Anexo 1. Guía ESOMAR

GUÍA ESOMAR PARA LA INVESTIGACIÓN ONLINE

Esta guía se actualizará periódicamente según sea necesario. También está disponible en formato web con enlaces activos a otras directrices de ESOMAR y fuentes útiles. Para ver esta guía en línea, vaya a la sección “Conocimiento y normas” > “Códigos y guías” de nuestro sitio web www.esomar.org

CONTENTS

Los códigos y guías de ESOMAR se elaboran en inglés y son los textos en inglés las versiones definitivas. Todos los códigos y guías de investigación de ESOMAR WorldResearch, incluyendo las actualizaciones más recientes, están disponibles online en www.esomar.org.

1. INTRODUCCIÓN

El Código Internacional ICC/ESOMAR para la investigación social y de mercados es tecnológicamente neutral y totalmente aplicable tanto a la investigación *online* como a cualquier otra forma de recolección de datos. Por lo tanto, los fundamentos esenciales establecidos en el Código ICC/ESOMAR (ver Apéndice 1) forman la base de esta Guía ESOMAR para la investigación online.

Si bien muchas de las cuestiones técnicas y metodológicas relacionadas con la investigación a través de internet se han aclarado desde que esta Guía se actualizó por última vez en 2005, el marco jurídico internacional que rige internet continúa evolucionando, lo que significa que la investigación *online* opera en un marco jurídico menos definido que otras formas de investigación, especialmente en entornos multinacionales. El objetivo de esta Guía es explicar la forma de aplicar algunos de los principios fundamentales del Código en el contexto de los entornos legales y regulatorios vigentes actualmente en todo el mundo, y apoyar a los investigadores en el tratamiento de las consideraciones legales, éticas y prácticas en el uso de las nuevas tecnologías al llevar a cabo una investigación *online*.

ESOMAR considera fundamental insistir en la diferenciación entre la investigación de mercados y *marketing*. La investigación de mercados no es una comunicación comercial y funciona dentro de una normativa menos restrictiva en todo el mundo. La distinción se puede explicar fácilmente: los datos personales recogidos para la investigación de mercados se utilizan sólo con fines de investigación y no se divulgan para hacer *marketing* dirigido a un individuo o para otros usos. Véase la *Guía ESOMAR para diferenciar la investigación de mercados de otras actividades de recolección de datos.*

ESOMAR ha trabajado en estrecha colaboración con CASRO en el desarrollo de esta Guía y, en concreto la sección sobre el uso de las tecnologías en la investigación se basa en, y está alineada con, las directrices de CASRO.

La revisión de este documento está todavía en curso. La orientación sobre los paneles de acceso en la sección 5.2 se mantiene sin cambios desde su primera publicación, pero se actualizará próximamente. También se pretende añadir orientación sobre otros temas importantes.

1.1. Principios fundamentales de la investigación *online*

Con leyes que varían de país a país y nuevas posibilidades emergiendo constantemente, debería haber tres principios rectores fundamentales para los investigadores *online*.

Primero, tratar al entrevistado (o a la persona dispuesta a participar en un estudio) con respeto. Los investigadores han de crear una relación con el público basada en la confianza, el respeto y la reciprocidad, asegurándose de que las personas que participen en un estudio online tengan una buena experiencia.

Segundo, los investigadores deben ser sensibles a las preocupaciones de los consumidores y ser conscientes de que el éxito de la investigación de mercados depende de la confianza del público. Los investigadores deberían evitar las actividades y prácticas tecnológicas que podrían minar la confianza pública en la industria de investigación de mercados.

Tercero, los investigadores deben mantener diligentemente la diferenciación entre la investigación y las actividades comerciales, como el *marketing* directo o la personalización de la publicidad. Cuando los investigadores participen en actividades que utilicen técnicas

de investigación como la entrevista personal, pero que no estén exclusivamente destinadas a fines de investigación, no deben describirlas como investigación de mercados, social o de opinión.

Además, los investigadores deben adherirse a los requisitos de protección de datos expuestos en el artículo 7c del Código Internacional ICC/ESOMAR para la investigación social y de mercados, que son los siguientes:

La información personal adquirida y almacenada en conformidad con el presente Código será:

- recolección con fines específicos de investigación y no se utilizará de manera incompatible con dichos fines;
- adecuada, pertinente y no excesiva en relación con el propósito de la investigación para la que se recogió y/o procesó; y
- conservada durante no más tiempo del necesario para el propósito con que se recogió o procesó la información.

Los investigadores se asegurarán de que la identidad de los entrevistados no sea revelada al cliente. El investigador podrá transmitir información personal identificativa del entrevistado al cliente, salvo que las disposiciones nacionales requieran normas más estrictas, en las siguientes condiciones:

i) el entrevistado ha manifestado explícitamente este deseo y/o

ii) que el demandado haya dado su consentimiento explícito y

iii) en el entendimiento de que ninguna actividad comercial (según se define en el artículo 1 del Código ICC/ESOMAR de investigación social y de mercados) se dirige a ellos como resultado directo de haber proporcionado sus datos personales.

2. CUESTIONES ÉTICAS

2.1. Manipulación de datos personales

Los datos proporcionados por los entrevistados son confidenciales y la identidad de éstos debe ser protegida. La identidad de los encuestados no debe ser revelada al usuario de la información sin el consentimiento expreso de los entrevistados. Además, el investigador debe garantizar que la información se recoge con fines exclusivos de investigación y no se utilizará de ninguna manera incompatible con dichos fines (véase el Artículo 7 del **Código Internacional ICC/ESOMAR**). Ninguna información personal identificativa podrá ser utilizada posteriormente para fines diferentes de la investigación tales como el *marketing* directo, la creación de listas, la calificación crediticia, la recaudación de fondos u otras actividades de *marketing* relacionadas con los entrevistados (véase el Artículo 1d de las **Notas** del Código Internacional ICC/ESOMAR).

