



Índice de Responsabilidad Corporativa 2019

Indicadores de investigación

Incluye guía y glosario de indicadores

Septiembre de 2018

Este trabajo tiene licencia internacional Creative Commons Attribution 4.0. Para ver una copia de esta licencia, visita <https://creativecommons.org/licenses/by/4.0/>.



Reconocimientos

Los siguientes miembros del equipo de Ranking Digital Rights colaboraron con la preparación y elaboración de la metodología del Índice de Responsabilidad Corporativa 2019:

- Rebecca MacKinnon, directora del proyecto
- Amy Brouillette, jefa de investigación y jefa de redacción
- Laura Reed, analista de investigación y coordinadora
- Andrea Hackl, analista de investigación
- Nathalie Maréchal, becaria de investigación
- Lisa Gutermuth, directora del programa

Para una lista completa del personal del proyecto visita:

<https://rankingdigitalrights.org/who/>

Queremos agradecer a todos los interesados que colaboraron con aportes esenciales sobre las revisiones propuestas a la metodología del Índice 2019.

Acerca de Ranking Digital Rights

Ranking Digital Rights (RDR) es una iniciativa de investigación sin fines de lucro de Open Technology Institute de New America que trabaja con una red internacional de socios para establecer normas globales de cómo las empresas en el sector de la tecnología de la información y la comunicación (TIC) deberían respetar la libertad de expresión y la privacidad.

Para saber más sobre RDR y su Índice de Responsabilidad Corporativa, visita:

www.rankingdigitalrights.org.

Para saber más sobre New America, visita:

<https://www.newamerica.org/>.

Para saber más sobre el Open Technology Institute, visita:

<https://www.newamerica.org/oti/>.

Para ver una lista completa de financistas y socios del proyecto, visita:

<https://rankingdigitalrights.org/who/partners/>.

Índice

Reconocimientos	1
Acerca de Ranking Digital Rights	1
Acerca del Índice de Responsabilidad Corporativa	4
Metodología del Índice	4
Revisiones del Índice 2019	5
Las empresas	5
Proceso de investigación	7
Evaluación y puntuación	8
Metodología del Índice 2019	9
Gobernabilidad	10
G1. Compromiso de la política	10
G2. Gobernabilidad y supervisión de gestión	10
G3. Implementación interna	11
G4. Evaluación del impacto	12
G5. Participación de los interesados	14
G6. Solución	15
Libertad de expresión	17
F1. Acceso a los términos de servicio	17
F2. Cambios a los términos de servicio	18
F3. Procesos para la aplicación de los términos de servicio	18
F4. Datos sobre la aplicación de los términos de servicio	20
F5. Proceso para responder solicitudes de terceros para restringir contenido o cuentas	20
F6. Datos sobre solicitudes gubernamentales para restringir contenido o cuentas	22
F7. Datos sobre solicitudes privadas para restringir contenido o cuentas	23
F8. Notificación al usuario sobre restricción de contenido y cuentas	24
F9. Gestión de red (empresas de telecomunicaciones)	25
F10. Cierre de red (empresas de telecomunicaciones)	26
F11. Política de identidad	27
Privacidad	28
P1. Acceso a políticas de privacidad	28
P2. Cambios a las políticas de privacidad	29
P3. Recopilación de información del usuario	30

P4. Difusión de información del usuario	31
P5. Objetivo de recopilar y difundir información del usuario	33
P6. Retención de información del usuario	33
P7. Control de los usuarios de su propia información de usuario	34
P8. Acceso de los usuarios a su propia información de usuario	36
P9. Recopilación de información del usuario por terceros (empresas internet y del ecosistema móvil)	36
P10. Proceso para responder solicitudes de terceros de información del usuario	37
P11. Datos sobre solicitudes de terceros de información del usuario	39
P12. Notificación al usuario sobre solicitudes de terceros de información del usuario	40
P13. Supervisión de seguridad	41
P14. Tratamiento a las vulnerabilidades de seguridad	41
P15. Filtraciones de datos	42
P16. Encriptación de comunicaciones del usuario y contenido privado (empresas de internet y del ecosistema móvil)	43
P17. Seguridad de las cuentas (empresas de internet y del ecosistema móvil)	44
P18. Información e instrucción a los usuarios sobre posibles riesgos	45
Glosario	46

Acerca del Índice de Responsabilidad Corporativa

Ranking Digital Rights (RDR) elabora un Índice de Responsabilidad Corporativa que clasifica a las mayores empresas de internet, móviles y telecomunicaciones del mundo por sus políticas y prácticas reveladas que afectan la libertad de expresión y la privacidad. El Índice es una herramienta que fija parámetros con la finalidad de exhortar a las empresas a cumplir con los principios internacionales que protegen la libertad de expresión y la privacidad.

Los parámetros que usa el Índice para medir a las empresas se basan en más de una década de trabajo de las comunidades de derechos humanos, privacidad y seguridad. Estos parámetros incluyen los [Principios Rectores de Naciones Unidas sobre Negocios y Derechos Humanos](#), que afirman que así como los Gobiernos tienen el deber de proteger los derechos humanos, las empresas también tienen la responsabilidad de respetar los derechos humanos. El Índice también se basa en los [principios](#) y [pautas de implementación](#) de [Global Network Initiative](#), que aborda las responsabilidades específicas de las empresas de tecnologías de la información y la comunicación hacia la libertad de expresión y la privacidad ante solicitudes gubernamentales de restringir contenido o entregar información del usuario. Además, recurre a un organismo de parámetros y normas globales emergentes en torno a protección de datos, seguridad y acceso a la información. Los datos y análisis elaborados por el Índice informan del trabajo de defensores, legisladores de derechos humanos e inversionistas responsables y las empresas los usan para mejorar sus políticas y prácticas.

Metodología del Índice

El Índice de Responsabilidad Corporativa de RDR se desarrolló a lo largo de tres años de investigación, pruebas, consultas y revisión. Desde sus inicios, el proyecto ha participado de cerca con investigadores en todo el mundo. Para el desarrollo de metodología, estudio piloto e Índice inaugural también nos asociamos con Sustainalytics, importante proveedor de investigación de inversión socialmente responsable (ambiental, social y gobernabilidad) para inversionistas.

En 2015, RDR publicó su Índice inaugural, que [clasificó](#) a 16 empresas de internet y telecomunicaciones.

Para el Índice 2017, RDR amplió su calificación a 22 empresas, que incluían las empresas calificadas en 2015 y agregó otras seis. Además de empresas de internet y telecomunicaciones, el Índice se amplió con nuevos tipos de servicios, incluidos los que elaboran software y dispositivos que llamamos “[ecosistemas móviles](#)”. Como resultado, el equipo de RDR [revisó la metodología de 2017](#) basándose en un resumen detallado de datos sin procesar del Índice de 2015 y también en consultas con interesados de la sociedad civil, el sector académico, la comunidad de inversionistas y las propias empresas.

El [Índice de 2018](#) aplicó la misma metodología para evaluar a las mismas 22 empresas del Índice de 2017. Esto nos permite generar análisis comparativos del desempeño de cada empresa y seguir las tendencias en general.

Revisiones del Índice 2019

El Índice de Responsabilidad Corporativa de Ranking Digital Rights ha sido elaborado como una tabla de posiciones anual, y como tal, RDR sigue elaborando la Metodología del Índice en respuesta a la naturaleza rápidamente cambiante del sector de tecnología.

Por tanto, la Metodología del Índice de 2019 se ha ampliado para abordar la revelación de las empresas de su uso de herramientas automatizadas de toma de decisiones, y también de sus políticas y prácticas de publicidad dirigida. También se revisó la metodología para mejorar nuestra evaluación de los procedimientos de reclamo y solución de las empresas.

Las revisiones se limitan a dos indicadores (G4, G6) con el fin de preservar la comparabilidad año a año. Específicamente, se han agregado dos nuevos elementos (Elementos 5 y 6) al Indicador G4, que califica si las empresas realizan evaluación de riesgos de derechos humanos asociados con sus productos y servicios. Estos nuevos elementos califican si las empresas realizan evaluaciones de riesgos asociadas con su uso de herramientas automatizadas de toma de decisiones (como algoritmos y otra inteligencia artificial), y con respecto a sus políticas y prácticas y publicidad dirigida.

Las revisiones al Indicador G6 tienen el objetivo de fortalecer y aclarar nuestra evaluación de los mecanismos y procedimientos de reclamo y solución de las empresas, y de alinear mejor los parámetros G6 con los articulados en los [Principios Rectores de Naciones Unidas sobre las Empresas y los Derechos Humanos](#).

En julio de 2018, RDR inició un periodo de [consultas públicas](#) para solicitar opinión y comentarios a los interesados sobre estas revisiones propuestas. Los cambios finales a G4 y G6, presentados en este documento, son resultado de esas opiniones y comentarios, y de investigación interna realizada por RDR.

Alentamos a los interesados a leer más sobre la elaboración de nuestra metodología: <https://rankingdigitalrights.org/methodology-development/>

Las empresas

El Índice de Responsabilidad Corporativa 2019 evalúa a 24 empresas, enumeradas debajo. Los investigadores examinarán las políticas y prácticas dominantes de las empresas “matrices”, además de las políticas y prácticas reveladas de los servicios seleccionados o de las empresas que operan localmente (dependiendo de la estructura de las empresas).

Empresas de telecomunicaciones: El Índice de 2019 calificará a 12 empresas de telecomunicaciones, donde hay dos **nuevas** en la calificación de este año (**resaltadas en azul**). Para cada una de estas empresas, evaluamos políticas globales a nivel de grupo para indicadores relevantes, además de los servicios móviles prepago y pospago de la subsidiaria que operan en el país de origen, y el servicio de banda ancha línea fija donde se ofrezca, como

sigue:

- América Móvil (México) — móviles prepago y pospago (Telcel)
- AT&T (Estados Unidos) — móviles prepago y pospago, banda ancha de línea fija
- Axiata (Malasia) — móviles prepago y pospago (Celcom)
- Bharti Airtel (India) — móviles prepago y pospago, banda ancha de línea fija
- [Deutsche Telekom \(Alemania\)](#) — [móviles prepago y pospago, banda ancha de línea fija](#)
- Etisalat (Emiratos Árabes Unidos) — móviles prepago y pospago, banda ancha de línea fija
- MTN (Sudáfrica) — móviles prepago y pospago
- Ooredoo (Qatar) — móviles prepago y pospago, banda ancha de línea fija
- Orange (Francia) — móviles prepago y pospago, banda ancha de línea fija
- Telefónica (España) — móviles prepago y pospago (Movistar), banda ancha de línea fija
- [Telenor \(Noruega\)](#) — [móviles prepago y pospago, banda ancha de línea fija](#)
- Vodafone (Reino Unido) — móviles prepago y pospago, banda ancha de línea fija

Empresas de internet y del ecosistema móvil: El Índice de 2019 evalúa a 12 empresas de internet y del ecosistema móvil. Para el Índice de 2019, ampliamos nuestra evaluación de servicios en la nube para cinco empresas: Google, Mail.Ru, Microsoft, Samsung y Tencent ([resaltadas en azul más abajo](#)). Además, ya no se incluye a Flickr en el Índice de 2019 pues el servicio ya no es propiedad de Oath.¹

Para cada empresa, examinamos hasta cinco servicios, como se señala a continuación:

- Apple (Estados Unidos) — ecosistema móvil iOS, iMessage, iCloud
- Baidu (China) — Baidu Search, Baidu Nube, Baidu PostBar
- Facebook (Estados Unidos) — Facebook, Instagram, WhatsApp, Messenger
- Google (Estados Unidos) — buscador, Gmail, YouTube, ecosistema móvil Android, [Google Drive](#)
- Kakao (Corea del Sur) — Kakao Search, Kakao Mail, KakaoTalk
- Mail.Ru (Rusia) — V Kontakte, correo electrónico Mail.ru, agente de mensajería Mail.ru, [Mail.Ru Nube](#)
- Microsoft (Estados Unidos) — Bing, Outlook.com, Skype, [OneDrive](#)
- Oath (Estados Unidos) — Yahoo Mail, Tumblr
- Samsung (Corea del Sur) — implementación de Android de Samsung, [Samsung Nube](#)
- Tencent (China) — QQZone, QQ, WeChat, [Tencent Nube](#)
- Twitter (Estados Unidos) — Twitter, Periscope
- Yandex (Rusia) — Yandex Mail, Yandex Search, Yandex Disk (almacenamiento en la nube)

Proceso de investigación

El proceso de investigación y evaluación para el Índice de Responsabilidad Corporativa 2019 lo

¹ La empresa SmugMug adquirió Flickr en abril de 2018.

llevará a cabo una red de investigadores globales y el equipo de investigación de RDR. Comprende las siguientes etapas:

- **Etapas 1: Recopilación de datos.** El equipo de investigación principal recopila datos para cada empresa y brinda una evaluación preliminar del desempeño de la empresa en todos los indicadores.
- **Etapas 2: Revisión secundaria.** Un segundo equipo de investigadores lleva a cabo la verificación de datos de las evaluaciones suministradas por los investigadores principales en la Etapa 1.
- **Etapas 3: Revisión y conciliación.** El equipo de RDR examina los resultados de las Etapas 1 y 2, y resuelve cualquier diferencia que pueda surgir.
- **Etapas 4: Primera revisión horizontal.** El equipo de RDR verifica los indicadores para garantizar que hayan sido evaluados sistemáticamente para cada empresa.
- **Etapas 5: Comentarios y opiniones de las empresas.** Los resultados iniciales se envían a las empresas para sus comentarios y opiniones.
- **Etapas 6: Revisión horizontal secundaria.** El equipo de RDR realiza una segunda revisión horizontal, se detiene en los comentarios y opiniones de las empresas reunidos en la Etapa 5, y verifica que los indicadores tengan consistencia y controla la calidad.
- **Etapas 7: Evaluación final.** El equipo de RDR calcula calificaciones finales.

Las empresas recibirán una puntuación acumulativa de su desempeño en todas las categorías del Índice, y los resultados también mostrarán cómo se desempeñaron las empresas por categoría e indicador individuales. Los hallazgos también presentarán tendencias comparativas año a año.

El Índice de 2019 se dará a conocer en mayo de 2019 en un sitio web interactivo y en un informe PDF descargable. Las puntuaciones de las empresas estarán acompañadas de un análisis narrativo sobre los hallazgos y tendencias claves.

Además, las “libretas de calificaciones” de las empresas analizarán el desempeño de cada empresa e incluirán información destacada que ayude a brindar contexto y matices a los resultados. Esa información puede incluir ejemplos específicos de prácticas de la empresa, contexto legal y regulatorio, u otras observaciones formuladas por los investigadores en asuntos que caen fuera de los parámetros de investigación de los indicadores.

Nota sobre contextos nacionales que afectan el desempeño de la empresa: 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 esos factores. En otras palabras, el Índice evalúa a las empresas según sus políticas y prácticas, independientemente de la razón. Sin embargo, los perfiles de narrativa de

cada empresa incluirán un análisis de cómo el ambiente legal, regulatorio y político de la jurisdicción del país de domicilio de la empresa ha afectado su puntuación. En algunos casos, la razón para el buen o mal desempeño de una empresa en un determinado indicador se deberá al ambiente legal, regulatorio o político del país donde domicilia esa empresa. En situaciones donde las leyes y regulaciones causen que las empresas se desempeñen deficientemente, exhortamos a las empresas a abogar por leyes que les permitan respetar plenamente los derechos a la libertad de expresión y la privacidad de sus usuarios, y que den a conocer fuertes compromisos, políticas y prácticas.

Evaluación y puntuación

El ciclo del Índice de 2019 evalúa políticas de empresas activas desde el 14 de enero de 2018 al 25 de enero de 2019. Las empresas reciben una puntuación acumulativa de su desempeño en todas las categorías del Índice, y los resultados muestran cómo se desempeñaron las empresas en cada categoría e indicador. Cada indicador tiene una lista de elementos, y las empresas reciben crédito (pleno, parcial o no reciben crédito) por cada elemento con el que cumplen. La evaluación incluye una evaluación de revelación para cada elemento de cada indicador, basándose en una de estas posibles respuestas:

- “Sí” / revelación total. La revelación de la empresa cumple con el requisito del elemento.
- “Parcial”. La revelación de la empresa ha cumplido con algunos, no con todos los aspectos del elemento, o la revelación no es suficientemente completa para satisfacer el alcance total de lo que pide el elemento.
- “No se encontró revelación alguna”. Los investigadores no pudieron encontrar información brindada por la empresa en su sitio web que responda la pregunta del elemento.
- “No”. Existe revelación de la empresa, pero no revela específicamente a los usuarios lo que el elemento pregunta. Es diferente a la opción “no se encontró revelación alguna”, aunque ninguna aporta crédito.
- “N/A”. No aplicable. Este elemento no se aplica a la empresa o servicio. Los elementos marcados como N/A no se contarán a favor ni en contra de una empresa en el proceso de calificación.

