan información, usarla solamente para ese fin y descartar la información de manera segura cuando ya no la necesiten para ese fin.

Evaluación: Si la revelación de una empresa afirma que no retiene información del usuario, al cumplir con el elemento A, la empresa recibe crédito total para el indicador. Si una empresa no cumple con el elemento A, el investigador buscará que la revelación de la empresa contenga todos los elementos de la lista de verificación de B. Una empresa solamente puede recibir crédito parcial si su revelación contiene todos los elementos en la lista de verificación de B.

En algunos casos, las leyes o regulaciones podrían requerir que las empresas retengan alguna información durante un periodo determinado. Los investigadores documentarán las situaciones donde este sea el caso, pero de todas maneras una empresa perderá puntos si no logra cumplir con todos los elementos. Esto representa una situación donde una ley causa que las empresas no sean competitivas, y exhortamos a las empresas a que aboguen por leyes que les permitan respetar completamente los derechos de los usuarios a la libertad de expresión y privacidad.

P8

Esperamos que las empresas revelen qué información del usuario recopilan de terceros. Esto ayuda a los usuarios a entender cómo sus actividades fuera del servicio pueden afectar su uso del servicio.

Evaluación: Si la revelación de una empresa afirma que no recopila información del usuario de terceros, al cumplir con el elemento A, la empresa recibe crédito total para el indicador. Si una empresa no cumple con el elemento A, el investigador buscará que la revelación de la empresa cumpla con los elementos de la lista de verificación de B. Una empresa solamente puede recibir crédito parcial si su revelación contiene todos los elementos en la lista de verificación de B.

Posibles fuentes:

- Política de privacidad de la empresa
- Política de la empresa sobre terceros

P9

Cada vez más, las empresas reciben solicitudes de terceros –sobre todo gobiernos, pero a veces otras partes o entidades– para entregar información sobre los usuarios o los contenidos de sus comunicaciones. Este indicador abarca solicitudes de agencias gubernamentales, juzgados y privados. Esperamos que las empresas revelen públicamente sus procesos explicando cómo responden a solicitudes por cada tipo de tercero.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos elementos de la lista de verificación.

En algunos casos, la ley puede impedir que una empresa revele información mencionada en los elementos de este indicador. Los investigadores documentarán las situaciones donde este sea el caso, pero de todas maneras una empresa perderá puntos si no logra cumplir con todos los elementos. Esto representa una situación donde la ley causa que las empresas no sean competitivas, y exhortamos a las empresas a abogar por leyes que les permitan respetar plenamente los derechos de los usuarios a la libertad de expresión y privacidad.

Posibles fuentes:

- Informe de transparencia de la empresa
- Guías de aplicación de la ley de la empresa
- Política de privacidad de la empresa
- Entradas de blog de la empresa

P10

Esperamos que las empresas revelen un compromiso para notificar a los usuarios, cuando sea legalmente posible, en casos en que terceros soliciten información sobre los usuarios. Sin embargo, reconocemos que esta notificación puede no ser posible en casos legítimos de una investigación en curso, pero las empresas deberían explicárselo a los usuarios.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si revelación cumple con todos los elementos de la lista de verificación.

Posibles fuentes:

- Informe de transparencia de la empresa
- Guías de aplicación de la ley de la empresa

P11

Este indicador examina los informes de la empresa sobre solicitudes gubernamentales y de otros terceros que las empresas reciben de información de los usuarios.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos dela lista de verificación.

En algunos casos, la ley puede impedir que una empresa revele información mencionada en los elementos de este indicador. Por ejemplo, esperamos que las empresas publiquen números exactos antes que rangos de números. Reconocemos que las leyes a veces impiden a las empresas hacerlo así, y los investigadores documentarán las situaciones donde se dé este caso. Pero una empresa perderá puntos si no logra cumplir con todos los elementos. Estos representa una situación donde la ley causa que las empresas no sean competitivas, y exhortamos a las empresas a abogar por leyes que les permitan respetar totalmente los derechos de libertad de expresión y privacidad de los usuarios.

Posibles fuentes:

- Informa de transparencia de la empresa

P12

Las empresas pueden tener acceso a enormes cantidades de información personal sobre los usuarios, y deberían tomar las máximas medidas para mantener esta información segura. Esperamos que las empresas revelen información sobre cómo mantienen la información segura para que los usuarios puedan tomar decisiones informadas sobre dónde enviar su información.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación.

Posibles fuentes:

- Políticas de privacidad de la empresa
- Guía de seguridad de la empresa

P13

Este indicador es solamente aplicable a las empresas de internet. Los usuarios confían significativas cantidades de su contenido a servicios en línea. Las empresas deberían permitir a los usuarios que encripten fácilmente esta información y aumentar radicalmente su seguridad. Este indicador se centra en la encriptación de contenido almacenado del usuario, no en encriptación de transmisión de contenido. Por esta razón, el indicador solamente se aplica a empresas de internet.

Evaluación: Este es un indicador con opción única, lo que significa que los investigadores deben elegir solamente una respuesta. Las categorías de respuesta se calificarán en una escala. El puntaje más alto posible se concede a la repuesta #1, y las empresas que la cumplen recibirán crédito total. Las empresas que cumplan con #2 recibirán crédito parcial (porcentaje a ser determinado), y las empresas que cumplan con #3 recibirán un porcentaje menor de crédito. Las empresas que reciban respuesta #4 o respuesta #5 recibirán crédito cero para este indicador.

Posibles fuentes:

- Términos de servicio de la empresa o política de privacidad
- Guía de seguridad de la empresa
- Centro de asistencia de la empresa
- Informes de sostenibilidad de la empresa
- Blog oficial de la empresa y/o comunicados de prensa

P14

Las empresas mantienen cantidades significativas de información del usuario, lo que los convierte en blancos de agentes maliciosos. Esperamos que las empresas ayuden a los usuarios a protegerse contra esas amenazas. Las empresas deben presentar esta guía al público usando un lenguaje claro, lo ideal es que esté acompañada de imágenes visuales, diseñadas para ayudar a los usuarios a entender la naturaleza de las amenazas que pueden enfrentar empresas y usuarios.

Evaluación: Este indicador se califica usando una lista de verificación, lo que significa que las empresas solamente pueden recibir crédito total si su revelación contiene todos los elementos de la lista de verificación.

Posibles fuentes:

- Centro de seguridad de la empresa
- Páginas de ayuda de la empresa o página de asistencia de la comunidad
- Página de configuraciones de cuenta de la empresa
- Blog de la empresa
- Informe de sostenibilidad de la empresa