2.1.1. Identificadores personales

La dirección de correo electrónico u otros identificadores personales de un entrevistado (por ejemplo, nombre de usuario o identificador de dispositivo cuando esto se reseñe en los

datos) son datos de carácter personal y deben ser protegidos de la misma manera que otros identificadores.

Si todos los datos que puedan conducir a la identificación de un individuo se eliminan de los registros de datos (incluyendo los números de serie que enlazan a un archivo separado de los datos de identidad), se considera que el conjunto de datos no contiene datos personales y deja de estar sujeto a los requisitos de las leyes de protección de datos y privacidad o a la eliminación temprana.

2.2. Notificaciones y mensajes de correo electrónico

Los investigadores deben ser conscientes de las preocupaciones sobre la privacidad y la intrusión, y no realizar envíos de correo electrónico no solicitados a los potenciales entrevistados, incluso en países donde todavía está permitido por la ley, a menos que estas personas tengan una expectativa razonable de ser contactadas para la investigación.

Los investigadores deben reducir las molestias que tales envíos de correo electrónico pueden provocar al destinatario indicando claramente su propósito en el asunto y manteniendo el mensaje lo más breve posible.

El mismo requisito se aplica a otros mensajes electrónicos (por ejemplo, mensajería instantánea, SMS, etc.). Vea la **sección 4.4** sobre dispositivos móviles interactivos.

2.2.1. Requisitos específicos

El principio general es que los investigadores de mercado no utilizarán mensajes de correo electrónico no solicitados para reclutar nuevos participantes para una investigación, ya sean consumidores o empresas.

Los investigadores están obligados a verificar que las personas contactadas por correo electrónico para la investigación podían esperar razonablemente ser contactadas para la misma. Tal acuerdo se puede dar por hecho cuando se dan lugar ***todas*** las condiciones siguientes:

i) Existe una relación previa entre las personas contactadas y la organización que investiga, el cliente o los dueños de la lista que proporcionan muestras para la investigación (identificados estos últimos como tales);

ii) Los individuos tienen una expectativa razonable, basada en una relación preexistente, de que pueden ser contactadas para una investigación;

iii) En cada invitación se ofrece a las personas la opción de ser eliminadas de futuros contactos electrónicos de una manera clara y concisa, y esto debe ser gratuito y fácil de realizar;

iv) La lista de invitados excluye a todas las personas que con anterioridad han tomado las medidas adecuadas y oportunas para solicitar al propietario de la lista su eliminación de la misma.

Los investigadores no deben utilizar ningún subterfugio para obtener direcciones electrónicas de potenciales participantes, como por ejemplo la recolección de direcciones de correo electrónico de dominios públicos, o con el pretexto de alguna otra actividad, o el

uso de tecnologías o técnicas para captar direcciones de correo electrónico sin el conocimiento de los individuos.

Los investigadores no deben usar direcciones de respuesta de correo electrónico falsas o engañosas en la búsqueda de participantes a través de internet.

Los investigadores pueden enviar invitaciones no solicitadas a los participantes de investigaciones de empresa a empresa, siempre y cuando cumplan con los puntos 3 y 4, así como con las políticas sobre spam de sus proveedores de servicios de internet y correo electrónico. Esto se aplica también a las direcciones de correo electrónico de profesionales cuyos datos hayan sido publicados en el dominio público; por ejemplo, en listas de médicos o abogados.

Cuando los investigadores reciben una lista de correo electrónico de los clientes o propietarios de la lista, deben hacer que los clientes o proveedores de la lista confirmen por escrito y/o en algún formato tangible que los individuos litados tienen una expectativa razonable de recibir contacto vía correo electrónico, como se definió anteriormente.

Una buena práctica es que los investigadores mantengan copias de los mensajes de correo electrónico y otros documentos recibidos de los encuestados en los que acuerdan o restringen el uso o el acceso a su información personal. Esto es un requisito legal en algunos países, entre los que se cuentan: todos los estados miembros de la UE (Unión Europea), Argentina, Australia, Canadá, Nueva Zelanda, y las compañías estadounidenses que participan en los programas Safe Harbour de Estados Unidos y la Unión Europea.

2.3. Políticas de privacidad

Los investigadores deben publicar el documento sobre su política de privacidad en su sitio web. Debe ser claro, conciso y fácil de localizar.

2.3.1. Contenido recomendado

La política de privacidad debe estar disponible a través de un enlace desde cada encuesta online y debe informar a participantes en la investigación de cómo su información personal se utiliza, mantiene segura y las condiciones, si las hubiere, en las que puede ser revelada a un tercero. Algunos elementos de la política serán comunes para todas las encuestas **(véase la sección A: elementos comunes para todas las declaraciones de privacidad).** Otros aspectos variarán dependiendo de los métodos de muestreo utilizados **(véase la sección B: tres elementos adicionales).** También puede ser necesario incluir información relacionada con la privacidad que sea relevante para un estudio en particular en la invitación a participar en el mismo, además de las declaraciones generales de la política de privacidad.

El orden y la redacción de la declaración de privacidad es una cuestión de elección. ESOMAR recomienda que las empresas consideren el uso de la notificación sobre privacidad en tres capas: la primera capa da un resumen conciso sobre la política de privacidad, la segunda da una breve visión general de la investigación de mercado y las prácticas de privacidad de la empresa, y la tercera capa proporciona la política detallada de privacidad de la empresa. El Apéndice 2 incluye un ejemplo de una declaración de privacidad en capas.

Elementos comunes para todas las declaraciones de privacidad

Declaración sobre **quién** está realizando la investigación. Podría incluir un hipervínculo a la página web de la compañía de la investigación para obtener más información.