Puntos

- Sí/revelación total = 100
- Parcial = 50
- No = 0
- No se encontró revelación alguna = 0
- N/A se excluye de las puntuaciones y promedios

Metodología del Índice de 2019

El Índice de 2018 califica a 24 empresas con 35 indicadores en tres categorías que miden la revelación de políticas y prácticas que afectan la libertad de expresión y la privacidad de los usuarios.

Cada categoría contiene **indicadores** que miden el desempeño de la empresa en esa categoría. Cada indicador está compuesto de **elementos** que miden el desempeño de la empresa en ese indicador.

Categorías del Índice:

- **Gobernabilidad (G):** esta categoría contiene seis indicadores que miden la revelación de la empresa de los compromisos con los principios de libertad de expresión y privacidad, junto con las medidas tomadas para implementar esos compromisos en las operaciones globales de la empresa.
- **Libertad de expresión (F):** esta categoría contiene 11 indicadores que miden la revelación de la empresa de sus políticas y prácticas que afectan los derechos de libertad de expresión de los usuarios.
- **Privacidad (P):** esta categoría contiene 18 indicadores que miden la revelación de la empresa de sus políticas y prácticas que afectan los derechos de privacidad de los usuarios.

Estas categorías e indicadores están resumidas más abajo. Cada indicador está acompañado de una breve sección “**Guía del indicador**” que describe qué evalúa el indicador.

También se anexa un **Glosario** de términos. Los términos definidos en el Glosario están en **negrita** en el texto del indicador.

Gobernabilidad

Los indicadores en esta categoría buscan evidencia de que la empresa tiene vigentes procesos de gobernabilidad para garantizar que respeta los derechos humanos a la libertad de expresión y la privacidad. Ambos derechos son parte de la [Declaración Universal de Derechos Humanos](#) y están consagrados en el [Pacto Internacional de Derechos Civiles y Políticos](#). Se aplican en línea y fuera de línea. Para que una empresa se desempeñe bien en esta categoría, la revelación de la empresa debe seguir, e idealmente superar, los [Principios Rectores sobre los Negocios y los Derechos Humanos de Naciones Unidas](#) y otros parámetros específicos para el sector de derechos humanos enfocados en libertad de expresión y privacidad, como [Global Network Initiative](#) (Iniciativa de Red Global).

G1. Compromiso de la política

La empresa debe comprometerse públicamente a respetar los derechos humanos a la libertad de expresión y la privacidad de los usuarios.

1. ¿La empresa hace un **compromiso de política explícito**, claramente articulado con los derechos humanos, que incluye la libertad de expresión y la privacidad?

Guía del indicador: Este indicador busca evidencia de que la empresa ha hecho compromisos de políticas explícitos con la libertad de expresión y la privacidad. Este parámetro está resumido en el Principio Operativo 16 de los [Principios Rectores sobre los Negocios y los Derechos Humanos de Naciones Unidas](#), que establece que las empresas deben adoptar públicamente políticas formales de afirmación de sus compromisos con principios y parámetros de derechos humanos internacionales. La empresa debe revelar claramente estos compromisos en documentos de políticas formales u otras comunicaciones que reflejen la política oficial de la empresa. Nótese que este indicador evalúa un compromiso político oficial de la empresa con la libertad de expresión y *también* la privacidad. Estos compromisos deben estar disponibles públicamente. Las empresas con políticas que mencionen solamente uno (ya sea libertad de expresión o privacidad) recibirán crédito parcial.

Posibles fuentes:

- Política de derechos de humanos de la empresa
- Afirmaciones, informes u otras comunicaciones de la empresa que reflejen la política oficial de la empresa
- Informe anual de la empresa o informe de sostenibilidad referido a documentos de la política oficial

G2. Gobernabilidad y supervisión de gestión

El personal directivo de la empresa deberá ejercer **supervisión** sobre cómo sus políticas y prácticas afectan la libertad de expresión y la privacidad.

Elementos:

1. ¿La empresa **revela claramente** que la **junta directiva** ejerce supervisión formal de cómo las prácticas de la empresa afectan la libertad de expresión y la privacidad?
2. ¿La empresa **revela claramente** que un comité de **nivel ejecutivo, equipo, programa o funcionario** supervisa cómo las prácticas de la empresa afectan la libertad de expresión y la privacidad?
3. ¿La empresa **revela claramente** que un comité de **nivel gerencial, equipo, programa o funcionario** supervisa cómo las prácticas de la empresa afectan la libertad de expresión y la privacidad?

Guía del indicador: Este indicador busca evidencia de que las estructuras de gobernabilidad y gestión interna de la empresa incluyen la consideración de la libertad de expresión y la privacidad. Las decisiones que toman los ejecutivos y gerentes de las empresas de internet y telecomunicaciones afectan significativamente la capacidad de las personas de tener libertad de expresión y privacidad. Confiamos en que estos procesos de toma de decisiones y la cadena de responsabilidad dentro de la empresa consideren explícitamente estos derechos humanos.

Para recibir crédito total en este indicador, las empresas deben revelar claramente que en todo nivel de mando (junta directiva, ejecutivo, gerencial) hay supervisión clara de los problemas de libertad de expresión y privacidad. A nivel de la junta directiva, esta supervisión podría incluir un directorio u otra explicación pública de cómo la junta ejerce la supervisión de los compromisos públicos de libertad de expresión y privacidad de la empresa. Por debajo del nivel de la junta directiva, puede incluir una unidad de la empresa o una persona que informe al ejecutivo o nivel gerencial. El comité, programa, equipo, funcionario, etc. debe identificar específicamente libertad de expresión y privacidad en la descripción de sus responsabilidades.

Posibles fuentes:

- Lista de junta de directores
- Documentos de gobernabilidad de la empresa
- Informe de sostenibilidad de la empresa
- Organigrama de la empresa
- Política de derechos humanos de la empresa
- Documentos de Global Network Initiative (si la empresa es miembro)

G3. Implementación interna

La empresa debe tener mecanismos vigentes para implementar sus compromisos con la libertad de expresión y la privacidad dentro de la empresa.

Elementos:

1. ¿La empresa **revela claramente** que brinda capacitación a sus trabajadores sobre asuntos de libertad de expresión y privacidad?

2. ¿La empresa **revela claramente** que mantiene un **programa de informante** a través del cual los trabajadores pueden informar de asuntos relacionados con cómo la empresa trata los derechos de libertad de expresión y privacidad de sus usuarios?

Guía del indicador: El indicador G2 evalúa si el personal directivo de la empresa se compromete a supervisar los asuntos de libertad de expresión y privacidad. Este indicador, G3, evalúa si la empresa revela cómo institucionaliza estos compromisos dentro de la empresa, y si es que los institucionaliza.

Más específicamente, este indicador busca revelar cómo la empresa ayuda a los trabajadores a entender la importancia de la libertad de expresión y la privacidad, y si es que los ayuda. Cuando los trabajadores escriben código informático para un producto nuevo, revisan solicitudes de datos del usuario o responden preguntas sobre cómo usar un servicio, actúan de maneras que pueden afectar directamente la libertad de expresión y la privacidad de los usuarios. Confiamos que las empresas revelen información sobre si ofrecen capacitación que informe a los trabajadores sobre su rol en el respeto a los derechos humanos que dan a los trabajadores un medio para expresar sus preocupaciones con respecto a los derechos humanos.

Una empresa solamente recibe crédito en este indicador si revela claramente información sobre capacitación de sus trabajadores sobre libertad de expresión y privacidad, y si existe un programa de informante que englobe estos asuntos. La revelación debería especificar que la capacitación de los trabajadores y los programas internos de informantes abarcan la libertad de expresión y la privacidad. Las empresas pueden recibir crédito en este indicador, aunque el programa interno de informante de la empresa no mencione específicamente las quejas referidas a la libertad de expresión y la privacidad en la medida que la empresa se haya comprometido de algún modo con estos principios de una manera de deje en claro que la empresa recibiría esos reclamos a través de su programa interno de informante.

Posibles fuentes:

- Código de conducta de la empresa
- Manual de los trabajadores
- Organigrama de la empresa
- Informe de sostenibilidad/responsabilidad corporativa de la empresa
- Publicaciones en el blog de la empresa

G4. Evaluación del impacto

La empresa debe realizar evaluaciones frecuentes, completas y creíbles con debida diligencia, como **evaluaciones de impacto en los derechos humanos**, para identificar cómo todos los aspectos de su actividad afectan la libertad de expresión y la privacidad, y para mitigar cualquier riesgo que esos impactos suponen.

Elementos:

1. Como parte de la toma de decisiones, ¿la empresa considera cómo afectan las leyes la

libertad de expresión y la privacidad en jurisdicciones donde opera?

2. ¿La empresa evalúa frecuentemente los riesgos a la libertad de expresión y privacidad asociados con productos y servicios existentes?
3. ¿La empresa evalúa los riesgos a la libertad de expresión y privacidad asociados con una nueva actividad, incluido el lanzamiento o adquisición de nuevos productos, servicios o empresas o entrada a nuevos mercados?
4. ¿La empresa evalúa los riesgos a la libertad de expresión y la privacidad asociados con los procesos y mecanismos usados para aplicar sus **términos de servicio**?
5. ¿La empresa revela que evalúa riesgos a la libertad de expresión y la privacidad asociados con el uso de **toma de decisiones automatizadas**, como el uso de **algoritmos o inteligencia artificial**?
6. ¿La empresa evalúa los riesgos asociados con la libertad de expresión y la privacidad asociados con las políticas y prácticas de su publicidad dirigida?
7. ¿La empresa realiza evaluaciones adicionales donde las evaluaciones de riesgos de la empresa identifican problemas?
8. ¿Los **altos ejecutivos** o integrantes de la junta de directores de la empresa revisan y toman en consideración los resultados de las evaluaciones con debida diligencia al tomar decisiones?
9. ¿La empresa realiza evaluaciones periódicamente?
10. ¿Las evaluaciones de la empresa están garantizadas por un **tercero externo**?
11. ¿El **tercero externo** que asegura la evaluación está acreditado por una organización creíble según un parámetro de derechos humanos relevante?

Guía del indicador: Las personas enfrentan riesgos de derechos humanos cuando usan herramientas digitales. Las evaluaciones de impacto de derechos humanos son una manera para que las empresas conozcan esos riesgos y sepan abordarlos, o al menos tratar de mitigarlos, sobre todo cuando presenten nuevos productos y servicios o ingresen a nuevos mercados, o cuando incorporen tomas de decisiones automatizadas.

El indicador examina si las empresas revelan la existencia de algún proceso de evaluación de riesgos de derechos humanos, y también cómo las empresas incorporan evaluaciones de consideraciones de libertad de expresión y privacidad en su toma de decisiones, si es que las incorporan. Estas evaluaciones representan un análisis sistemático interno para garantizar que las decisiones y prácticas de una empresa estén en línea con su compromiso (y responsabilidad) de respetar la libertad de expresión y la privacidad. Confiamos en que las empresas revelen que evalúan los riesgos con la libertad de expresión y la privacidad asociados con nuevas actividades, cuando lanzan nuevos productos o entran a nuevos

mercados. También confiamos que las empresas evalúen riesgos asociados con la aplicación de los acuerdos de sus términos de servicio, con el uso de tecnologías automatizada de toma de decisiones (a través del uso de algoritmos o inteligencia artificial), y con sus políticas y prácticas de publicidad dirigida.

Aunque este indicador usa términos de evaluación de impacto de derechos humanos, las empresas pueden usar diferentes nombres para este proceso de revisión. El nombre que las empresas dan a sus procesos es menos importante que lo que el proceso comprende y logra. Este indicador incluirá una revisión de Evaluaciones de Impacto a la Privacidad y otros procesos de evaluación que contienen características o componentes enumerados en este indicador, pero no necesariamente se llaman “evaluaciones de impacto de derechos humanos”.

Nótese que este indicador no espera que las empresas publiquen resultados detallados de sus evaluaciones de impacto en derechos humanos, pues una evaluación minuciosa incluye información delicada. En cambio, confía que las empresas revelen que realizan evaluaciones de riesgos de derechos humanos y que brinden información sobre qué comprende su proceso de evaluación de riesgos de derechos humanos. Si una empresa realiza evaluaciones de riesgos de derechos humanos pero no revela públicamente que realiza esas evaluaciones, la empresa no recibirá crédito.

Posibles fuentes:

- Informes de responsabilidad corporativa/de sostenibilidad de la empresa
- Política de derechos humanos de la empresa
- Documentos regulatorios (por ejemplo, la Comisión Federal de Comercio de Estados Unidos)
- Informes de asesores o acreditadores externos
- Informes de evaluación de Global Network Initiative

G5. Participación de los interesados

La empresa debe **participar** con diversos **interesados** en problemas de libertad de expresión y privacidad.

Elementos:

1. ¿La empresa integra una **iniciativa con múltiples participantes** cuya atención incluye un compromiso de defender la libertad de expresión y la privacidad basándose en los principios internacionales de derechos humanos?
2. Si la empresa no integra una **iniciativa con múltiples participantes**, ¿integra la empresa alguna organización que participa sistemática y frecuentemente con interesados ajenos al sector y no gubernamentales en libertad de expresión y privacidad?
3. Si la empresa no integra una de estas organizaciones, ¿la empresa revela que inicia o participa en reuniones con **interesados** que representan, defienden o son personas

cuya libertad de expresión y privacidad se ven directamente impactadas por los negocios de la empresa?

Guía del indicador: Este indicador busca evidencia de que la empresa participa con interesados —y sobre todo con los que enfrentan riesgos de derechos humanos en relación con sus actividades en línea. Confiamos en que la participación de los interesados sea un componente medular del proceso de elaboración de políticas y la evaluación del impacto de una empresa. La participación de los interesados se debe llevar a cabo en toda la gama de asuntos relativos a la libertad de expresión y privacidad de los usuarios, incluido el proceso para elaborar términos de servicio, políticas de privacidad e identidad de una empresa junto con las prácticas de aplicación de esas políticas.

Puede ser delicado participar con interesados, sobre todo los que operan en ambientes de alto riesgo. Una empresa puede no estar cómoda de tener que revelar detalles específicos sobre qué interesados consulta, dónde o cuándo se encuentran y qué discuten. Aunque alentamos a las empresas a brindar detalles sobre participación no delicada de los interesados, buscamos como mínimo revelación pública de que una empresa participa con interesados que son o representan a usuarios cuyos derechos de libertad de expresión y privacidad estén en riesgo. Una manera en que el público puede saber que una empresa participa en este tipo de participación es a través de su intervención en una iniciativa con muchos interesados que ponga a la empresa en contacto con representantes de diversos grupos de interesados, como organizaciones de derechos humanos y otras que defienden los derechos de grupos en riesgo.

Si una empresa recibe crédito total en el Elemento 1, automáticamente recibirá crédito total en el Elemento 2 y el Elemento 3.

Posibles fuentes:

- Informes de responsabilidad corporativa/ sostenibilidad de la empresa
- Informe anual de la empresa
- Blog de la empresa
- Listas de integrantes de Global Network Initiative y sitios web de Industry Dialogue
- Preguntas frecuentes o centro de ayuda de la empresa

G6. Solución

La empresa debe tener mecanismos de **reclamo y solución** para abordar asuntos de libertad de expresión y privacidad de los usuarios.

Elementos:

1. ¿La empresa **revela claramente** que tiene un **mecanismo de reclamo** que permite que los usuarios presenten sus quejas si sienten que su libertad de expresión o su privacidad se ha visto afectada negativamente por las políticas o prácticas de la empresa?
2. ¿La empresa **revela claramente** sus procedimientos para dar una **solución** a reclamos

relacionados con la libertad de expresión o la privacidad?

3. ¿La empresa **revela claramente** los plazos para sus procedimientos de **reclamo y solución**?
4. ¿La empresa **revela claramente** la cantidad de quejas que recibe relacionadas con la libertad de expresión y la privacidad?
5. ¿La empresa **revela claramente** evidencia de que está resolviendo los reclamos de libertad de expresión y privacidad?