Para quiénes: explicación de que cada encuesta contendrá información acerca de la identidad de la empresa/organización para la que se está llevando a cabo la investigación, a menos que haya buenas razones para no proporcionar esta información. Si la empresa de investigación está proporcionando un servicio de recolección de datos, se debe facilitar la identidad y datos de contacto de la empresa que recibe los datos de carácter personal y por lo tanto es el "controlador de datos", en terminología de la UE. Para obtener orientación adicional sobre este tema, vea las **Notas** sobre la aplicación del Código Internacional ICC/ESOMAR en el Artículo 4.

Garantizar que la identidad de los entrevistados y sus respuestas se tratarán como **confidenciales** y únicamente se utilizarán con fines de investigación en todas las circunstancias, a menos que el entrevistado solicite explícitamente o esté de acuerdo con la comunicación de dichos datos a un tercero.

No le engañaremos. Por ejemplo: “Al obtener su cooperación no le engañaremos acerca de la naturaleza de la investigación o los usos que daremos a los resultados”.

Voluntariedad. Por ejemplo: “Al igual que con todas las formas investigación de mercado, social y de opinión, su cooperación es voluntaria. No intentamos obtener ningún dato personal de o sobre usted sin su previo conocimiento y acuerdo”.

Retractación. Por ejemplo: “Usted tiene derecho a retirarse en cualquier etapa de la entrevista, o posteriormente, a solicitar que parte o la totalidad de la grabación de su entrevista sea destruida o borrada. Siempre que sea razonable y práctico cumpliremos dicha solicitud”.

Identificación y tecnologías de rastreo: descripción clara de las tecnologías y métodos de procesamiento que se están utilizando para la investigación. Además de un *software* específico que se puede descargar al ordenador o dispositivo que utiliza el entrevistado, la mayoría de los sondeos por internet pueden detectar información sobre el entrevistado sin su conocimiento, como el tipo de navegador, su nombre de usuario y la identificación del equipo. La descripción deberá exponer claramente qué información se captura y se utiliza durante la entrevista (por ejemplo, datos recogidos con fines de seguimiento para mostrar una página optimizada para el navegador en uso), y si alguna parte de esta información está siendo retenida como parte de la encuesta o registros administrativos.

***Cookies*:** información clara sobre su uso en el estudio, y en caso de usarlas, por qué; por ejemplo, "Nosotros utilizamos *cookies* y otros sistemas similares con moderación y sólo para el control de calidad, validación y para evitar molestias por reiteración de preguntas”. Si se está usando *cookies*, es aconsejable incluir un recordatorio de que el entrevistado tiene control sobre si su equipo acepta las *cookies*; por ejemplo, “Asegúrese de que su navegador está configurado para que le avise cuando se haga uso de las *cookies*. También puede borrar las cookies ajustando la configuración de su navegador".

Niños: exposición clara acerca de cómo se llevarán a cabo las entrevistas con los niños; por ejemplo, “En las investigaciones con niños, solicitaremos el permiso verificable de un progenitor, tutor legal u otro responsable legal del niño antes del comienzo de una entrevista”.

Cómo contactar con nosotros: por ejemplo, “Facilitaremos una dirección postal, una dirección de correo electrónico y/o un número de teléfono gratuito en el que los encuestados pueden contactar con nosotros para discutir cualquier tema acerca de una encuesta en concreto”.

Medidas de seguridad: por ejemplo, *“Nuestro sitio web cuenta con medidas de seguridad para evitar la pérdida, mal uso y alteración de la información que usted nos proporciona. Sólo empleados autorizados tienen acceso a la información para el análisis de datos y el control de calidad. Si se transfieren datos personales a terceros, nos aseguramos de que empleen medidas de seguridad a un nivel equivalente como mínimo”.*

Correo no solicitado: política estatal sobre el envío de correo postal no solicitado o la transmisión de direcciones de correo electrónico a otras personas con este propósito.

Acceso a información personal[1]: cómo tener acceso, y si fuera necesario, corregir la información almacenada sobre un entrevistado.

Dónde se conservan y/o procesan los datos, ya que muchas empresas operan a nivel mundial y pueden captar los datos en un país y procesarlos en otro.

Domicilio social de la organización.

Fecha en que la política fue actualizada por última vez.

Tres elementos adicionales que deberán incluirse en función de las metodologías utilizadas para contactar con potenciales entrevistados.

*i. Cuando el entrevistado está siendo **invitado a participar en un panel** para realizar estudios de mercado, o ya está participando:*

El proceso de inscripción: describir el proceso de registro.

La base de datos del panel: describir la información que se almacenará en una base de datos de participantes en la investigación, para la gestión del panel, control y selección de muestras, así como el proceso para actualizarla, borrarla o eliminar todos los identificadores personales.

La frecuencia de contacto: dar una indicación de lo que implica la participación; por ejemplo, con qué frecuencia, durante cuánto tiempo.

Sistema de identidad con contraseña: si se utiliza, describir cómo funciona y qué seguridad ofrece.

Políticas de **suscripción y baja** para comunicaciones distintas de las encuestas como el mantenimiento del panel o programas de incentivos. Declarar qué comunicaciones se enviarán, cuáles son opcionales y aclarar cualquier posible comunicación en nombre de terceros.

[1] Nota para los investigadores: en Europa, Australia, Canadá, Nueva Zelanda y otras jurisdicciones con leyes de privacidad detalladas, todo individuo tiene derecho legal a acceder a su información personal almacenada por organizaciones, sujeto a ciertas condiciones. Los derechos individuales de acceso también se aplican a las empresas estadounidenses que participan en los programas Safe Harbour de Estados Unidos y la Unión Europea.