Guía del indicador: Los derechos humanos solamente se pueden proteger y respetar si se compensa a las personas cuando creen que sus derechos han sido violados. Este indicador examina si las empresas brindan esos mecanismos de solución y si han revelado públicamente procesos para responder a reclamos de personas que consideran que la empresa ha violado o facilitado directamente la violación de su libertad de expresión o privacidad.

Confiamos en que las empresas revelen claramente un mecanismo de reclamo que permita a los usuarios hacer llegar sus quejas si sienten que las políticas o prácticas de la empresa han violado su libertad de expresión o su privacidad. Para obtener crédito total en el Elemento 1, el mecanismo de reclamo de una empresa no tiene que afirmar explícitamente que se aplica a quejas relacionadas con la libertad de expresión y la privacidad. Sin embargo, debe quedar claro que este mecanismo se puede usar para presentar cualquier reclamo relacionado con derechos humanos. Confiamos también en que el mecanismo de reclamo de una empresa esté claramente accesible a los usuarios. Además, la empresa también debe explicar su proceso para dar solución a este tipo de quejas, y revelar evidencia de que les da solución. Las empresas deben describir plazos claros para abordar cada etapa de los procesos de reclamo y solución. Estos parámetros están resumidos en el Principio 31 de los Principios Rectores de Naciones Unidas sobre las Empresas y los Derechos Humanos, que establece que las empresas deben publicar procesos de solución claros, accesibles y previsibles.

Posibles fuentes:

- Términos de servicio de la empresa o acuerdos de usuario equivalentes
- Política de contenidos de la empresa
- Políticas de privacidad de la empresa, guías de privacidad o sitio de recursos de privacidad
- Informes de responsabilidad corporativa/sostenibilidad de la empresa
- Centro de ayuda de la empresa o guía del usuario
- Informe de transparencia de la empresa (por la cantidad de quejas recibidas)

Libertad de expresión

Los indicadores en esta categoría buscan evidencia de que la empresa demuestra que respeta el derecho a la libertad de expresión, como está expresado en la [Declaración Universal de Derechos Humanos](#), el [Pacto Internacional de Derechos Civiles y Políticos](#) y otros instrumentos de internacionales de derechos humanos. Las políticas y prácticas reveladas de la empresa demuestran cómo funciona para evitar contribuir con acciones que puedan interferir con este derecho, salvo cuando esas acciones sean lícitas, proporcionadas y con un fin justificable. 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 pedidos gubernamentales y otros, sino también cómo determinan, comunican y aplican reglas privadas y prácticas comerciales que afectan la libertad de expresión de los usuarios.

F1. Acceso a los términos de servicio

La empresa debe ofrecer **términos de servicio** que sean **fáciles de encontrar** y **fáciles de entender**.

Elementos:

1. ¿Los **términos de servicio** de la empresa son **fáciles de encontrar**?
2. ¿Los **términos de servicio** están disponibles en el idioma que habla la mayoría de usuarios de la empresa?
3. ¿Los **términos del servicio** están presentados de **manera comprensible**?

Guía del indicador: Los términos de servicio de una empresa resumen las relaciones entre el usuario y la empresa. Estos términos contienen reglas sobre contenido y actividades prohibidas, y las empresas también pueden tomar acción contra los usuarios por violar las reglas descritas en los términos. Así, confiamos en que las empresas garanticen que los términos sean fáciles de acceder y de entender.

Este indicador evalúa si los usuarios pueden ubicar fácilmente los términos de la empresa. Un documento fácil de encontrar está en la página de inicio de la empresa o servicio, o a uno o dos clics de la página de inicio, o en un lugar lógico donde los usuarios pueden esperar encontrarlos. Los términos también deben estar disponibles en el idioma principal, o idiomas principales, del mercado de operación principal. Además, confiamos en que una empresa tome medidas para ayudar a los usuarios a entender la información que presenta en sus documentos. Esto incluye, sin limitarse, a ofrecer resúmenes, consejos o pautas que expliquen qué significan los términos, usar encabezados de las secciones, tamaño de letra legible u otras características gráficas que ayuden a los usuarios a entender el documento, o escribir los términos con sintaxis legible.

Posibles fuentes:

- Términos de servicio de la empresa, términos de uso, términos y condiciones, etc.

- Políticas de uso de la empresa, pautas comunitarias, reglas, etc. que sean aceptables.

F2. Cambios a los términos de servicio

La empresa debe **revelar claramente** que brinda **notificación y documentación** a los usuarios cuando cambia sus **términos de servicio**.

Elementos:

1. ¿La empresa **revela claramente** que notifica a los usuarios sobre cambios a sus **términos del servicio**?
2. ¿La empresa **revela claramente** cómo notificará directamente a los **usuarios** de los cambios?
3. ¿La empresa **revela claramente** el plazo dentro del cual hará las notificaciones antes de que los cambios entren en vigencia?
4. ¿La empresa conserva un **archivo público o cambia los registros**?

Guía del indicador: Es habitual que las empresas modifiquen sus términos de servicio a medida que su negocio evoluciona. Sin embargo, estos cambios, que pueden incluir reglas sobre contenido y actividades prohibidas, pueden tener un impacto significativo en los derechos de libertad de expresión de los usuarios. Por lo tanto, confiamos en que las empresas se comprometan a notificar a los usuarios cuando modifiquen esos términos y que brinden información a los usuarios que los ayude a entender qué significan esos cambios.

Este indicador busca revelación clara de las empresas del método y plazo para notificar a los usuarios sobre modificaciones a sus términos de servicio. Confiamos en que las empresas se comprometan a notificar directamente a los usuarios antes de que los cambios entren en vigencia. El método de notificación directa puede variar según el tipo de servicio. Para servicios que requieran cuentas de usuario, la notificación directa puede incluir enviar un correo electrónico o un mensaje SMS. Para servicios que no requieran de una cuenta de usuario, la notificación directa puede incluir publicar una notificación destacada en la página principal por donde los usuarios acceden al servicio. Este indicador también busca evidencia de que una empresa brinda registros disponibles públicamente de los términos anteriores, para que las personas puedan entender cómo han evolucionado los términos de la empresa con el tiempo.

Posibles fuentes:

- Términos de servicio de la empresa

F3. Procesos para la aplicación de los términos de servicio

La empresa debe **revelar claramente** las circunstancias bajo las cuales puede restringir **contenido o cuentas de usuario**.

Elementos:

1. ¿La empresa **revela claramente** qué tipo de **contenido** o actividades no permite?
2. ¿La empresa **revela claramente** por qué puede **restringir la cuenta de un usuario**?
3. ¿La empresa **revela claramente** información sobre los procesos que usa para identificar **contenido** o **cuentas** que violen las reglas de la empresa?
4. ¿La empresa **revela claramente** si alguna autoridad estatal recibe consideración prioritaria cuando marca contenido a ser restringido por violar las reglas de la empresa?
5. ¿La empresa **revela claramente** si alguna entidad privada recibe consideración prioritaria cuando marca contenido a ser restringido por violar las reglas de la empresa?
6. ¿La empresa **revela claramente** los procesos para aplicar sus reglas?
7. ¿La empresa brinda ejemplos claros para ayudar al usuario a entender cuáles son las reglas y cómo se aplican?

Guía del indicador: Las empresas pueden fijar reglas sobre qué contenido pueden publicar los usuarios referido a un servicio y también en qué actividades pueden participar los usuarios en ese servicio. Las empresas también pueden restringir la cuenta de un usuario, lo que significa que el usuario no puede acceder al servicio por violar estas reglas. Para ecosistemas móviles, esto puede incluir restricciones al acceso a la cuenta de un usuario final o la cuenta de un programador.

Por lo tanto, confiamos en que las empresas revelen claramente cuáles son esas reglas y cómo las aplican las empresas. Esto incluye información sobre cómo las empresas toman conocimiento de materiales o actividades que violan sus términos. Por ejemplo, las empresas pueden tener personal que revise el contenido o la actividad del usuario, o pueden usar mecanismos de marcas comunitarias que permitan a los usuarios marcar el contenido de otros usuarios o actividad para que la empresa revise. Confiamos también en que las empresas revelen claramente si tienen una política que conceda prioridad o consideración prioritaria a cualquier autoridad estatal o miembros de organizaciones privadas u otras entidades que identifiquen su afiliación organizacional cuando denuncien contenido o usuarios que supuestamente violen las reglas de la empresa. Para ecosistemas móviles, confiamos en que las empresas revelen qué tipos de aplicaciones restringirían. En esta revelación, la empresa también debe dar ejemplos que ayuden a los usuarios a entender qué significan estas reglas.

Posibles fuentes:

- Términos de servicio de la empresa, contrato del usuario
- Política de uso aceptable, parámetros comunitarios, pautas de contenido, política sobre comportamiento abusivo o documento similar de la empresa que explique las reglas que los usuarios deben seguir.
- Asistencia, centro de ayuda o preguntas frecuentes de la empresa (por ejemplo,

preguntas sobre por qué se retira contenido, por qué se suspende una cuenta, etc.)

F4. Datos sobre aplicación de los términos de servicio

La empresa debe **revelar claramente** y publicar con frecuencia datos sobre el volumen y naturaleza de las acciones que toma para restringir contenido o cuentas que violen las reglas de la empresa.

Elementos:

1. ¿La empresa **revela claramente** datos sobre el volumen y naturaleza del contenido y cuentas restringidas por violar las reglas de la empresa?
2. ¿La empresa publica estos datos al menos una vez al año?
3. ¿Los datos que publica la empresa se pueden exportar como un archivo de **datos estructurados**?

Guía del indicador: Las empresas aplican sus términos de servicio por diversas razones, y confiamos en que las empresas revelen públicamente la cantidad de casos en los que toman acciones para restringir las cuentas o servicios de los usuarios. La revelación de estos datos ofrece al público una visión más transparente y precisa del proceso de retiro de contenido y del rol de las empresas en el retiro del contenido.

Este indicador evalúa la revelación de datos de la empresa sobre la cantidad de casos de retiro de contenido o de restricción de acceso de los usuarios por violaciones a los términos de servicio de la empresa. Hacer públicos esos datos brindará al público una visión más precisa del ecosistema de retiro de contenido y del rol de las propias empresas en el retiro de contenido. Las empresas solamente pueden recibir crédito total en este indicador si ofrecen evidencia de que revelan claramente y publican con frecuencia datos sobre sus decisiones de retiro de contenido. Esta información se debe publicar al menos una vez al año en un archivo de datos estructurados.

Posibles fuentes:

- Informe de transparencia de la empresa

F5. Proceso para responder solicitudes de terceros para restringir contenido o cuentas

La empresa debe **revelar claramente** su proceso para responder a **solicitudes gubernamentales** (incluidas órdenes judiciales) y **solicitudes privadas** para retirar, filtrar o restringir **contenido o cuentas**.

Elementos:

1. ¿La empresa **revela claramente** su proceso para responder a **solicitudes**

gubernamentales no judiciales?

2. ¿La empresa **revela claramente** su proceso para responder a **órdenes judiciales**?
3. ¿La empresa **revela claramente** su proceso para responder a **solicitudes gubernamentales** de jurisdicciones extranjeras?
4. ¿La empresa **revela claramente** su proceso para responder a **solicitudes privadas**?
5. ¿Las explicaciones de la empresa **revelan claramente** la base legal bajo la cual pueden cumplir con las **solicitudes gubernamentales**?
6. ¿Las explicaciones de la empresa **revelan claramente** la base legal bajo la cual pueden cumplir con **solicitudes privadas**?
7. ¿La empresa **revela claramente** que actúa con la debida diligencia en las **solicitudes gubernamentales** antes de decidir cómo responder?
8. ¿La empresa **revela claramente** que actúa con la debida diligencia en las **solicitudes privadas** antes de decidir cómo responder?
9. ¿La empresa se compromete a denegar **solicitudes gubernamentales** que sean inapropiadas o excesivas?
10. ¿La empresa se compromete a denegar **solicitudes privadas** que sean inapropiadas o excesivas?
11. ¿La empresa brinda una guía clara o ejemplos de su proceso de respuesta a **solicitudes gubernamentales**?
12. ¿La empresa brinda una guía clara o ejemplos de su proceso de respuesta a **solicitudes privadas**?

Guía del indicador: Las empresas reciben con frecuencia solicitudes para retirar, filtrar o restringir el acceso a contenido y cuentas. Estas solicitudes pueden venir de agencias estatales o juzgados (nacionales y extranjeros) y también de entidades privadas (entidades no estatales y no judiciales). Confiamos en que las empresas revelen públicamente sus procesos para responder a solicitudes gubernamentales y de juzgados, y también solicitudes privadas que vienen a través de algún proceso definido u organizado. Las solicitudes privadas pueden venir a través de un proceso establecido por ley (por ejemplo, solicitudes realizadas al amparo de la Ley de Derechos de Autor de la Era Digital de Estados Unidos, la resolución europea de derecho al olvido, etc.) o un acuerdo autorregulatorio (por ejemplo, acuerdos de la empresa para bloquear algunos tipos de imágenes).

Este indicador evalúa si la empresa revela claramente cómo responde a solicitudes gubernamentales y privadas para retirar, filtrar o restringir contenido o cuentas. La empresa debe revelar las razones legales por las que retiraría contenido. En algunos casos, la ley puede impedir que una empresa revele información mencionada en los elementos de este indicador.

RDR documentará las situaciones en las que esto ocurra, pero una empresa perderá puntos si no cumple con todos los elementos. Esto representa una situación donde la ley causa que las empresas no sean competitivas, y alentamos a las empresas a defender las leyes que les permitan respetar totalmente los derechos de los usuarios a la libertad de expresión y la privacidad.

Posibles fuentes:

- Informe de transparencia de la empresa
- Pautas de aplicación de la ley de la empresa
- Términos de servicio de la empresa
- Centro de ayuda o asistencia de la empresa
- Publicaciones en el blog de la empresa
- Política de la empresa sobre derechos de autor o propiedad intelectual

F6. Datos sobre solicitudes gubernamentales para restringir contenido o cuentas

La empresa debe publicar con frecuencia datos sobre **solicitudes gubernamentales** (incluidas órdenes judiciales) para retirar, filtrar o restringir **contenido o cuentas**.

Elementos:

1. ¿La empresa desagrega por país la cantidad de solicitudes que recibe?
2. ¿La empresa hace una lista de la cantidad de **cuentas** afectadas?
3. ¿La empresa hace una lista de la cantidad de **contenido** o URL afectados?
4. ¿La empresa hace una lista de los asuntos asociados con las solicitudes que recibe?
5. ¿La empresa hace una lista de la cantidad de solicitudes que vienen de diferentes autoridades legales?
6. ¿La empresa hace una lista de la cantidad de solicitudes que recibe a sabiendas de funcionarios del Gobierno para restringir **contenido o cuentas** a través de procesos no oficiales?
7. ¿La empresa hace una lista de la cantidad de solicitudes que acató?
8. ¿La empresa publica las solicitudes originales o revela que suministra copias al **archivo público de un tercero**?
9. ¿La empresa informa de estos datos al menos una vez al año?
10. ¿Los datos se pueden exportar como un archivo de **datos estructurados**?

Guía del indicador: Las empresas reciben con frecuencia solicitudes de Gobiernos de retirar,

filtrar o restringir contenido o cuentas. Confiamos en que una empresa publique con frecuencia datos sobre la cantidad y tipo de solicitudes gubernamentales que recibe, y con cuántas solicitudes cumple. Las empresas pueden recibir estas solicitudes a través de procesos oficiales, como una orden judicial, a través de canales informales, o a través del sistema de marcas para permitir que los privados denuncien contenido que viole los términos del servicio. Las empresas deben ser transparentes sobre la naturaleza de estas solicitudes. Si una empresa sabe que una solicitud viene de una entidad estatal o juzgado, la empresa debe revelarlo como parte de sus informes de solicitudes gubernamentales. Revelar estos datos ayuda al público a entender mejor las relaciones entre empresas y Gobiernos en la vigilancia de contenido en línea, y ayuda al público a pedir que empresas y Gobiernos respondan por sus obligaciones de respetar y proteger los derechos de libertad de expresión.

En algunos casos, la ley puede impedir que una empresa revele información mencionada en los elementos de este indicador. Por ejemplo, confiamos en que las empresas publiquen números exactos en vez de rangos de números. Reconocemos que, a veces, las leyes impiden que las empresas lo hagan así, y los investigadores documentarán las situaciones en que ese sea el caso. Pero una empresa perderá puntos si no cumple con los parámetros especificados en todos los elementos mencionados arriba. Esto representa una situación en la que, por causa de la ley, las empresas no cumplen con las mejores prácticas, y alentamos 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

F7. Datos sobre solicitudes privadas para restringir contenido o cuentas

La empresa debe publicar con frecuencia datos sobre **solicitudes privadas** para retirar, filtrar o restringir acceso a **contenido** o **cuentas**.

Elementos:

1. ¿La empresa desagrega por país la cantidad de solicitudes que recibe?
2. ¿La empresa hace una lista de la cantidad de **cuentas** afectadas?
3. ¿La empresa hace una lista de la cantidad de **contenido** o URL afectados?
4. ¿La empresa hace una lista de las razones para retirar contenido asociadas con las solicitudes que recibe?
5. ¿La empresa describe los grupos de los que reciben solicitudes?
6. ¿La empresa hace una lista de la cantidad de solicitudes que cumplió?
7. ¿La empresa publica las solicitudes originales o revela que brinda copias al **archivo público de un tercero**?

8. ¿La empresa informa de estos datos al menos una vez al año?
9. ¿Los datos se pueden exportar como un archivo de **datos estructurados**?
10. ¿La empresa **revela claramente** que sus informes abarcan todos los tipos de **solicitudes privadas** que recibe?

Guía del indicador: Las empresas reciben con frecuencia solicitudes de parte a través de procesos privados (no gubernamentales o no judiciales) para retirar, filtrar o restringir contenido o cuentas. Confiamos en que las empresas publiquen con frecuencia datos sobre la cantidad y tipo de solicitudes recibidas a través de procesos privados, y la cantidad de esas solicitudes que cumple. Este indicador se centra en solicitudes que vienen de algún proceso definido u organizado. Esto se puede establecer por ley (por ejemplo, solicitudes realizadas bajo la Ley de Derechos de Autor de la Era Digital, la resolución europea de derecho al olvido, etc.) un acuerdo autorregulatorio (por ejemplo, acuerdos de la empresa para bloquear algunos tipos de imágenes). Este indicador no examina los informes de la empresa sobre contenido o cuentas restringidos bajo mecanismos de aplicación de los términos de servicio. Eso se evalúa en el indicador F4.

Posibles fuentes:

- Informe de transparencia de la empresa

F8. Notificación al usuario sobre restricción de contenido y cuentas

La empresa debe **revelar claramente** que **notifica a los usuarios** cuando restringe **contenido o cuentas**.

Elementos:

1. Si la empresa aloja **contenido** generado por el usuario, ¿la empresa **revela claramente** que notifica a los **usuarios** que generaron el **contenido** cuando lo restringen?
2. ¿La empresa **revela claramente** que notifica a los usuarios que intentan acceder a **contenido** que ha sido restringido?
3. En su notificación, ¿la empresa **revela claramente** una razón para la restricción del **contenido** (legal u otra)?
4. ¿La empresa **revela claramente** que notifica a los usuarios cuando restringe su **cuenta**?

Guía del indicador: El indicador F3 analiza la revelación de la empresa de las restricciones a lo que los usuarios pueden publicar o hacer en un servicio. El indicador F8 se centra en si una empresa revela claramente que notifica a los usuarios cuando toma acciones de este tipo (ya sea por aplicación de los términos de servicio o por solicitudes de restricción de terceros). La decisión de una empresa de restringir o retirar el acceso a contenido o cuentas puede tener un impacto significativo en el derecho a la libertad de expresión y acceso a la información de los

usuarios. Por lo tanto, confiamos que una empresa revele que notifica a sus usuarios cuando retire contenido, restrinja la cuenta de un usuario o restrinja de otra manera la capacidad de los usuarios de acceder a un servicio. Si una empresa retira contenido que un usuario ha publicado, confiamos en que la empresa informe a ese usuario sobre la decisión. Si otro usuario intenta acceder a acceso contenido que la empresa ha restringido, confiamos en que la empresa notifique a ese usuario sobre la restricción de contenido. También confiamos en que las empresas especifiquen las razones de sus decisiones. Esta revelación debe ser parte de las explicaciones de las empresas de sus prácticas de restricción de acceso y contenido.

Posibles fuentes:

- Términos de servicio de la empresa, política de uso aceptable, parámetros comunitarios, pautas de contenido, política sobre comportamiento abusivo o documento similar de la empresa que explique las reglas que los usuarios deben seguir.
- Página de asistencia, centro de ayuda o preguntas frecuentes de la empresa (por ejemplo, preguntas sobre por qué se retira contenido, por qué se suspende una cuenta, etc.)
- Pautas de la empresa para programadores
- Política de derechos humanos de la empresa

F9. Gestión de red (empresas de telecomunicaciones)

La empresa debe **revelar claramente** que no **prioriza**, bloquea ni retrasa algunos tipos de tráfico, **aplicaciones**, **protocolos** o **contenido** por ninguna razón más allá de asegurar la calidad del servicio y la confiabilidad de la red.

Elementos:

1. ¿La empresa **revela claramente** que no **prioriza**, bloquea ni retrasa algunos tipos de tráfico, **aplicaciones**, **protocolos** o **contenido** por razones más allá de asegurar la calidad del servicio y la confiabilidad de la red?
2. Si la empresa interviene en estas prácticas, ¿**revela claramente** sus motivos?

Guía del indicador: Este indicador evalúa si las empresas de telecomunicaciones revelan claramente si emprenden prácticas que afectan el flujo de contenido a través de sus redes, como **ahogar** o **dar forma al tráfico**. Confiamos en que estas empresas se comprometan públicamente a evitar dar prioridad o degradar contenido. En algunos casos, una empresa puede intervenir en prácticas legítimas de dar forma al tráfico para garantizar el flujo de tráfico a través de sus redes. Confiamos en que la empresa revele esto públicamente y que explique con qué finalidad lo hace. Nótese que este indicador no aborda el bloqueo de contenido. Eso está contemplado en el indicador F3. Sin embargo, este indicador incluye revelación de la empresa relativa al bloqueo de servicios, aplicaciones o dispositivos, que se consideran una forma de priorización.

Posibles fuentes:

- Explicación de la gestión de redes o prácticas de gestión de redes de la empresa

F10. Cierre de red (empresas de telecomunicaciones)

La empresa debe explicar claramente las circunstancias bajo las que puede **cerrar o restringir el acceso a la red** o a **protocolos**, servicios o **aplicaciones** específicos en la red.

Elementos:

1. ¿La empresa explica claramente la razón o razones por las que puede cerrar el servicio a una zona particular o a un grupo de usuarios?
2. ¿La empresa explica claramente por qué puede restringir el acceso a aplicaciones o protocolos específicos (por ejemplo, VoIP, mensajería) en una zona particular o a un grupo específico de usuarios?
3. ¿La empresa explica claramente su proceso para responder solicitudes de **cierre de una red** o restringir el acceso a un servicio?
4. ¿La empresa se compromete a denegar solicitudes de **cierre de una red o restringir el acceso a un servicio**?
5. ¿La empresa **revela claramente** que notifica a los usuarios directamente cuando **cierra la red o restringe el acceso a un servicio**?
6. ¿La empresa enumera la cantidad de solicitudes de **cierre de red** que recibe?
7. ¿La empresa identifica claramente la autoridad legal específica que formula la solicitud?
8. ¿La empresa enumera la cantidad de solicitudes que ha cumplido?

Guía del indicador: Los cierres de red son una creciente amenaza a los derechos humanos. El [Consejo de Derechos Humanos de Naciones Unidas](#) ha condenado los cierres de redes como una violación del derecho internacional de derechos humanos y ha pedido a los Gobiernos que se abstengan de tomar esas acciones. No obstante, los Gobiernos [ordenan cada vez más](#) a las empresas de telecomunicaciones que cierren sus redes, que a su vez ejerce presión sobre las empresas para que tomen acciones que violan su responsabilidad de respetar los derechos humanos. Confiamos en que las empresas revelen totalmente las circunstancias por las que puede tomar esa acción y que denuncien las denuncias que reciben para tomar esas acciones.

Posibles fuentes:

- Términos del servicio de la empresa, política de uso aceptable, parámetros comunitarios, pautas de contenido, política sobre comportamiento abusivo o documento similar de la empresa que explique las reglas que los usuarios deben seguir.
- Informe de transparencia de la empresa

- Pautas de aplicación de la ley de la empresa

F11. Política de identidad

La empresa no debe **solicitar** a los usuarios que confirmen su identidad con su **identificación oficial** ni otras formas de identificación que pueden estar conectadas con su identidad fuera de línea.

1. ¿La empresa **solicita** a los usuarios que confirmen su identidad con su **identificación oficial**, o con otras formas de identificación que pueden estar conectadas con su identidad fuera de línea?

Guía del indicador: La capacidad de comunicarse anónimamente es esencial para la libertad de expresión en línea y fuera de línea. Usar el nombre verdadero en línea o pedir a los usuarios que proporcionen a la empresa información que los pueda identificar facilita un vínculo entre actividades en línea y una persona específica. Esto presenta riesgos a los derechos humanos para quienes, por ejemplo, expresan opiniones que no son iguales a las opiniones de un Gobierno o que participan en activismo que un Gobierno no permite. También presenta riesgos para las personas perseguidas por creencias religiosas u orientación sexual.

Por lo tanto, confiamos en que las empresas revelen si piden a los usuarios que verifiquen su identidad con sus identificaciones oficiales u otras formas de identificación que pueden estar conectadas con su identidad fuera de línea. Reconocemos que los usuarios pueden haber brindado información que podría estar conectada con su identidad fuera de línea para acceder a características pagadas de diversos productos y servicios. Sin embargo, los usuarios deben poder acceder a características que no requieren pago sin tener que brindar información que se pueda relacionar con su identidad fuera de línea.

Este indicador se aplica a empresas de internet, empresas del ecosistema móvil y servicios móviles prepago (para empresas de telecomunicaciones).

Posibles fuentes:

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

Privacidad

Los indicadores esta categoría buscan evidencia de que, en sus políticas y prácticas reveladas, la empresa demuestra maneras concretas en que respeta el derecho a la privacidad de usuarios, como lo expresa la [Declaración Universal de Derechos Humanos](#), el [Pacto Internacional de Derechos Civiles y Políticos](#) y otros instrumentos internacionales de derechos humanos. Las políticas y prácticas reveladas de la empresa demuestran cómo funcionan para evitar colaborar con acciones que puedan interferir con la privacidad de los usuarios, salvo cuando esas acciones sean legítimas, proporcionadas y con un objetivo justificable. También demostrarán un fuerte compromiso para proteger y defender la seguridad digital de los usuarios. Las empresas que se desempeñan bien en estos indicadores demuestran un fuerte compromiso público con la transparencia, no solamente en términos de cómo responden a los pedidos gubernamentales y de otros, sino también cómo determinan, comunican y aplican reglas privadas y prácticas comerciales que afectan la privacidad de los usuarios.

P1. Acceso a políticas de privacidad

La empresa debe brindar **políticas de privacidad** que sean **fáciles de encontrar** y **fáciles de entender**.

Elementos:

1. ¿Las políticas de privacidad de la empresa son **fáciles de encontrar**?
2. ¿Las políticas de privacidad están disponibles en el idioma más hablado por los usuarios de la empresa?
3. ¿Las políticas están presentadas de **manera comprensible**?
4. (Para **ecosistemas móviles**): ¿La empresa revela que se necesitan aplicaciones disponibles en su **tienda de aplicaciones** para brindar a los usuarios una política de privacidad?

Guía del indicador: Las políticas de privacidad abordan cómo las empresas reúnen, gestionan, usan y garantizan la información sobre los usuarios y también información proporcionada por los usuarios. Así, las empresas deben garantizar que los usuarios puedan ubicar fácilmente la política y hacer un esfuerzo para ayudar a que los usuarios entiendan qué significan.

Este indicador confía que las empresas brinden políticas de privacidad que sean fáciles de encontrar, que estén disponibles en los idiomas de los principales mercados en los que opera la empresa y que garanticen que las políticas sean fáciles de entender. Si la empresa ofrece múltiples productos y servicios, debe quedar muy claro a qué productos y servicios se aplican las políticas.

Un documento que sea “fácil de encontrar” debe estar en la página de inicio de la empresa o

servicio, a uno o dos clics de la página de inicio, o en un lugar lógico donde es probable que los usuarios lo encuentren. Los términos también deben estar disponibles en el principal idioma, o idiomas, del mercado de operación principal. Además, confiamos en que una empresa tome medidas para ayudar a los usuarios a entender la información que presentan en sus documentos. Esto incluye, sin limitarse, a ofrecer resúmenes, consejos o pautas que expliquen qué significan los términos, usar encabezados de las secciones, tamaño de letra legible u otras características gráficas que ayuden a los usuarios a entender el documento o escribir los términos con sintaxis legible. Los términos de servicio no están incluidos en este indicador pues están en indicadores separados en la categoría “Libertad de Expresión”.

Posibles fuentes:

- Política de privacidad de la empresa
- Política de uso de datos de la empresa

P2. Cambios a las políticas de privacidad

La empresa debe **revelar claramente** que brinda **avisos y documentación** a los usuarios cuando modifica sus **políticas de privacidad**.

Elementos:

1. ¿La empresa **revela claramente** que notifica a los usuarios sobre cambios a sus políticas de privacidad?
2. ¿La empresa **revela claramente** cómo notificará directamente de los cambios a los usuarios?
3. ¿La empresa **revela claramente** el plazo en el cual notifica antes de que los cambios surtan efecto?
4. ¿La empresa conserva un **archivo público o cambia el registro**?
5. (Para **ecosistemas móviles**): ¿La empresa revela que se necesitan aplicaciones disponibles en su **tienda de aplicaciones** para brindar a los usuarios una política de privacidad?

Guía del indicador: Con frecuencia, las empresas cambian sus políticas de privacidad a medida que su negocio evoluciona. Sin embargo, estos cambios pueden afectar la privacidad de los usuarios si se modifica qué información del usuario las empresas pueden recopilar, compartir y almacenar. Por lo tanto, confiamos en que las empresas se comprometan a notificar a los usuarios cuando modifiquen esas políticas y brindar a los usuarios información que les ayude a entender qué significan estos cambios.

Este indicador busca que las empresas revelen claramente su método y plazo para notificar los cambios a las políticas de privacidad. Confiamos en que las empresas se comprometan a notificar directamente a los usuarios antes de que los cambios entren en vigencia. El método de

notificación directa puede variar según el tipo de servicio. Para servicios que requieran cuentas de usuario, la notificación directa puede incluir enviar un correo electrónico o un mensaje SMS. Para servicios que no requieran de una cuenta de usuario, la notificación directa puede incluir la publicación de una notificación destacada en la página web principal o plataforma por donde los usuarios acceden al servicio. Este indicador también busca evidencia de que una empresa brinda registros disponibles públicamente de los términos anteriores, para que las personas pueden entender cómo han evolucionado los términos de la empresa con el tiempo.

Posibles fuentes:

- Política de privacidad de la empresa
- Política de uso de datos de la empresa

P3. Recopilación de información del usuario

La empresa debe **revelar claramente** qué **información del usuario** **recopila** y cómo.

Elementos:

1. ¿La empresa **revela claramente** qué tipo de información del usuario **recopila**?
2. Para cada tipo de **información del usuario** que la empresa **recopila**, ¿la empresa **revela claramente** cómo recopila esa información del usuario?
3. ¿La empresa **revela claramente** que limita la recopilación de **información del usuario** a lo que es directamente relevante y necesario para lograr el objetivo de su servicio?
4. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad** de **aplicaciones** de terceros disponibles a través de su **tienda de aplicaciones** dan a conocer qué **información del usuario** recopilan las aplicaciones?
5. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las **aplicaciones** de terceros disponibles a través de su **tienda de aplicaciones** limitan la recopilación de **información del usuario** a lo que es directamente relevante y necesario para lograr el objetivo de la aplicación?

Guía del indicador: Las empresas recopilan gran variedad de información personal de los usuarios —desde detalles personales y perfiles de cuenta a las actividades y ubicación de un usuario. Confiamos en que las empresas revelen claramente qué información del usuario (*como la define RDR, más abajo*) recopilan y cómo la recopilan. Confiamos también en que las empresas se comprometan con el principio de **minimización de datos** y demostrar cómo este principio da forma a sus prácticas con respecto a información del usuario. Si las empresas recopilan varios tipos de información, confiamos que brinden detalles de cómo manejan cada tipo de información. Para ecosistemas móviles, confiamos en que la empresa revele claramente si las políticas de privacidad de las aplicaciones disponibles en su tienda de aplicaciones especifican qué información del usuario recopila la aplicación y si es que esas políticas

cumplen con los principios de minimización de datos.