Recompensa: explicar cualquier programa de incentivos y si esto forma la base para un contrato.

*ii. Cuando el investigador ha obtenido **una lista de direcciones de correo electrónico** para enviar invitaciones para participar en una encuesta:*

Fuente de información: exposición clara sobre la procedencia de la dirección de correo electrónico o sobre si ésta se incluirá en la información dada en la propia encuesta. Una declaración de que el proveedor de la lista ha demostrado al investigador que las personas que forman parte de la lista tienen una expectativa razonable de recibir contactos por correo electrónico.

***Spam*:** no enviará deliberadamente correo electrónico a personas que no hayan accedido a ayudar en la investigación y debe incluir un mecanismo para que el investigador elimine su nombre de las futuras encuestas o para notificar al proveedor de la lista de direcciones de correo electrónico.

Sistema de identidad con contraseña: si se utiliza, describir cómo funciona y qué seguridad ofrece.

Interrupción y reinicio del proceso de entrevista: si esto es posible explicar cómo, y qué información se almacena para hacerlo posible.

iii. Encuestas de intercepción en las que el entrevistado es seleccionado como muestra "1 de N" de los visitantes a un sitio web, o técnicas similares:

Explica la técnica de intercepción: por ejemplo, selección aleatoria.

Sistema de identidad con contraseña: si se utiliza, describir cómo funciona y qué seguridad ofrece.

Interrupción y reinicio del proceso de entrevista: si esto es posible explicar cómo, y qué información se almacena para hacerlo posible.

Procesamiento invisible: describir cualquier tratamiento invisible usado para realizar la intercepción de los encuestados, o redireccionarlos a la encuesta.

Véase el Apéndice 2 — Ejemplo de política de privacidad

2.4. Niños y jóvenes

Los investigadores deben ser sensibles a las preocupaciones de los padres, los grupos de consumidores y los legisladores acerca de la posible explotación de los niños y los jóvenes en internet. Se deben tomar todas las medidas razonables para asegurar la obtención del permiso veraz y explícito de un progenitor o tutor legal para invitar a un niño a participar en una encuesta, aunque se reconoce que en este momento no es posible identificar con certeza a niños y jóvenes a través de internet.

2.4.1. Obtención de permisos

Los investigadores deben respetar todas las leyes y códigos nacionales relacionados específicamente con los niños y los jóvenes teniendo en cuenta que la definición de la edad de los niños varía entre países. Cuando no hay una definición nacional específica, la Guía ESOMAR sobre **entrevistas a niños y jóvenes** recomienda que los menores de 14 años sean tratados como "niños" y los de 14-17, como "jóvenes" ya que la investigación de

mercado se basa en las ciencias sociales y reconoce diferentes etapas de desarrollo mental y psicológico[2].

Antes de entrevistar a niños, los investigadores deben asegurarse de obtener el permiso de un progenitor, tutor legal u otra persona legalmente responsable del niño (en lo sucesivo, “padre”).

Los cuestionarios en sitios web dirigidos a niños deben exigir al niño que facilite su edad antes de solicitarle cualquier otra información personal. Si la edad es inferior a la definición acordada a nivel nacional, no se debería invitar al niño a facilitar más información personal hasta obtener el permiso adecuado. Esta notificación debe ser clara y evidente, incluir una explicación del asunto y hacer referencia al hecho de que el permiso se verificará cuando sea necesario. El proveedor que lleva a cabo la investigación debe proporcionar a los padres (o enviar por correo electrónico) una solicitud de su autorización.

Cuando la información personal obtenida de los niños sólo se utilice con fines de investigación y no se cedan datos personales para ningún otro propósito, el permiso puede ser enviado por el padre por correo electrónico u otro método adecuado que cumpla con las leyes pertinentes y los códigos nacionales.

Deben tomarse medidas razonables para comprobar que realmente han dado su consentimiento mediante seguimiento a través de correo electrónico, por carta o teléfono (por ejemplo), tras haber solicitado al niño los datos de contacto de sus padres para solicitar permiso.

No se requiere permiso previo de los padres para:

- Recolectar la dirección de correo electrónico de un niño o un padre exclusivamente para avisar de la recolección de datos y solicitar permiso.
- Recolectar la edad del niño para fines de selección y exclusión. Si este filtrado conduce a la decisión de que el niño es elegible para la entrevista, entonces se ha de solicitar permiso a sus padres para continuar con la entrevista.

Siempre que sea posible, se debe evitar hacer preguntas a niños o jóvenes sobre temas que se consideren delicados, y en cualquier caso se deben manejar estas cuestiones con sumo cuidado; por otro lado, deben tomarse precauciones razonables para garantizar que los entrevistados no se vean afectados negativamente como resultado de participar en un proyecto de investigación.

No se debe obtener a través de los niños información personal relativa a otras personas (por ejemplo, los padres).

Cuando los investigadores se dispongan a seleccionar a niños para encuestas recurrentes, deben considerar:

- Buscar a padres con niños de la edad requerida, y gestionar el proceso de la investigación con el acuerdo y la supervisión de la actividad por parte del padre.
- Habilitar la protección de las encuestas con una contraseña que sólo conozca el padre, lo que significa que éste debe estar de acuerdo para introducirla antes de que el niño pueda participar en la investigación.

[2]Nótese que la definición de la edad de “niño” varía en cada país y es, por ejemplo, “menor de 16 años” en el Reino Unido.

Cuando sea necesario, los investigadores deben consultar con su asociación nacional de investigación o la Guía de ESOMAR para obtener orientación.

3. CUESTIONES DE REGULACIÓN

3.1. Datos personales y direcciones IP

La legislación sobre privacidad de datos se aplica únicamente a los datos personales identificativos, no a conjuntos de datos en los que es imposible identificar a un individuo. Bajo estas leyes, los interesados normalmente tienen derecho a acceder a los datos almacenados en una forma que permita identificarles, a ver los registros almacenados a su nombre y a solicitar su rectificación si hay errores. Este derecho de acceso no se aplica una vez que los elementos de identificación personal se han eliminado del conjunto de datos.

La inclusión en un conjunto de datos de, por ejemplo, un nombre, dirección, dirección de correo electrónico o teléfono crearía datos personales identificativos. También podría ocurrir si hubiera una ubicación geográfica exacta o código postal que pueda ser combinado con otra información del conjunto de datos. Los investigadores deben tomar precauciones para asegurar que los conjuntos de datos recogidos para la investigación de mercado que contengan datos personales identificativos se almacenan de forma segura y sólo se utilizan para la investigación de mercados.

Una dirección IP es necesaria para conectarse a internet y normalmente es registrada por sitios web y por el *software* de servidores y ordenadores personales conectados a internet. En general, el usuario es incapaz de evitar que se registre la dirección IP. Una dirección IP puede convertirse en un dato personal en combinación con otros datos de identificación, pero no hay consenso internacional sobre el estado de las direcciones IP. A menudo pueden identificar a un ordenador u otro dispositivo único, pero puede o no identificar a un usuario. En consecuencia, ESOMAR exige el cumplimiento de la ley y/o regulación nacional y/o local si ésta clasifica las direcciones IP como datos personales.

3.2. Jurisdicción nacional

El Código Internacional ICC/ESOMAR se debe aplicar en el contexto de la legislación correspondiente y de las normas o reglas más estrictas que puedan ser necesarias en un mercado específico. Sin embargo, aún se están definiendo a nivel internacional las responsabilidades y los requisitos sobre privacidad de datos.

La recomendación de ESOMAR a los investigadores es que consideren el punto de vista del entrevistado y que, al participar en estudios, los entrevistados asumirán que se cumple con los requisitos legales de su propio país. Cuando es posible conocer el país de residencia de los encuestados, el investigador debe seguir los requisitos legales de ese país ya que los requisitos en la UE no son exactamente los mismos; por ejemplo, Alemania e Italia tienen requisitos más estrictos que otros estados miembros.

3.2.1. Recopilación de datos a distancia y transferencia de datos

Se recomienda a los investigadores aclarar en qué país o países pretenden realizar la investigación, sobre todo si difiere del país donde esté establecida la empresa de investigación. El idioma del sitio web o el cuestionario tendrá un papel a la hora de aclarar el país o países objetivo. También se pueden especificar en la política de privacidad, que debería cumplir con las regulaciones del lugar en el que se ubica la compañía de investigación.

En la primera página de la encuesta, en el punto donde se solicita el consentimiento a los entrevistados, éstos deben ser informados sobre la ley o leyes bajo la que se recolectarán los datos, y también se aclarará las condiciones en las circunstancias en las que no se conoce el país de residencia del entrevistado; por ejemplo, en encuestas de satisfacción del cliente a nivel mundial o en la observación de un sitio web en el que los encuestados pueden residir en cualquier lugar. Para investigaciones que no utilicen un panel de encuestados (incluyendo intercepción web), la práctica antes mencionada es la más apropiada. Para paneles de investigación, es una práctica común informar a los encuestados de la ley en vigor en la inscripción al panel y en las políticas de privacidad.

En la UE, ESOMAR requiere que el investigador que recoge los datos (el controlador de datos) cumpla con la ley del país en el que está establecido y, si se recogen datos en varios países, también debe cumplir con las leyes de los países en los que se lleva a cabo la recolección de datos. La ley de la UE relativa a esta área todavía está siendo clarificada y ESOMAR hará un seguimiento de su evolución.

Antes de que los datos personales se transfieran desde el país de recolección a un tercer país, el investigador debe asegurarse de que la transferencia de datos es legal, y que se adoptan medidas razonables para garantizar una seguridad adecuada para mantener los derechos de protección de datos de los individuos. Esto también se aplica en caso de utilizar un servidor “remoto” en un país diferente para recopilar datos del entrevistado, o si se procesan en una “nube” internacional.

El investigador debe explicar este proceso en su política de privacidad (véase el **contenido recomendado para la política de privacidad** y el ejemplo de política de privacidad) y proveer las garantías apropiadas para proteger los datos personales cuando se solicite permiso al entrevistado para la transferencia de datos.

Se recomienda el uso de cláusulas contractuales estándar que las empresas pueden utilizar para asegurar las garantías adecuadas cuando los datos personales se transfieren desde la UE a países no comunitarios, por ejemplo, las desarrolladas por la Comisión Europea y la ICC.

3.3. Registro

En países con legislación sobre protección de datos, normalmente se requiere que los gestores de datos se registren ante las autoridades. Los investigadores deben registrar sus actividades con las autoridades competentes. Para más información sobre el impacto de las leyes de protección de datos en la investigación de mercados en países como Alemania, el Reino Unido y los Estados Unidos de América, véase la **sección 6.**

3.4. Seguridad

Los investigadores y sus subcontratistas deben tomar precauciones adecuadas para proporcionar el más alto nivel de seguridad en la recolección de datos de carácter personal y, en particular, de cualquier información sensible que la legislación de protección de datos considere merecedora de especial cuidado (véase la sección 6).

Los investigadores también deben tomar medidas adecuadas para asegurarse de que cualquier información confidencial que les es proporcionada por los clientes u otros está protegida contra el acceso no autorizado (por ejemplo, por un cortafuegos o *firewall* y control por contraseña).