RDR hace una interpretación amplia de “**información del usuario**” que, según nuestra definición, constituye “todo dato relacionado con una persona identificable, o que se puede vincular a esa persona si se combinan conjuntos de datos o se utilizan técnicas de minería de datos”.

Como explicación adicional, **información del usuario** es toda la información que documente las características o actividades del usuario. Esta información puede o no estar vinculada a la cuenta de un usuario específico. Esta información incluye, sin limitarse a, correspondencia personal, contenido generado por el usuario, preferencias y configuración de la cuenta, datos de registro y acceso, datos sobre las actividades o preferencias del usuario recopiladas a partir de información de terceros, ya sea a través de seguimiento del comportamiento o de adquisición de datos, y todas las formas de metadatos. La información del usuario nunca se considera anónima, salvo que esté incluida únicamente como una base para generar medidas globales (por ejemplo, cantidad de usuarios activos por mes). Por ejemplo, la afirmación: ‘Nuestro servicio tiene un millón de usuarios activos por mes’ contiene datos anónimos, pues no brinda suficiente información para saber quiénes son ese millón de usuarios.

Datos anónimos son “datos que de ninguna manera están relacionados con otra información que permitiría que se identificara a un usuario”.

Esta visión amplia es necesaria para reflejar varios hechos. Primero, los analistas capacitados pueden “desanonimizar” grandes conjuntos de datos. Esto hace que casi sea imposible cumplir las promesas de anonimización. En esencia, todos los datos vinculados con un “identificador anónimo” no son anónimos. Más bien, a menudo son datos pseudónimos que pueden estar vinculados con la identidad fuera de línea del usuario. Segundo, los metadatos pueden revelar más de las asociaciones e intereses de un usuario que los datos de contenido, por lo que estos datos son de vital interés. Tercero, las entidades que tienen acceso a muchas fuentes de datos, como intermediarios de datos y Gobiernos, pueden agrupar dos o más fuentes de datos para revelar información sobre los usuarios. Así, los actores sofisticados pueden usar datos que parecen anónimos para construir una mayor imagen de un usuario.

En algunos casos, las leyes o regulaciones pueden solicitar que las empresas recopilen alguna información o pueden prohibir o disuadir a la empresa de revelar qué información del usuario recopila. Los investigadores documentarán situaciones en las que sea el caso, pero una empresa perderá puntos si no logra cumplir con todos los elementos. Esto representa una situación en que la ley cause 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 la privacidad.

Posibles fuentes:

- Política de privacidad de la empresa
- Página web de la empresa o sección sobre protección de datos o recopilación de datos

P4. Difusión de información del usuario

La empresa debe **revelar claramente** qué **información del usuario difunde** y con quién.

Elementos:

1. Para cada tipo de **información del usuario** que la empresa recopila, ¿la empresa **revela claramente** si difunde esa información del usuario?
2. Para cada tipo de **información del usuario** que la empresa difunde o comparte, ¿la empresa **revela claramente** con qué tipo de **terceros** difunde o comparte esa información del usuario?
3. ¿La empresa **revela claramente** que puede difundir o o compartir información del usuario con el Gobierno o autoridades legales?
4. Para cada tipo de **información del usuario** que la empresa difunde o o comparte, ¿la empresa **revela claramente** los nombres de todos los **terceros** con quienes difunde o comparte la información del usuario?
5. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad de aplicaciones** de terceros disponibles a través de su **tienda de aplicaciones** revelan qué información del usuario difunden o comparten las aplicaciones?
6. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las **políticas de privacidad de aplicaciones** de terceros disponibles a través de su **tienda de aplicaciones** revelan el tipo de terceros a los que difunde o comparte la información del usuario?

Guía del indicador: Las empresas recopilan una gran variedad de nuestra información personal —desde nuestros detalles personales y perfiles de cuentas a nuestras actividades de navegación y ubicación. Las empresas a menudo difunden o comparten esta información con terceros, incluidos anunciantes, Gobiernos y autoridades legales. Confiamos en que las empresas revelen claramente qué información del usuario (tal como lo define RDR) difunde o comparte y con quién. Las empresas deben especificar si difunden o comparten información del usuario a Gobiernos y entidades comerciales. Para ecosistemas móviles, confiamos en que las empresas revelen claramente si las políticas de privacidad de las aplicaciones disponibles en su tienda de aplicaciones especifican qué información del usuario difunden o comparten con las aplicaciones a terceros.

En algunos casos, las leyes o regulaciones pueden solicitar a las empresas difundir o compartir alguna información o pueden prohibir o desalentar a la empresa revele qué información del usuario difunde o comparte. Los investigadores documentarán situaciones donde este sea el caso, pero una empresa perderá puntos si no cumple con todos los elementos. Esto representa una situación donde la ley genera que las empresas no sean competitivas, y exhortamos a las empresas a proponer leyes que les permitan respetar plenamente los derechos de los usuarios

a la libertad de expresión y la privacidad.

Posibles fuentes:

- Política de privacidad de la empresa
- Política de la empresa relacionadas con la difusión de datos, interacción con terceros

P5. Objetivo de recopilar y difundir información del usuario

La empresa debe **revelar claramente** por qué **recopila y difunde información del usuario**.

Elementos:

1. Para cada tipo de **información del usuario** que la empresa recopila, ¿la empresa **revela claramente** el objetivo de la recopilación?
2. ¿La empresa **revela claramente** si combina **información del usuario** de diversos servicios de la empresa y por qué?
3. Para cada tipo de **información del usuario** que la empresa difunde o comparte, ¿la empresa **revela claramente** el objetivo de la difusión?
4. ¿La empresa **revela claramente** que limita el uso de **información del usuario** al objetivo por el que la recopiló?

Guía del indicador: Confiamos en que las empresas revelen claramente el objetivo de recopilar y difundir cada tipo de información del usuario que recopile y difunda. Además, muchas empresas tienen u operan diversos productos y servicios, y confiamos en que las empresas revelen claramente cómo se puede difundir o compartir la información del usuario a través de los servicios. Finalmente, las empresas deben comprometerse públicamente con el principio de limitación de uso, que es parte de las pautas de privacidad de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), entre otros marcos de trabajo.

Posibles fuentes:

- Política de privacidad de la empresa
- Página web de la empresa o sección sobre protección de datos o recopilación de datos

P6. Retención de información del usuario

La empresa debe **revelar claramente** cuánto tiempo **retiene información del usuario**.

Elementos:

1. Para cada tipo de **información del usuario** que la empresa recopila, ¿la empresa **revela claramente** cuánto tiempo **retiene** esa información del usuario?
2. ¿La empresa **revela claramente** qué **información sin identificación del usuario**

retiene?

3. ¿La empresa **revela claramente** el proceso para **retirar la identificación a la información del usuario**?
4. ¿La empresa **revela claramente** que elimina toda la **información del usuario** después de que los usuarios cancelan sus cuentas?
5. ¿La empresa **revela claramente** el periodo en el que eliminará la **información del usuario** después de que los usuarios cancelan sus cuentas?
6. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las políticas de privacidad de **aplicaciones** de terceros disponibles a través de su **tienda de aplicaciones** revelan cuánto tiempo retienen información del usuario?
7. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las políticas de privacidad de las **aplicaciones** de terceros disponibles a través de su **tienda de aplicaciones** declaran que se elimina toda la información del usuario cuando los usuarios cancelan sus cuentas o eliminan la aplicación?

Guía del indicador: De la misma manera que confiamos en que las empresas revelen qué información nuestra recopilan y difunden, también confiamos en que las empresas revelen claramente cuánto tiempo la retienen y hasta qué grado eliminan identificadores de la información del usuario que almacenan. Además, los usuarios también deberían poder entender qué ocurre con su información cuando cancelan sus cuentas. En algunos casos, las leyes o regulaciones pueden solicitar a las empresas que retengan alguna información por un periodo determinado. En estos casos, las empresas deben revelar claramente estas regulaciones a los usuarios. Las empresas que eligen retener información del usuario por periodos extendidos también deben tomar medidas para garantizar que los datos no estén vinculados a un usuario específico. Reconociendo los debates actuales sobre la eficacia de los procesos de “desidentificación” y la creciente sofisticación en torno a prácticas de “reidentificación”, consideramos que retirar elementos de identificación es una medida positiva que pueden tomar las empresas para proteger la privacidad de sus usuarios.

Además, si las empresas recopilan múltiples tipos de información, confiamos en que revelen claramente cuánto tiempo retienen *cada tipo de información*. Para ecosistemas móviles, confiamos en que las empresas revelen si las políticas de privacidad de las aplicaciones que están disponibles en su tienda de aplicaciones indican cuánto tiempo retienen la aplicación información del usuario y si eliminan toda la información del usuario si los usuarios cancelan o eliminan la aplicación.

Posibles fuentes:

- Política de privacidad de la empresa
- Página web de la empresa o sección sobre protección de datos o recopilación de datos

P7. Control del usuario de su propia información de usuario

La empresa debe **revela claramente** a los usuarios qué **opciones tienen para controlar** la **recopilación, retención** y uso que hace la empresa de su información de usuario.

Elementos:

1. Para cada tipo de **información del usuario** que la empresa recopila, ¿la empresa **revela claramente** si los usuarios pueden controlar la recopilación de la empresa de esta información del usuario?
2. Para cada tipo de **información del usuario** que la empresa recopila, ¿la empresa **revela claramente** si los usuarios pueden eliminar esta información del usuario?
3. ¿La empresa **revela claramente** que ofrece a los usuarios **opciones para controlar** cómo se usa la información del usuario para publicidad dirigida?
4. ¿La empresa **revela claramente** que la publicidad dirigida está inhabilitada por defecto?
5. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que ofrece a los usuarios opciones para controlar las funciones de **geolocalización** del dispositivo?

Guía del indicador: Confiamos en que las empresas revelen claramente qué opciones tienen los usuarios de controlar la información que las empresas recopilan y retienen sobre ellos. Permitir que los usuarios controlen qué información suya recopila y retiene una empresa implicaría dar a los usuarios la capacidad de borrar tipos específicos de información del usuario sin que tengan que eliminar toda su cuenta. Por lo tanto, confiamos en que las empresas revelen claramente si los usuarios tienen la opción de eliminar tipos específicos de información del usuario.

Además, confiamos en que las empresas permitan que los usuarios controlen el uso de su información con los fines de la publicidad dirigida. La publicidad dirigida requiere gran recopilación y retención de información del usuario, que es fundamental para rastrear. Por tanto, las empresas deben revelar claramente si los usuarios tienen la opción de controlar cómo se usa su información para estos fines.

Para ecosistemas móviles, confiamos en que las empresas revelen claramente qué opciones tienen los usuarios para controlar la recopilación de información de su ubicación. La ubicación de un usuario cambia frecuentemente, y muchos usuarios llevan sus dispositivos móviles casi a todas partes, con lo que la recopilación de este tipo de información se vuelve particularmente delicada. Además, las configuraciones de ubicación en los ecosistemas móviles pueden influir en cómo otros productos y servicios acceden a información de su ubicación. Por ejemplo, las aplicaciones móviles pueden permitir que los usuarios controlen la información de la ubicación. Sin embargo, si el dispositivo en donde funcionan esas aplicaciones móviles recopila datos de geolocalización por defecto y no brinda a los usuarios manera de desactivarlo, es posible que los usuarios no puedan limitar esa recopilación de información de su ubicación que hace esa

aplicación móvil. Por estas razones, confiamos en que las empresas revelen que los usuarios puedan controlar cómo su dispositivo interactúa con la información de su ubicación.

Posibles fuentes:

- Política de privacidad de la empresa
- Página de configuración de cuenta de la empresa

P8. Acceso de los usuarios a su propia información de usuario

Las empresas deben permitir que los usuarios obtengan toda su **información de usuario** que tiene la empresa.

Elementos:

1. ¿La empresa **revela claramente** que los usuarios pueden obtener una copia de su **información de usuario**?
2. ¿La empresa **revela claramente** qué **información del usuario** pueden obtener los usuarios?
3. ¿La empresa **revela claramente** que los usuarios pueden obtener su **información de usuario** en un formato de **datos estructurados**?
4. ¿La empresa **revela claramente** que los usuarios pueden obtener toda la **información del usuario** que el público ve y toda la información privada que una empresa tiene del usuario?
5. (Para **ecosistemas móviles**): ¿La empresa **revela claramente** que evalúa si las políticas de privacidad de **aplicaciones** de terceros disponibles a través de su **tienda de aplicaciones** revelan que los usuarios pueden obtener toda la **información del usuario** que tiene la aplicación?

Guía del indicador: Los usuarios deberían poder obtener toda la información suya que tienen las empresas. Confiamos en que las empresas revelen claramente qué opciones tienen los usuarios para obtener esta información, qué datos contiene este registro y en qué formatos los pueden obtener los usuarios. Para ecosistemas móviles, confiamos en que la empresa revele a los usuarios si las aplicaciones disponibles en su tienda de aplicaciones especifican que los usuarios pueden obtener toda la información del usuario que la aplicación tiene.

Posibles fuentes:

- Política de privacidad de la empresa
- Configuraciones de cuenta de la empresa
- Centro de ayuda de la empresa
- Publicaciones en el blog de la empresa

P9. Recopilación de información del usuario por terceros (empresas de internet y del ecosistema móvil)

La empresa debe **revelar claramente** sus prácticas con respecto a la **información del usuario** que recopila de sitios web de terceros o **aplicaciones** por **medios técnicos**.

Elementos:

1. ¿La empresa **revela claramente** qué **información del usuario** recopila de sitios web de terceros a través de medios técnicos?
2. ¿La empresa **explica claramente** cómo recopila **información del usuario** de terceros a través de medios técnicos?
3. ¿La empresa **revela claramente** con qué fin recopila **información del usuario** de terceros a través de medios técnicos?
4. ¿La empresa **revela claramente** cuánto tiempo conserva la **información del usuario** que recopila de terceros a través de medios técnicos?
5. ¿La empresa **revela claramente** que respeta las **señales generadas por el usuario** de optar por la no recopilación de sus datos?

Guía del indicador: Confiamos en que las empresas revelen qué información sobre los usuarios recopilan de terceros, que en este caso suele significar información recopilada por sitios web de terceros o aplicaciones a través de medios técnicos, por ejemplo, a través de cookies, programas adicionales o widgets. La revelación de la empresa de estas prácticas ayuda a los usuarios a entender cómo las empresas rastrean sus actividades, si es que las rastrean, aunque no estén alojados en el sitio web de una empresa o sean usuarios de un servicio o plataforma particular.

Posibles fuentes:

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

P10. Proceso para responder solicitudes de terceros de información del usuario

La empresa debe **revelar claramente** su proceso para responder las **solicitudes gubernamentales** y otros **terceros** de **información del usuario**.

Elementos:

1. ¿La empresa **revela claramente** su proceso para responder **solicitudes gubernamentales** no judiciales?

2. ¿La empresa **revela claramente** su proceso para responder **órdenes judiciales**?
3. ¿La empresa **revela claramente** su proceso para responder solicitudes gubernamentales de jurisdicciones extranjeras?
4. ¿La empresa **revela claramente** su proceso para responder a **solicitudes hechas por privados**?
5. ¿Las explicaciones de la empresa **revelan claramente** la base legal con la que puede cumplir con **solicitudes gubernamentales**?
6. ¿Las explicaciones de la empresa **revelan claramente** la base legal con la que puede cumplir con **solicitudes de privados**?
7. ¿La empresa **revela claramente** que lleva a cabo con la debida diligencia las **solicitudes gubernamentales** antes de decidir cómo responder?
8. ¿La empresa **revela claramente** que lleva a cabo con la debida diligencia las **solicitudes privadas** antes de decidir cómo responder?
9. ¿La empresa se compromete a denegar las **solicitudes gubernamentales** inapropiadas o excesivas?
10. ¿La empresa se compromete a denegar las **solicitudes privadas** inapropiadas o excesivas?
11. ¿La empresa ofrece una guía clara o ejemplos de implementación de su proceso de **solicitudes gubernamentales**?
12. ¿La empresa ofrece una guía clara o ejemplos de implementación de su proceso de **solicitudes privadas**?