Los clientes deben estar plenamente informados y ser conscientes de los riesgos potenciales de publicar datos de información confidencial en las encuestas de internet, y se les debe requerir la aplicación de procedimientos de seguridad estrictos. Por norma general, los conceptos e ideas no se pueden proteger utilizando sólo medios tecnológicos o declaraciones después de distribuirlos, incluso cuando están protegidos por acuerdos de confidencialidad; estos datos son fáciles de reenviar y es imposible retirarlos de la circulación una vez publicados.

3.4.1. Gestión de la seguridad

Los investigadores deben utilizar tecnologías de seguridad para proteger los datos personales recogidos o almacenados en sitios web o servidores, utilizando sistemas seguros de cifrado como el modo de encriptación SSL (*secure socket layer*) o seguridad de nivel equivalente. Si la legislación nacional aplicable lo requiere, los datos “en reposo” (definidos por lo general como todos los datos en almacenamiento, con la excepción de los datos que recorren la red con frecuencia o que residen en la memoria temporal) también deben ser cifrados a un nivel adecuado.

La seguridad de los datos también es importante para prevenir el acceso no autorizado, la manipulación o la revelación de datos de carácter personal durante la transferencia de datos. El proveedor que realiza la investigación debe tener políticas y procedimientos claros para gestionar la seguridad. El acceso a los datos debe ser restringido y permitido solamente en base a una necesidad de conocimiento. El investigador debe asegurarse de que todos los gerentes y personas clave que manejan estos datos confidenciales han firmado la confirmación de que seguirán el Código ICC/ESOMAR y de que no revelarán datos personales.

Si el almacenamiento temporal de los datos recogidos se lleva a cabo en un servidor que es operado por un subcontratista o proveedor de servicios, el investigador debe obligar por contrato a los subcontratistas a tomar las precauciones necesarias para prevenir el acceso no autorizado mientras que los datos están almacenados o durante la transferencia de los mismos. Los datos identificativos que estén en poder del proveedor de servicios deben ser eliminados lo antes posible.

4. USO DE TECNOLOGÍAS ONLINE DE IDENTIFICACIÓN Y SEGUIMIENTO EN LA INVESTIGACIÓN

Las tecnologías *online* de identificación y seguimiento se han desarrollado con rapidez en los últimos años a escala mundial. Si bien muchas de esas tecnologías están diseñadas para mejorar la experiencia informática del usuario, han conducido a un estrecho control

por parte de grupos de defensa de la privacidad que están preocupados por la posibilidad de que organizaciones o individuos identifiquen y monitoricen el comportamiento online de las personas sin su conocimiento.

Las tecnologías online de identificación y seguimiento desarrolladas para la investigación de mercados, social y de opinión se aplican para mejorar la integridad de los paneles de investigación y las técnicas de muestreo, ya que el investigador y el participante, por lo general, sólo interactuarán online.

ESOMAR, trabajando en estrecha colaboración con CASRO y con la industria global de investigación, ha establecido directrices claras para la investigación de mercados, social y de opinión utilizando las tecnologías *online* y, al hacerlo, promueve los estándares profesionales, las buenas prácticas y las relaciones respetuosas con quienes participan en la investigación.

4.1. Tecnologías de identificación y rastreo para la investigación de mercados, social y de opinión

Las tecnologías de identificación y rastreo son las tecnologías utilizadas para identificar, validar y realizar un seguimiento de los entrevistados o de la actividad de los mismos para la investigación en internet. Los usos de estas tecnologías pueden incluir el seguimiento de anuncios, el control de cuotas del estudio, la prevención de fraude y la investigación de la conducta. Los términos *spyware* (programas espía) y *malware* (programas maliciosos) son ampliamente utilizados para describir el uso inaceptable de las tecnologías de seguimiento e identificación *online*. La investigación de mercados, social y de opinión no deben utilizar la tecnología en formas que puedan clasificarse como *spyware* o *malware*. Esta sección establece los usos aceptables e inaceptables de esta tecnología y ofrece orientación sobre tipos específicos de tecnología.

4.1.1. Tecnologías específicas

Las tecnologías de identificación y seguimiento para la investigación incluyen:

Cookies

Las *cookies* son pequeños archivos de texto almacenados en un ordenador por un sitio web que le asigna una ID de usuario numérica y contiene cierta información sobre su navegación online. Las *cookies* se utilizan en los sitios de la encuesta para ayudar a los investigadores a reconocer al entrevistado como un usuario anterior, así como para otros controles de la encuesta o para funciones de calidad. Los datos almacenados en las *cookies* no son personales y pueden ser rechazadas o eliminadas a través de la configuración del navegador.

Los investigadores deben incluir información clara, concisa y visible acerca de si se utilizan *cookies*, y en caso afirmativo, por qué (véase la sección sobre la **guía de política de privacidad**). Si se utilizan *cookies*, el investigador debe asegurarse de que se incluye una descripción de los datos recogidos y su uso en la política de privacidad de la organización investigadora.

La legislación de la UE aprobada en 2009, que se traducirá en legislación nacional en 2011, establece que se puede almacenar una *cookie* en el ordenador de un usuario, o ser accesible desde dicho ordenador, sólo si el usuario "*ha dado su consentimiento, después de haber recibido información clara y completa*". Existe una excepción cuando la *cookie* es

"*estrictamente necesaria"* para la prestación de un servicio "*solicitado expresamente*" por el usuario, asegurándose de que a los usuarios de sus sitios web se les proporcionó "*información clara* y *completa sobre los fines de almacenamiento de, o el acceso a, esa información*" y, en definitiva, proporcionar al usuario la posibilidad de impedir dicho almacenamiento de, y/o el acceso a dicha información. Los investigadores que realicen investigaciones en la UE deben consultar las actualizaciones sobre si la legislación nacional requiere que obtengan consentimiento para utilizar *cookies*.

Los investigadores que recojan datos de un panel de investigación y que monitoricen el comportamiento de los encuestados en todo internet deben cubrir estos aspectos en su declaración de privacidad (véase la sección sobre datos de **paneles de investigación**) y también deben explicar esta actividad en la página de inscripción del panel con el fin de asegurar de que los encuestados tienen claro qué información se recoge sobre ellos.

Cookies de flash

Las *cookies* de *flash* se originan en la codificación encontrada en el reproductor *flash* de Adobe, una aplicación utilizada en la gran mayoría de los sitios web comerciales que cuentan con animaciones o videos.

Si se utiliza en una técnica de investigación, los investigadores deben notificar el uso de esta información, dar detalles sobre la forma de eliminarlos en su política de privacidad (ver la sección sobre guía de política de privacidad) y obtener el consentimiento previo de los encuestados. Además, se están desarrollando otras técnicas como el almacenamiento local HTML5 que no son fáciles de eliminar.

ID de dispositivo (también conocido como huella digital o ID de la máquina)

Estas son tecnologías que implementan un algoritmo que analiza un gran número de características técnicas y la configuración para generar un identificador único que puede denominar a un ordenador concreto, produciendo una identificación del dispositivo o de la máquina.

Tecnologías de agente activo

Las tecnologías de agente activo para la investigación son dispositivos de *software* o *hardware* que capturan el comportamiento de entrevistado en segundo plano; por lo general se ejecutan simultáneamente con otras actividades. Estas incluyen:

- *Software* de escritorio descargado directamente al ordenador de un usuario, que se utiliza con el único fin de alertar a potenciales participantes sobre la descarga de contenidos de la encuesta o para hacer preguntas de la encuesta. No hace seguimiento de los interesados cuando navegan por internet y todos los datos recogidos son suministrados directamente por el usuario;
- *Software* de seguimiento que puede capturar los datos de comportamiento online actual del sujeto como puedan ser accesos a páginas web, páginas web visitadas, transacciones realizadas online, formularios cumplimentados online, ratios de *click-through* o impresiones publicitarias y compras online. Este *software* también tiene la capacidad de capturar información sobre el correo electrónico del interesado y sobre otros documentos almacenados en un dispositivo como el disco duro. Parte de esta

tecnología ha sido etiquetada como *spyware* (programas espía), en particular cuando la descarga o instalación se produce sin el pleno conocimiento del interesado y sin contar con su consentimiento.

El uso de *spyware* por parte de los investigadores está estrictamente prohibido.

4.1.2. Revelación de tecnologías de identificación y seguimiento

Las revelaciones sobre el uso de tecnologías de identificación y seguimiento deben ser transparente y realizarse antes o en el momento de la recolección de datos. Para proyectos individuales, tales revelaciones pueden formar parte de la invitación a la participación y podría aplicarse una política de privacidad específica para el proyecto. Si una determinada tecnología se utiliza en varios o todos los proyectos, la información sobre la tecnología debe formar parte de la política de privacidad general para entrevistados online de la organización investigadora. Los enlaces a políticas de privacidad para proyectos específicos y/o generales deben ser fácilmente accesibles para los entrevistados (por ejemplo, en invitaciones a participar en estudios y/o en la página de destino de las encuestas *online*).

El Apéndice 2 presenta ejemplos de declaraciones informativas para el uso de:

- Cookies
- *Cookies* para *flash*
- *Cookies* y aplicaciones de *software* para seguimiento
- Identificación de dispositivo/máquina

4.2. Prácticas que las organizaciones de investigación debieran adoptar

A continuación, se describen algunas prácticas que deberían adoptar los investigadores que implementan tecnologías de identificación y seguimiento para investigación. Los investigadores que adopten estas prácticas y no tomen parte en cualquiera de las prácticas consideradas inaceptables **(Sección 4.3 de esta guía)** no serán considerados usuarios de *spyware*.

La transparencia es crucial. Los investigadores deben ofrecer a los interesados información sobre las tecnologías de identificación y seguimiento y otro *software* de manera abierta y oportuna. Esta comunicación debe proporcionar información acerca de cómo el investigador utiliza y comparte la información del interesado

i) Sólo después de recibir el permiso del titular de los datos (permiso paternal o del tutor legal en el caso de los niños) si cualquier *software* de investigación pueden descargar en el ordenador de la persona, PDA u otro dispositivo[3]

ii) Los investigadores deben comunicar claramente a los participantes los tipos de datos que están siendo recogidos y almacenados (si así fuera) por una tecnología de identificación y seguimiento concreta.

[3] Este requisito y muchos otros de los reseñados en esta sección no se aplican a ordenadores o equipos de captura de datos proporcionados al entrevistado por el investigador, caso en el que el investigador sigue siendo el propietario y controlador del dispositivo.

iii) La divulgación para permitir que los entrevistados desinstalen fácilmente el *software* de la investigación sin perjuicio o daño para ellos o para sus equipos informáticos también es necesaria.

iv) La información personal sobre el entrevistado no se debe utilizar para fines secundarios ni compartir con terceros sin su consentimiento expreso.

v) Los investigadores deben asegurarse de que la participación es una actividad consciente y voluntaria. En consecuencia, nunca se debe utilizar incentivos para ocultar o disfrazar la aceptación del uso de tecnologías de identificación y seguimiento para la investigación.

vi) Los investigadores deben asegurarse de que existe un método para recibir consultas de los usuarios finales.

vii) De forma sistemática y continua, en consonancia con las políticas establecidas por la empresa de la investigación, los interesados que participan en el panel de investigación deben recibir una notificación clara y periódica de que están activamente registrados como participantes, a fin de garantizar que su participación es voluntaria. Los investigadores deben proporcionar a los encuestados que participan en un panel de investigación un método definido claramente para desinstalar el *software* de seguimiento sin causar perjuicio al interesado.

viii) Cuando se instalen actualizaciones de *software* para corregir errores, problemas de seguridad o nuevas versiones que no expanden el alcance de los datos personales que se recogen, si no hay respuesta a la notificación después de un tiempo razonable (30 días), se puede asumir que el participante está de acuerdo. Esta asunción debe estar presente en la declaración de privacidad. Si el investigador decide reducir el período de notificación de 30 días para una aplicación específica, debe mencionarlo explícitamente en un lugar destacado de su sitio web.