Guía del indicador: Cada vez más, las empresas reciben solicitudes de entregar información del usuario. Estas solicitudes pueden venir de agencias gubernamentales o cortes (nacionales y extranjeras), y también a través de procesos privados (es decir, procesos no gubernamentales y no judiciales). Confiamos en que las empresas revelen públicamente el proceso para responder solicitudes en cada tipo de proceso, junto con la base para cumplir estas solicitudes. Las empresas también deben comprometerse públicamente a denegar las solicitudes gubernamentales o privadas que sean inapropiadas o excesivas.

En algunos casos, la ley podría impedir que una empresa revelara información mencionada en los elementos de este indicador. Los investigadores documentarán situaciones en las que se presente este caso, pero una empresa perderá puntos si no cumple con todos los elementos. Esto representa una situación en que la ley causa que las empresas no cumplan con las mejores prácticas, 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 la privacidad.

Posibles fuentes:

- Informe de transparencia de la empresa
- Pautas de aplicación de la ley de la empresa
- Política de privacidad de la empresa
- Publicaciones en el blog de la empresa

P11. Datos sobre solicitudes de terceros de información del usuario

La empresa debe publicar con frecuencia datos sobre **solicitudes gubernamentales** y otras **solicitudes privadas de información del usuario**.

Elementos:

1. ¿La empresa hace una lista de la cantidad de solicitudes que recibe por países?
2. ¿La empresa hace una lista de la cantidad de solicitudes que recibe de información del usuario guardada y de **acceso a las comunicaciones en tiempo real**?
3. ¿La empresa hace una lista de la cantidad de cuentas afectadas?
4. ¿La empresa hace una lista de si un pedido buscaba **contenido** de las comunicaciones o no buscaba **contenido** o ambos?
5. ¿La empresa identifica a la autoridad legal específica o tipo de proceso legal a través del cual se realizan los pedidos de aplicación de la ley y seguridad nacional?
6. ¿La empresa incluye solicitudes que vienen de **órdenes judiciales**?
7. ¿La empresa hace una lista de la cantidad de solicitudes que recibe de privados?
8. ¿La empresa hace una lista de la cantidad de solicitudes que cumplió, separadas por categoría de pedido?
9. ¿La empresa hace una lista de qué tipos de solicitudes gubernamentales las leyes prohíben revelar?
10. ¿La empresa informa de estos datos al menos una vez al año?
11. ¿Los datos que una empresa informa se pueden exportar como un archivo de **datos estructurados**?

Guía del indicador: Con frecuencia, las empresas reciben solicitudes de terceros de entregar información del usuario. Estas solicitudes pueden venir de agencias gubernamentales o cortes (nacionales y extranjeras), y también a través de procesos privados (es decir, procesos no gubernamentales y no judiciales). Confiamos en que las empresas publiquen con frecuencia datos sobre la cantidad y tipos de solicitudes que reciben, y con cuántas solicitudes cumplen.

Las empresas deben revelar datos sobre las solicitudes que reciben por país, incluido el suyo propio y Gobiernos extranjeros, y también de las autoridades, cortes y procesos privados. También confiamos que la revelación de la empresa indique la cantidad de cuentas afectadas por estas solicitudes y que defina por categoría las solicitudes que ha cumplido. Reconocemos que a veces, las empresas no pueden revelar las solicitudes de información del usuario que hacen los Gobiernos. Sin embargo, en estos casos, confiamos en que las empresas informen qué tipo de solicitudes gubernamentales no están autorizadas a revelar por ley. Las empresas también deben informar de estos datos una vez al año y se deben asegurar de que los datos se puedan exportar en un archivo de datos estructurados.

En algunos casos, la ley puede impedir que una empresa revele información mencionada en este indicador. Por ejemplo, confiamos en que las empresas publiquen números exactos y no rangos de números. Reconocemos que a veces las leyes impiden que las empresas los publiquen, y los investigadores documentarán las situaciones en que ese sea el caso. Pero una empresa perderá puntos si no cumple con todos los elementos. Esto representa una situación en que la ley cause que las empresas no cumplan con las mejores prácticas, y exhortamos a las empresas a abogar por leyes que les permitan respetar plenamente el derecho de los usuarios a la libertad de expresión y la privacidad.

Posibles fuentes:

- Informe de transparencia de la empresa

P12. Notificación al usuario sobre solicitudes de terceros de información del usuario

La empresa debe **notificar** a los usuarios hasta donde sea legalmente posible cuando Gobiernos o terceros hayan **solicitado** su **información de usuario**.

Elementos:

1. ¿La empresa **revela claramente** que notifica a los usuarios cuando **entidades gubernamentales (incluidos juzgados y otros entes judiciales)** solicitan su **información de usuario**?
2. ¿La empresa **revela claramente** que notifica a los usuarios cuando los privados solicitan su **información de usuario**?
3. ¿La empresa **revela claramente** situaciones en que podría no **notificar** a los usuarios, incluida una descripción de los tipos de **solicitudes gubernamentales** que la ley prohíbe revelar a los usuarios?

Guía del indicador: Confiamos en que las empresas revelen claramente un compromiso de notificación a los usuarios cuando Gobiernos y privados soliciten datos sobre usuarios. Reconocemos que estas notificaciones pueden no ser posible en casos legítimos de una investigación en curso. Sin embargo, confiamos en que las empresas especifiquen qué tipo de solicitudes gubernamentales están prohibidas por ley de ser reveladas.

Posibles fuentes:

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

P13. Supervisión de seguridad

La empresa debe **revelar claramente** información sobre sus procesos institucionales para garantizar la seguridad de sus productos y servicios.

Elementos:

1. ¿La empresa **revela claramente** que tiene sistemas vigentes para limitar y dar seguimiento al acceso de los trabajadores a información del usuario?
2. ¿La empresa **revela claramente** que tiene un equipo de seguridad que lleva a cabo auditorías de seguridad sobre los productos y servicios de la empresa?
3. ¿La empresa **revela claramente** que encarga auditorías de seguridad a terceros para sus productos y servicios?

Guía del indicador: Ya que las empresas manejan y almacenan cantidades inmensas de información sobre los usuarios, deben contar con medidas de seguridad claras para garantizar que esta información esté segura. Confiamos que las empresas revelen claramente que tienen sistemas implementados para limitar y dar seguimiento el acceso de los trabajadores a información del usuario. También confiamos que la empresa revele claramente que tiene equipos de seguridad internos y externos para realizar auditorías de seguridad en sus productos y servicios.

Posibles fuentes:

- Políticas de privacidad de la empresa
- Pautas de seguridad de la empresa

P14. Tratamiento a las vulnerabilidades de seguridad

La empresa debe enfrentar las **vulnerabilidades de seguridad** cuando las descubran.

Elementos:

1. ¿La empresa **revela claramente** que tiene un mecanismo a través del cual los **investigadores de seguridad** pueden presentar las **vulnerabilidades** que descubren?
2. ¿La empresa **revela claramente** el periodo en el que revisará denuncias de **vulnerabilidades**?
3. ¿La empresa se compromete a no iniciar acción legal contra los investigadores que

denuncien **vulnerabilidades** dentro de los términos de mecanismo de denuncia de la empresa?

4. (Para ecosistemas móviles) ¿La empresa **revela claramente** que las **actualizaciones de software, parches** de seguridad, componentes adicionales o extensiones se descargan por un canal **encriptado**?
5. (Para ecosistemas móviles y empresas de telecomunicaciones) ¿La empresa **revela claramente** qué **modificaciones ha hecho a un sistema operativo móvil**, y si es que las ha hecho?
6. (Para ecosistemas móviles y empresas de telecomunicaciones) ¿La empresa **revela claramente** qué efecto tienen esas modificaciones en la capacidad de la empresa de enviar **actualizaciones de seguridad** a los usuarios, si es que tienen efecto?
7. (Para ecosistemas móviles) ¿La empresa **revela claramente** la fecha hasta la que seguirá brindando **actualizaciones de seguridad** para el **dispositivo/sistema operativo**?
8. (Para ecosistemas móviles) ¿La empresa se compromete a brindar **actualizaciones de seguridad** para el sistema operativo y demás software fundamental por un mínimo de cinco años tras el lanzamiento?
9. (Para ecosistemas móviles y empresas de telecomunicaciones) Si la empresa usa un sistema operativo adaptado de un sistema existente, ¿la empresa se compromete a brindar **parches** de seguridad en el término de un mes desde que una **vulnerabilidad** se anuncia al público?

Guía del indicador: El código informático no es perfecto. Cuando las empresas toman conocimiento de vulnerabilidades que pueden poner en riesgo a los usuarios y su información, deben tomar acciones para mitigar esos problemas. Esto incluye garantizar que las personas puedan hacer llegar a la empresa cualquier vulnerabilidad que descubran. Creemos que es especialmente importante que las empresas revelen claramente a los usuarios la manera y el periodo en que los usuarios recibirán actualizaciones de seguridad. Además, como los proveedores de telecomunicaciones pueden alterar los sistemas operativos móviles de fuente abierta, confiamos en que estas empresas revelen información que pueda afectar la capacidad de un usuario de acceder a estas actualizaciones fundamentales.

Posibles fuentes:

- Políticas de privacidad de la empresa
- Guía de seguridad de la empresa
- Foros de “ayuda” de la empresa

P15. Filtraciones de datos

La empresa debe revelar públicamente información sobre sus procesos para responder a las **filtraciones de datos**.

Elementos:

1. ¿La empresa **revela claramente** que notificará a las autoridades relevantes sin demora injustificada cuando ocurra una **filtración de datos**?
2. ¿La empresa **revela claramente** su proceso para notificar los datos a quienes pueden verse afectados por una **filtración de datos**?
3. ¿La empresa **revela claramente** qué medidas tomará para enfrentar el impacto de una **filtración de datos** de sus usuarios?

Guía del indicador: Las empresas deben tener vigentes procesos claramente revelados para abordar las filtraciones de datos, incluidas políticas claras para notificar a los usuarios afectados. Como las filtraciones de datos pueden resultar en amenazas significativas a la seguridad financiera o personal de alguien, además de exponer información privada, las empresas deben hacer que estos procesos estén disponibles para el público. Así, las personas pueden tomar decisiones informadas y evaluar los posibles riesgos antes de suscribirse a un servicio o de brindarle su información a una empresa.

Confiamos en que las empresas tengan políticas formales vigentes con respecto a su manejo de filtración de datos cuando ocurren, si es que ocurren, y hacer que esta información sobre las políticas y compromisos sea pública antes de que ocurra una filtración.

Posibles fuentes:

- Términos de servicio de una empresa o política de privacidad
- Guía de seguridad de una empresa

P16. Encriptación de comunicaciones del usuario y contenido privado (empresas de internet y ecosistema móvil)

La empresa debe **encriptar** la comunicación del usuario y **contenido** privado para que los usuarios puedan controlar quién tiene acceso.

Elementos:

1. ¿La empresa **revela claramente** que la transmisión de las comunicaciones del usuario está **encriptada** por defecto?
2. ¿La empresa **revela claramente** que la transmisión de las comunicaciones del usuario está **encriptada** con llaves únicas?
3. ¿La empresa **revela claramente** que los usuarios pueden asegurar su contenido privado con **encriptación de extremo a extremo**, o **encriptación total del disco** (donde sea aplicable)?
4. ¿La empresa **revela claramente** que la **encriptación de extremo a extremo**, o

encriptación total del disco, está habilitada por defecto?

Guía del indicador: La encriptación es una herramienta importante para proteger la libertad de expresión y la privacidad. El [relator especial de Naciones Unidas sobre Libertad de Expresión ha afirmado](#) sin lugar a dudas que la encriptación y el anonimato son esenciales para el ejercicio y protección de los derechos humanos. Confiamos que las empresas revelen claramente que las comunicaciones del usuario están encriptadas por defecto, que las transmisiones están protegidas por “secreto perfecto hacia adelante”, que los usuarios tienen la opción de activar la encriptación de extremo a extremo, y si la empresa ofrece encriptación de extremo a extremo por defecto. Para ecosistemas móviles, confiamos que las empresas revelen claramente que permiten la encriptación total del disco.

Posibles fuentes:

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

P17. Seguridad de las cuentas (empresas de internet y del ecosistema móvil)

La empresa debe ayudar a los usuarios a mantener sus **cuentas** seguras.

Elementos:

1. ¿La empresa **revela claramente** que implementa métodos de autenticación avanzados para evitar el acceso fraudulento?
2. ¿La empresa **revela claramente** que los usuarios pueden ver la actividad reciente de su cuenta?
3. ¿La empresa **revela claramente** que notifica a los usuarios sobre actividad inusual de la cuenta y posible acceso no autorizado a sus cuentas?

Guía del indicador: Las empresas deben ayudar a los usuarios a mantener sus cuentas seguras. Deben revelar claramente que usan técnicas de autenticación avanzadas para evitar el acceso no autorizado a cuentas e información del usuario. También confiamos que las empresas brinden a los usuarios herramientas que les permitan asegurar sus cuentas y que sepan cuando sus cuentas pueden estar comprometidas.

Posibles fuentes:

- Centro de seguridad de la empresa
- Páginas de ayuda de la empresa o página de apoyo comunitario
- Página de configuración de cuenta de la empresa
- Blog de la empresa

P18. Información e instrucción a los usuarios sobre posibles riesgos

La empresa debe publicar información para ayudar a los usuarios a defenderse de **ciberriesgos**.

1. ¿La empresa publica material práctico que instruya a los usuarios sobre cómo protegerse de **ciberriesgos** relevantes a sus productos o servicios?

Guía del indicador: Como las empresas tienen enormes cantidades de datos de los usuarios, a menudo son blanco de actores maliciosos. Confiamos en que las empresas ayuden a los usuarios a protegerse de esos riesgos. Esto puede incluir publicar materiales sobre cómo configurar autenticación avanzada de la cuenta, adaptar las configuraciones de privacidad, consejos para evitar software malicioso, *phishing* y ataques de ingeniería social, cómo evitar o enfrentar el acoso o *bullying* en línea, y qué significa “navegación segura”. Las empresas deben presentar estas pautas con un lenguaje claro, idealmente acompañado de imágenes, diseñadas para ayudar a los usuarios a entender la naturaleza de los riesgos que pueden enfrentar empresas y usuarios. Pueden incluir consejos, tutoriales, guías instructivas u otros recursos, y deben presentarse de una manera que los usuarios puedan entender fácilmente (por ejemplo, con imágenes, gráficos, cuadros sinópticos y listas).

Posibles fuentes:

- Centro de seguridad de la empresa
- Páginas de ayuda de la empresa o página de apoyo comunitario
- Blog de la empresa

Glosario

Nota: *Este no es un glosario general. Las definiciones y explicaciones que aparecen a continuación fueron escritas específicamente para guiar a los investigadores en evaluar a las empresas de tecnología de la información y la comunicación en los indicadores de este proyecto de investigación.*

Acceso a comunicaciones en tiempo real — Vigilancia de una conversación u otra comunicación electrónica en “tiempo real” mientras se lleva a cabo la conversación, o interceptación de datos en el mismo momento en que se transmite. También se le llama “interceptación”. Considera la diferencia entre una solicitud de interceptación y una solicitud de datos archivados. Una interceptación brinda a las autoridades acceso a futuras comunicaciones, mientras una solicitud para datos archivados da acceso a las autoridades a registros de comunicaciones ocurridas en el pasado. El Gobierno estadounidense puede obtener acceso a las comunicaciones en tiempo real a través de la Ley de Interceptaciones y la Ley de Registro, ambas integrantes de la Ley de Privacidad de Comunicaciones Electrónicas (ECPA, por su nombre en inglés); el Gobierno ruso puede hacerlo a través del “Sistema para Actividades Operativas de Investigación” (SORM, por su nombre en inglés).

Actualización de seguridad — Reparación dada a conocer ampliamente para una vulnerabilidad específica de un producto y relacionada con la seguridad. Las vulnerabilidades de seguridad se califican por su gravedad: críticas, importantes, moderadas o bajas.

Actualización de software — Una actualización de software (a veces llamado parche de software) es una descarga gratuita para una aplicación o paquete de software que brinda reparaciones para características que no funcionan como deberían funcionar o agrega mejoras y compatibilidad de software menores. Una actualización también puede incluir actualizaciones de unidades que mejoran el funcionamiento del hardware o periféricos, o agregan respaldo para nuevos modelos de periféricos.

Actualización fundamental (de software) — Una reparación ampliamente lanzada para una vulnerabilidad específica de un producto y relacionada con la seguridad. Las vulnerabilidades de seguridad se califican por su severidad: críticas, importantes, moderadas o bajas.

Ahogar — Manera terminante de dar forma al tráfico en la que el operador de la red reduce la velocidad del flujo de paquetes a través de una red. Los operadores móviles pueden ahogar el tráfico para aplicar límites a la cantidad de datos transferidos. Para mayor información, ver: Open Signal: “Ahogo de datos: Por qué los operadores reducen la velocidad de tu conexión”, <http://opensignal.com/blog/2015/06/16/data-throttling-operators-slow-connection-speed/>

Algoritmos: Un algoritmo es un conjunto de instrucciones usadas para procesar información y entregar un resultado según lo estipulado en las instrucciones. Los algoritmos pueden ser simples partes de código, pero también pueden ser increíblemente complejos, y “codificar miles de variables a través de millones de puntos de datos”. En el contexto de empresas de internet, móviles y de telecomunicaciones, algunos algoritmos —por su complejidad, la cantidad y tipo de información del usuario que se les ingresa, y la función de toma de decisiones para la que

serven— tienen consecuencias significativas para los derechos humanos de los usuarios, incluidas la libertad de expresión y la privacidad. Leer más en: “[Responsabilidad algorítmica: Manual básico](#)” de Data & Society.

Altos ejecutivos — Director ejecutivo y demás miembros del equipo ejecutivo como aparecen en el sitio web de la empresa u otros documentos oficiales, como su informe anual. Si no hay una lista del equipo ejecutivo definido por la empresa, otras posiciones con nivel de jefe y las que están en las posiciones más altas de gestión (por ejemplo, vicepresidente ejecutivo, dependiendo de la empresa) se consideran altos ejecutivos.

Aplicación — Programa independiente o porción de software diseñado para cumplir un objetivo particular; aplicación de software, sobre todo si un usuario la descarga a un dispositivo móvil.

Archivo público — Recurso públicamente disponible que contiene versiones anteriores de las políticas de una empresa, como términos de servicio o política de privacidad, o que explica exhaustivamente todas las rondas de cambios que la empresa hace a esas políticas.

Ciberriesgos — Situaciones en las que la seguridad, privacidad u otros derechos relacionados de un usuario pueden verse amenazados por un actor malicioso (como por ejemplo, delincuentes, informantes o Estados) que pueden obtener acceso no autorizado a datos del usuario por medio de hackeo, *phishing* u otras técnicas engañosas.

Cierre o restricción de acceso a la red — Cierre de red se refiere a la interrupción intencional de internet o comunicaciones electrónicas, incluidos servicios de telecomunicaciones como telefonía celular y mensajes SMS. Esto incluye un cierre general de todos los servicios celulares o de internet dentro de una zona geográfica y bloqueo dirigido de servicios específicos, como medios sociales o aplicaciones de mensajería.

Compromiso de política — Declaración disponible públicamente que representa la política oficial de la empresa que ha sido aprobada en los niveles más altos de la empresa.

Contenido — La información contenida en comunicaciones por cable, oral o electrónica (por ejemplo, una conversación que tiene lugar por teléfono o cara a cara, el texto escrito y transmitido en un mensaje SMS o correo electrónico).

Cookie(s) — “Las [cookies](#) son una tecnología web que permite a los sitios web reconocer tu navegador. Originalmente, las cookies fueron diseñadas para permitir que los sitios ofrecieran carritos de compra en línea, guardar preferencias o mantener tu sesión en un sitio. También permiten rastrear y hacer perfiles, para que los sitios puedan reconocerte y saber más de a dónde vas, qué dispositivos usas y qué te interesa – aunque no tengas cuenta en ese sitio o no hayas iniciado sesión”. Fuente: <https://ssd.eff.org/en/glossary/cookies>

Cuenta / cuenta de usuario — Grupo de datos asociados con el usuario particular de un sistema informático, servicio o plataforma. Como mínimo, la cuenta de usuario comprende un nombre de usuario y una contraseña, que se usan para autenticar el acceso del usuario a sus

datos.

Dar forma al tráfico — Configurar el flujo de tráfico a través de una red. Puede incluir hacer más lentos algunos tipos de tráfico condicionalmente. Se puede usar para dar forma al tráfico con fines de un manejo legítimo de redes (por ejemplo, dar prioridad a tráfico VoIP antes que tráfico web normal para facilitar comunicación en tiempo real) o por razones que responden a principios de neutralidad en la red (por ejemplo, reducir intencionalmente el tráfico del video para disuadir a los usuarios de utilizar aplicaciones con gran ancho de banda).

Datos anónimos — Datos que de ninguna manera están relacionados con otra información que permitiría que se identificara a un usuario. La naturaleza amplia de esta definición que se usa en el proyecto de Ranking Digital Rights es necesaria para reflexionar sobre varios hechos. Primero, analistas especializados pueden “desanonimizar” grandes conjuntos de datos. Esto hace que sea imposible cumplir con casi todas las promesas de anonimización. En esencia, ningún dato vinculado con un “identificador anónimo” es anónimo. Más bien, suelen ser datos pseudónimos que se pueden conectar con la identidad fuera de línea del usuario. Segundo, los metadatos pueden ser más o igualmente reveladores de las asociaciones e intereses de un usuario que los datos de contenido, por lo que estos datos son de vital interés. Tercero, las entidades que tienen acceso a muchas fuentes de datos, como agentes de datos y Gobiernos, pueden juntar una o más fuentes de datos que revelan información sobre los usuarios. Por tanto, agentes sofisticados pueden usar los datos que parecen anónimos para construir una mayor imagen de un usuario.

Datos de ubicación— Información recopilada por una red o servicio sobre dónde está o estuvo ubicado el teléfono u otro dispositivo del usuario —por ejemplo, rastrea la ubicación de un teléfono móvil por datos recopilados por estaciones base en una red de telefonía móvil o a través de posicionamiento de GPS o de redes inalámbricas.

Datos estructurados — “Datos en campos fijos dentro de un registro o archivo. Las bases de datos relacionales y hojas de cálculo son ejemplos de datos estructurados. Aunque los datos en archivos XML no están fijos en un lugar como los registros de bases de datos tradicionales, están estructurados porque los datos están etiquetados y se les puede identificar con precisión”. A la inversa, los datos no estructurados son datos que “no están ubicados en lugares fijos. El término generalmente se refiere a texto sin formato, que es ubicuo. Los ejemplos son documentos de procesamiento de palabras, archivos PDF, mensajes de correo electrónico, blogs, páginas web y sitios sociales”.

Fuentes: PC Mag Encyclopedia:

“datos estructurados” <http://www.pcmag.com/encyclopedia/term/52162/structured-data>

“datos no estructurados” <http://www.pcmag.com/encyclopedia/term/53486/unstructured-data>

Desidentificar (información del usuario) — Esto se refiere a información del usuario que las empresas recopilan y retienen, pero solamente después de retirar u ocultar toda información que lo pueda identificar. Esto significa retirar identificadores explícitos como nombres, dirección de correo electrónico y cualquier número de identificación oficial, así como identificadores como

direcciones IP, cookies y números únicos de dispositivos.

Despliegue / desplegar — Serie de anuncios de productos relacionados que se llevan a cabo con el tiempo; el proceso de hacer parches, actualizaciones de software y mejoras de software disponibles para usuarios finales.

Difusión / difundir — La empresa permite a terceros acceder a la información del usuario, ya sea por entrega de la información libremente a un tercero (al público o a otros usuarios) o por venta a un tercero.

Dispositivo / dispositivo portátil / dispositivo móvil — Objeto físico, como un smartphone o un teléfono básico, que se usa para acceder a redes de telecomunicaciones diseñado para que el usuario lo porte y lo use en diversos lugares.

Documentación — La empresa brinda registros que los usuarios pueden consultar, como un registro de cambios a los términos de servicio o documentos de política de privacidad.

Ecosistema móvil — Conjunto indivisible de bienes y servicios que ofrece una empresa de dispositivos móviles, que comprende el hardware del dispositivo, sistema operativo, tiendas de aplicaciones y cuenta de usuario.

Encriptación — En esencia, oculta el contenido de comunicaciones o archivos de tal manera que solamente el destinatario pueda verlo a quien estaba dirigido. El proceso usa un algoritmo para convertir el mensaje (texto sin formato) en un formato codificado (texto cifrado) para que quien quiera que vea el mensaje lo vea como una serie aleatoria de caracteres. Solamente alguien con la clave de encriptación apropiada puede descifrar el mensaje, revertir el texto cifrado en texto sin formato. Los datos pueden estar encriptados cuando se guardan y cuando están en una transmisión.

Por ejemplo, los usuarios pueden encriptar los datos de su disco duro para que solamente el usuario con la clave de encriptación pueda descifrar los contenidos del disco. Además, los usuarios pueden enviar un mensaje de correo electrónico encriptado, lo que impediría que alguien viera el contenido del correo electrónico mientras el mensaje se mueve por la red para llegar al destinatario a quien estaba dirigido. Con encriptación en tránsito (por ejemplo, cuando un sitio web usa HTTPS), la comunicación entre un usuario y un sitio web está encriptada, para que los externos, como el proveedor de servicio de internet del usuario, solamente puedan ver la visita inicial al sitio web, pero no lo que el usuario comunica en ese sitio web ni las subpáginas que el usuario visita. Para más información, ver este recurso:

<http://www.explainthatstuff.com/encryption.html>.

Encriptación de extremo a extremo — Con encriptación de extremo a extremo, solamente el remitente y el destinatario pueden leer el contenido de las comunicaciones encriptadas. Terceros, incluida la empresa, no podrán descifrar el contenido.

Encriptación total del disco — Encriptación completa de todos los datos almacenados en un dispositivo físico, de tal manera que solamente el usuario puede acceder al contenido al suministrar la contraseña, o contraseñas, generada por el usuario y/u otros medios de

desencriptación (huella digital, código de autenticación de dos factores, autenticador físico, etc.).

Equipo / programa — Unidad definida dentro de una empresa que tiene responsabilidad en cómo los productos o servicios de la empresa se intersectan, en este caso, con la libertad de expresión o privacidad.

Evaluación de impacto en los derechos humanos (evaluación de riesgos de derechos humanos) — La evaluación de riesgos de derechos humanos es un enfoque sistemático a la debida diligencia. Una empresa lleva a cabo estas evaluaciones o revisiones para ver cómo sus productos, servicios y prácticas empresariales afectan la libertad de expresión y la privacidad de sus usuarios.

Para más información sobre Evaluación de impacto en los derechos humanos y mejores prácticas para llevarla a cabo, revisa esta página especial alojada en el Centro de Recursos de Negocios y Derechos Humanos: <https://www.business-humanrights.org/es/node/86208/principios-rectores-sobre-empresas-y-derechos-humanos-0/implementaci%C3%B3n-ejemplos-y-herramientas/implementaci%C3%B3n-por-parte-de-empresas-ejemplos-y-herramientas/evaluaci%C3%B3n-de>

El Instituto Danés para los Derechos Humanos ha elaborado una herramienta relativa a Evaluación de cumplimiento de derechos humanos (<https://hrca2.humanrightsbusiness.org>), y la organización Business for Social Responsibility (BSR) ha elaborado una guía útil para llevar a cabo evaluación de riesgos de derechos humanos: <http://www.bsr.org/en/our-insights/bsr-insight-article/how-to-conduct-an-effective-human-rights-impact-assessment>

Para una guía específica del sector de tecnologías de la información y la comunicación, ver el extracto del capítulo del libro (“Negocios, derechos humanos e internet: Marco para la Implementación”) de Michael Samway en el sitio web del proyecto en: http://rankingdigitalrights.org/resources/readings/samway_hria.

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

Fácil de encontrar — Los términos de servicio o la política de privacidad están a uno o dos clics de la página de inicio de la empresa o servicio, o están en un lugar lógico donde es probable que los usuarios los encuentren.

Fácil de entender / manera comprensible — La empresa ha tomado medidas para ayudar a los usuarios a entender sus términos de servicio y política de privacidad. Esto incluye, entre otros, brindar resúmenes, consejos u orientación que expliquen qué significan los términos, con encabezados de sección, tipo de letra legible u otras características gráficas para ayudar a los usuarios a entender el documento, o redactar los términos con sintaxis legible.

Filtración de datos — Una filtración de datos ocurre cuando una parte no autorizada adquiere acceso a la información del usuario que una empresa recopila, retiene o procesa de alguna manera, y que compromete la integridad, seguridad o confidencialidad de esa información.

Funcionalidad básica — Las funciones o características más esenciales de un producto o servicio. Por ejemplo, la funcionalidad básica de un smartphone incluiría hacer y recibir llamadas, mensajes de texto y correos electrónicos, descargar y ejecutar aplicaciones y acceder a internet.

Funcionario —Trabajador de jerarquía responsable de un conjunto explícito de riesgos e impactos, en este caso, privacidad y libertad de expresión.

Geolocalización — Identificación de la ubicación geográfica en el mundo real de un objeto, como una fuente de radar, teléfono móvil o terminal de cómputo conectada a internet. La geolocalización se puede referir a la práctica de evaluar la ubicación o a la propia ubicación evaluada.

Información del usuario — Todo dato relacionado con una persona identificable, o que se puede vincular a esa persona si se combinan conjuntos de datos o se utilizan técnicas de minería de datos. Como explicación adicional, información del usuario es todo dato que documente las características y actividades de un usuario. Esta información puede o no estar vinculada a la cuenta de un usuario específico. Esta información incluye, entre otros, correspondencia personal, contenido generado por el usuario, preferencias y configuraciones de cuenta, datos de registro y acceso, datos sobre las actividades o preferencias de un usuario recopiladas de terceros a través de rastreo de comportamiento o compra de datos, y todas las formas de metadatos. La información del usuario nunca se considera anónima, salvo cuando está incluida únicamente como base para generar medidas globales (por ejemplo, cantidad de usuarios activos por mes). Por ejemplo, la afirmación “Nuestro servicio tiene un millón de usuarios activos por mes” contiene datos anónimos pues no brinda suficiente información para saber quiénes son ese millón de usuarios.

Iniciativa de múltiples interesados — Una organización creíble de múltiples interesados incluye y está regida por miembros de al menos otros tres grupos interesados además de la industria: sociedad civil, inversionistas, académicos, representantes de usuarios o clientes en general, comunidad de técnicos y Gobierno. Su modelo de financiamiento se deriva de más de un tipo de fuente (empresas, Gobiernos, fundaciones, donaciones públicas, etc.). Su independencia, rigor y profesionalismo son muy altos, con fuerte participación de organizaciones de derechos humanos que tienen sólido historial de independencia de control corporativo y gubernamental. Global Network Initiative es un ejemplo de iniciativa de múltiples interesados dedicada a la libertad de expresión y la privacidad en el sector de tecnologías de la información y la comunicación.

Inteligencia artificial — La inteligencia artificial tiene una variedad de usos y significados. Para fines de la metodología de RDR, la inteligencia artificial se refiere a sistemas que se parecen, llevan a cabo o imitan funciones que típicamente necesitan inteligencia. Los ejemplos incluyen software de reconocimiento facial, procesamiento natural del lenguaje y otros, y cuyo uso por las empresas de internet, móviles y de telecomunicaciones tienen consecuencias en los derechos de libertad de expresión y privacidad de las personas. Ver: [“Privacidad y libertad de expresión en la era de la inteligencia artificial”](#).

Interesados — Personas que tienen un “interés” porque de alguna manera se ven afectadas por las acciones o decisiones de una empresa. Nótese que interesado no es lo mismo que “titulares de derechos” y que hay diferentes tipos de interesados; los directamente afectados, e “interesados intermediarios”, cuyo rol es defender los derechos de los interesados directos. Los titulares de derechos son las personas cuyos derechos humanos pueden verse directamente impactados. Interactúan con la empresa y sus productos y servicios a diario, por lo general como trabajadores, clientes o usuarios. Los usuarios intermediarios incluyen personas y organizaciones informadas y que pueden hablar en nombre de los titulares de derechos, como organizaciones de la sociedad civil, grupos activistas, académicos, formadores de opinión y diseñadores de políticas” (p. 10 de 28). Fuente: Compromiso de las partes interesadas en la diligencia debida en materia de derechos humanos: desafíos y soluciones para empresas de TIC por BSR, septiembre de 2014

http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf

Investigador de seguridad — Alguien que estudia cómo garantizar los sistemas técnicos y las amenazas a la seguridad informática y de red para encontrar una solución.

Junta directiva — La supervisión a nivel directivo debe incluir a los miembros de la junta que tengan supervisión directa de asuntos relacionados con la libertad de expresión y la privacidad. No tiene que ser un comité formal, pero la responsabilidad de los directivos de supervisar las prácticas de la empresa en estos asuntos debe estar claramente articulada y revelada en el sitio web de la empresa.

Limitación de uso / propósito — Según el principio de minimización de uso o propósito, las entidades que manejan información del usuario deben declarar con qué fin lo hacen y deben limitar el uso de esa información para cualquier otro propósito a menos que reciban consentimiento del usuario. *Ver también principio de minimización de datos (más abajo).*

Medios técnicos — Las empresas despliegan diversas tecnologías, como cookies, widgets y botones para rastrear la actividad de los usuarios en sus servicios y en sitios y servicios de terceros. Por ejemplo, una empresa puede insertar contenido en el sitio web de un tercero y recopilar información del usuario cuando un usuario pone “me gusta” o interactúa de otra manera con este contenido.

Mejora de software — Una mejora de software es una nueva versión de un software que ofrece una mejora o cambio significativo a la versión actual.

Minimización de datos — Según el principio de minimización de datos, las empresas deben limitar la recopilación de información del usuario a lo que es relevante y necesario para lograr un objetivo claramente especificado. *Ver también: limitación de uso (ya definido).*

Modificaciones a un sistema operativo móvil — Cambios hechos a la versión estándar de un sistema operativo móvil que puede afectar la funcionalidad básica, la experiencia del usuario o el proceso de mostrar actualizaciones de software. Las funcionalidades básicas son las funciones o características más esenciales de un producto o servicio. Por ejemplo, una funcionalidad básica de un smartphone incluye hacer y recibir llamadas telefónicas, mensajes

de texto y correos electrónicos, descargar y ejecutar aplicaciones, y acceso a internet. Esto se aplica a smartphones Android fabricados por empresas además de Google.

Nivel gerencial —Comité, programa, equipo o funcionario que no es parte del directorio de la empresa ni del equipo ejecutivo.

No rastrear — También conocido por las siglas “DNT” (por la frase en inglés “Do not track”), se refiere a una configuración en las preferencias del navegador de un usuario que comunica a empresas o terceros que no lo “rastreen”. En otras palabras, cada vez que un usuario abre un sitio web, se comunica a todas las partes involucradas en presentar la página (que suelen ser muchas, sobre todo anunciantes) que no recopilen ni guarden ninguna información de la visita del usuario a esa página. Sin embargo, es solamente una solicitud educada, pues una empresa puede ignorar una solicitud de no rastrear, y muchas la ignoran.

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

Opciones para controlar — La empresa brinda al usuario un mecanismo directo y fácil de entender para elegir o no elegir recopilación, uso o difusión de datos. “Elegir” (opt-in) significa que la empresa no recopila, usa ni difunde datos para un propósito determinado hasta que los usuarios señalen explícitamente que quieren que se haga. “No elegir” (opt-out) significa que la empresa usa los datos para un propósito determinado por defecto, pero que dejará de recopilar una vez que el usuario le diga a la empresa que deje de hacerlo. Nótese que esta definición es potencialmente controvertida, pues muchos defensores de la privacidad creen que solamente “elegir” constituye control aceptable. Sin embargo, para propósitos de RDR, hemos elegido contar “no elegir” como forma de control.

Órdenes judiciales — Órdenes emitidas por un juzgado a corte, tanto en casos penales como civiles.

Parche — Pieza de software diseñada para actualizar un programa informativo o los datos de apoyo, para repararlo o mejorarlo. Esto incluye reparar las vulnerabilidades seguridad y otros fallos, con parches conocidos como *bugfixes* (reparación de fallos), y mejorar la facilidad de uso del programa de cómputo, aplicación o sistema operativo.

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, otras comunicaciones, etc.

Participar — Interacciones entre la empresa y los interesados. Las empresas o interesados pueden iniciar estas interacciones, y pueden tomar diversos formatos, incluidos mensajes, otra comunicación, etc.

Plataforma — En el sentido más general, plataforma informática es toda pieza informática u objeto de código preexistente diseñado para ejecutarse según sus restricciones y que usa sus servicios. El término plataforma informática puede referirse a diferentes niveles de abstracción, incluida una arquitectura de hardware, un sistema operativo (OS) y bibliotecas de ejecución.^[1]

En total, se puede decir que es la etapa en que los programas informáticos se pueden ejecutar.

Políticas de privacidad — Documentos que definen las prácticas de una empresa que incluyen la recopilación y uso de información, sobre todo información sobre los usuarios.

Priorización — La priorización ocurre cuando un operador de red “gestiona su red de una manera que beneficie un contenido, aplicaciones, servicios o dispositivos particulares”. Para propósito de RDR, esta definición de priorización incluye la decisión de una empresa de bloquear el acceso a aplicación, servicio o dispositivo particular.

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

Programa de informante — Es un programa a través del cual los trabajadores de una empresa pueden denunciar cualquier presunta actividad ilícita que vean al interior de la empresa, incluidos asuntos relativos a derechos humanos. Suele tomar la forma de una línea de ayuda anónima y suele ser responsabilidad de un ejecutivo de conformidad o funcionario de ética.

Programador / programador de terceros — Persona, o grupo de personas, que crean un programa de software o aplicación que se distribuye a través de la tienda de aplicaciones de la empresa.

Protocolo — Conjunto de reglas que rigen el intercambio o transmisión de datos entre dispositivos.

Publicidad dirigida — También se le conoce como “publicidad basada en intereses” o “publicidad personalizada”, y se refiere a la práctica de transmitir anuncios a la medida a los usuarios según su historial de navegación, información de ubicación, perfiles y actividades en medios sociales, y características demográficas y otras funciones. La publicidad dirigida depende de prácticas de gran recopilación de datos, que pueden incluir rastrear las actividades de los usuarios por internet con cookies, widgets y otras herramientas de rastreo, para crear perfiles de usuario detallados.

Reclamo — RDR toma la definición de reclamo de los Principios Rectores de Naciones Unidas sobre Negocios y Derechos Humanos: “percepción de una injusticia que afecte a los derechos reivindicados por una persona o grupo de personas sobre la base de una ley, un contrato, promesas explícitas o implícitas, prácticas tradicionales o nociones generales de justicia de las comunidades agraviadas” (p. 33 de 43.) Fuente: “Principios rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de las Naciones Unidas para ‘proteger, respetar y remediar’” 2011, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf.

Recopilar / recopilación — Todos los medios a través de los cuales una empresa puede reunir información sobre los usuarios. Por ejemplo, una empresa puede recopilar esta información directamente en diversas situaciones, que incluye cuando los usuarios publican

contenido para difusión pública, enviar números de teléfono para verificación de cuentas, transmitir información personal en conversaciones privadas entre ellos, etc. Una empresa también puede recopilar esta información indirectamente, por ejemplo, con un archivo de datos de registro, información de la cuenta, metadatos y otra información relacionada que describa a los usuarios o documente sus actividades.

Registro de cambios — Registro que describe los cambios específicos en un documento, en este caso, un documento de términos de servicio o de política de privacidad.

Requerir — Requerimiento que puede ocurrir cuando un usuario se suscribe a una cuenta o más adelante, a solicitud de una empresa.

Restricción de cuenta / restringir la cuenta de un usuario — Limitación, suspensión, desactivación, eliminación o cancelación de la cuenta o permisos de la cuenta de un usuario específico.

Retención de información del usuario — Una empresa puede recopilar datos y luego eliminarlos. Si la empresa no los elimina, los datos quedan “retenidos”. El tiempo entre la recopilación y eliminación es el “periodo de retención”. Esos datos pueden caer dentro de nuestra definición de “información del usuario”, o pueden ser anónimos. Hay que tener en cuenta que los datos realmente anónimos de ninguna manera se pueden relacionar con un usuario, identidad, comportamiento o preferencia de un usuario, algo que no suele suceder.

Un tema relacionado es el “periodo de retención”. Por ejemplo, una empresa puede recopilar datos de registro continuamente, pero purga (elimina) los datos una vez por semana. En este caso, el periodo de retención de datos es de una semana. Sin embargo, si no se especifica periodo de retención, se debe asumir por defecto que los datos no se eliminan nunca, y el periodo de retención es indefinido. En muchos casos, los usuarios pueden querer que se retengan sus datos mientras usen activamente el servicio, pero quisieran que se eliminaran (por lo tanto, que no se retengan) cuando dejen de usar el servicio, si es que dejan de usarlo. Por ejemplo, los usuarios pueden querer que el servicio de una red social conserve todos sus mensajes privados, pero cuando el usuario sale de la red puede querer que todos sus mensajes privados se eliminen.

Revelar claramente — La empresa presenta o explica sus políticas o prácticas en sus materiales visibles para el público de una manera fácil de encontrar y entender para los usuarios.

Secreto hacia adelante / secreto perfecto hacia adelante — Método de encriptación usado sobre todo en el tráfico web HTTPS y en aplicaciones de mensajería, en el que se genera un nuevo par de llaves para cada sesión (HTTPS), o para cada mensaje intercambiado entre las partes (aplicaciones de mensajería). De esta manera, si un adversario obtiene una llave de descryptación, no podrá descryptar transmisiones anteriores o futuras ni mensajes en la conversación. El secreto hacia adelante es diferente a la encriptación de extremo a extremo, que se refiere a datos que se encriptan mientras “descansan” en servidores remotos de la empresa. Para leer más, visita [“Presionar para secreto perfecto hacia adelante”](#), de Electronic Frontier Foundation.

Señales generadas por el usuario — Muchas empresas permiten que los usuarios “elijan” salir del rastreo con la configuración de diversas cookies específicas de las empresas. Si un usuario elimina cookies para proteger la privacidad, se les rastrea hasta que vuelven a configurar la cookie de “elegir salir”. Además, algunas empresas pueden pedirle a un usuario que instale un componente adicional para evitar el rastreo. Estos dos escenarios comunes son ejemplos de cómo se obliga a los usuarios a usar señales que son específicas para las empresas, y que por tanto no cuentan. En cambio, una señal generada por el usuario viene del usuario y es un mensaje universal de que no se debe rastrear al usuario. La principal opción para una señal generada por el usuario es el encabezado “No rastrear” (ya definido), pero esta redacción deja la puerta abierta a medios futuros para que los usuarios indiquen que no quieren que se les rastree.

Sin contenido — Datos sobre un caso de comunicación o sobre un usuario. Las empresas pueden usar diferentes términos para referirse a estos datos, como metadatos, información básica del suscriptor, datos de transacción sin contenido, datos de cuenta o información del cliente.

En Estados Unidos, la [Ley de Comunicaciones Almacenadas](#) define comunicaciones o registros del cliente sin contenido como “nombre, dirección, registros de conexión telefónica local y de larga distancia o registros de hora y duración de sesiones; duración del servicio (incluida fecha de inicio) y tipos de servicio utilizado; número de teléfono o instrumento u otro número de identidad del suscriptor (incluida toda dirección de red temporalmente asignada), y medios y fuente de pago por el servicio (incluido todo número de tarjeta de crédito o cuenta bancaria)”. El [Manual sobre la ley de Protección de Datos Europea de la Unión Europea](#) afirma: “La confidencialidad de las comunicaciones electrónicas concierne al contenido de una comunicación y también a datos de tráfico, como información de quién se comunica con quién, cuándo y cuánto tiempo, y datos de ubicación, como desde dónde se comunicaron esos datos”.

Sistema operativo — Software que respalda las funciones básicas de una computadora, como programación de tareas, ejecución de aplicaciones y control de unidades periféricas. Un sistema operativo móvil es el sistema operativo de un dispositivo móvil, como smartphone o tableta.

Software malicioso / malware — Término amplio usado para referirse a diversas formas de software hostil o invasivo, como virus informáticos, gusanos, troyanos, *ransomware*, software espía, software publicitario o adware, *scareware* y otros programas maliciosos. Puede tomar la forma de código ejecutable, texto, contenido activo u otro software.

Solicitudes gubernamentales — Este incluye solicitudes de ministerios o agencias estatales, autoridades y órdenes judiciales en casos penales y civiles.

Solicitudes gubernamentales no judiciales — Son solicitudes que vienen de entidades gubernamentales que no son entes judiciales, juzgados ni cortes. Pueden incluir solicitudes de ministerios, agencias, departamentos de policía, oficiales de policía (que actúen en calidad oficial) y otras oficinas, autoridades o entes gubernamentales no judiciales.

Solicitudes privadas — Solicitudes hechas a través de un proceso privado más que un proceso judicial o gubernamental. Las solicitudes privadas de restricción de contenido pueden venir de un ente autorregulatorio como Internet Watch Foundation, o un sistema de notificación y cierre, como la Ley de Derechos de Autor de la Era Digital estadounidense. Para mayor información sobre notificación y cierre, y también para la Ley de Derechos de Autor de la Era Digital específicamente, ver el reciente informe de la UNESCO, “Fomentando la libertad en línea: el papel de los intermediarios de Internet” en <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf> (p. 40-52 de 211).

Solución — “La solución puede incluir disculpas, restitución, rehabilitación, compensación financiera o no financiera y sanciones punitivas (ya sean penales o administrativas, como multas), y también la prevención de daños a través de, por ejemplo, mandatos judiciales o garantías de no repetición. Los procedimientos para la disposición de soluciones deben ser imparciales, estar protegidas de corrupción y libres de intentos políticos o de otra índole que puedan influir en el resultado” (p. 22 de 27).

Fuente: “Informe del representante especial del secretario general en asuntos de derechos humanos y empresas transnacionales y otras empresas, John Ruggie. Principios rectores en negocios y derechos humanos: Implementando el marco de trabajo de Naciones Unidas: ‘Protección, respeto y solución’”, 2011.
<http://business-humanrights.org/sites/default/files/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf>

Supervisión / supervisor — Los documentos de gobernabilidad de la empresa o el proceso de toma de decisiones asignan a un comité, programa, equipo o funcionario con autoridad formal de supervisión con una función particular. Este grupo o persona tiene la responsabilidad para la función y se evalúa según el grado con el que cumple esa responsabilidad.

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

Terceros — “Parte” o entidad diferente al usuario o la empresa. Para los propósitos de esta metodología, los terceros pueden incluir organizaciones gubernamentales, cortes u otros privados (por ejemplo, una empresa, una ONG o una persona individual).

Términos de servicio — También se le puede llamar Términos de uso, Términos y Condiciones, etc. Los términos de servicio “a menudo brindan los principios básicos necesarios de cómo se deben usar diversos servicios en línea”, como establece EFF, y representa un acuerdo legal entre la empresa y el usuario. Las empresas pueden tomar acciones contra los usuarios y su contenido basándose en la información en los términos del servicio. Fuente: Electronic Frontier Foundation, “Términos de (ab)uso” <https://www.eff.org/issues/terms-of-abuse>

Tienda de aplicaciones — Plataforma a través de la cual una empresa hace que sus propias aplicaciones y las creadas por programadores de terceros estén disponibles para descarga. Una tienda de aplicaciones (o mercado de aplicaciones) es una plataforma de distribución

digital para software de computadora, a menudo en un contexto móvil.

Toma de decisiones automatizadas — Tecnología que toma decisiones sin supervisión o aporte humano significativo en el proceso de toma de decisiones, como a través del uso de inteligencia artificial o algoritmos.

Usuario — Persona que usa un producto o servicio. Incluye a personas que publican o transmiten contenido en línea, y también a quienes tratan de acceder o recibir el contenido. Para los indicadores en la categoría de libertad de expresión, esto incluye programadores de terceros que crean aplicaciones que están alojadas o se distribuyen a través del producto o servicio de una empresa.

Vulnerabilidad de la seguridad — Debilidad que permite a un atacante reducir la seguridad de la información de un sistema. Una vulnerabilidad es la intersección de tres elementos: susceptibilidad o defecto de un sistema, acceso de un atacante al defecto y capacidad de atacante de explotar el defecto.

Widget — Parte de un código que permite a un usuario o una empresa insertar aplicaciones y contenido de un sitio web o servicio en el sitio o servicio de un tercero diferentes. En algunos casos, las empresas usan widgets en el sitio web de un tercero y recopilan información sobre los visitantes de ese sitio web sin su conocimiento.