El manejo responsable de los datos es fundamental. Los investigadores deben tomar medidas para proteger la información recolección de los entrevistados.

i) Los datos personales o sensibles no deben ser recogidos a menos que se obtenga consentimiento del entrevistado. Si no se dispone de dicho consentimiento y la recolección es inevitable, los datos deben ser destruidos inmediatamente. De no ser posible, estos datos deben recibir el mayor nivel de seguridad y no se deben recuperar ni utilizar para ningún otro fin.

ii) Los investigadores deben establecer garantías que reduzcan al mínimo el riesgo de amenazas a la seguridad de los datos y a la privacidad de la persona interesada.

iii) Es importante que los investigadores comprendan el impacto de su tecnología en los usuarios finales, especialmente cuando su *software* se descarga en un paquete con otros productos de *software* similares.

iv) Los investigadores deben hacer todos los esfuerzos posibles para asegurar que estos productos (ya sean de forma gratuita o no) sean seguros y no causen riesgos indebidos de privacidad o seguridad de los datos.

v) Los investigadores también deben hacer una gestión proactiva de la distribución del software y controlar con firmeza su canal de distribución, y buscar signos que sugieran circunstancias inusuales, tales como altas tasas de rotación.

4.3. Prácticas inaceptables

A continuación, se presenta una lista de prácticas inaceptables que los investigadores deben prevenir o prohibir estrictamente. Se considera que un investigador está utilizando *spyware* cuando no adopta todas las prácticas establecidas a continuación:

i) Descargar *software* sin obtener el consentimiento del interesado;

ii) Descargar *software* sin dar un aviso detallado y sin revelar qué tipo de información se recolectará del interesado, y cómo puede ser utilizada dicha información. Esta notificación debe ser clara, concisa y evidente;

iii) Recolectar información que identifique al titular de los datos sin obtener su consentimiento;

iv) Utilizar *keyloggers* (aplicaciones o dispositivos que registran el tecleo del usuario) sin obtener el consentimiento del interesado;

v) Instalar *software* que modifique la configuración del ordenador del interesado más allá de lo que es necesario para llevar a cabo en la investigación;

vi) Instalar *software* que desactive los programas *antispyware*, antivirus o antispam, o que tome el control del ordenador o dispositivo del sujeto;

vii) No hacer todos los esfuerzos que sean razonables para garantizar que el *software* no cause ningún conflicto con los principales sistemas operativos y no provoque que otro *software* instalado se comporte de forma errática o inesperada;

viii) Instalar *software* que vaya oculto dentro de otros programas descargables o que sea difícil de desinstalar;

ix) Instalar *software* que muestre contenido publicitario, con la excepción del *software* para realizar pruebas de publicidad;

x) Instalar actualizaciones de *software* sin notificarlo a los usuarios y dar al participante la oportunidad de darse de baja;

xi) Cambiar la naturaleza de las tecnologías de identificación y seguimiento sin notificarlo al usuario;

xii) No informar al usuario de cambios en las prácticas de privacidad relacionadas con mejoras del *software*;

xiii) Rastrear el contenido del correo electrónico del interesado;

xiv) Si el navegador del entrevistado está en modo privado, el investigador no debe rastrear el comportamiento a menos que disponga de consentimiento expreso;

xv) Cuando el entrevistado se encuentre en un sitio con autenticación segura (SSL, por ejemplo), el investigador no debe recolectar datos personales a menos que disponga del consentimiento del entrevistado.

4.4. Dispositivos móviles interactivos y teléfonos inteligentes (*smartphones*)

Los dispositivos móviles interactivos y los teléfonos inteligentes son capaces de combinar las características de un teléfono móvil y un navegador de internet. ESOMAR ha publicado directrices tanto sobre investigación online (el presente documento) como sobre

investigación usando teléfonos móviles. La elección de la guía a seguir para dispositivos móviles interactivos depende de si el investigador contacta con el encuestado utilizando los servicios de un teléfono móvil (es decir, llamando o enviando mensajes de texto) o el uso de servicios de internet (correo electrónico, enlaces web o aplicaciones descargadas). Si se utiliza una combinación de ambos métodos (por ejemplo, teléfono móvil de contacto y navegador de internet para responder), entonces se deberían aplicar las partes correspondientes de las dos guías.

4.4.1. Uso de dispositivos móviles interactivos

Cómo ponerse en contacto

Si los investigadores contactan con individuos utilizando metodologías online, no deben enviar invitaciones no solicitadas por correo electrónico u otros mensajes (por ejemplo, mensajería instantánea, mensajes de texto, etc.) a los posibles participantes, incluso en países donde todavía está permitido por la ley. Están obligados a verificar que las personas contactadas para la investigación por esos medios esperan recibir contacto para la investigación. Véase la **sección 2.2**sobre notificaciones y mensajes de correo electrónico.

Seguridad y descargas

Cuando los investigadores instalen aplicaciones en dispositivos móviles interactivos, deben cumplir con las **secciones 4.1.1** y **4.1.2** de esta guía. Los investigadores deben ofrecer a los encuestados un canal adecuado y mecanismos para dar permiso, así como un lugar donde leer más sobre la política de privacidad. Además de cumplir con la **sección 3.4**, los investigadores deben asegurarse de que los datos almacenados localmente en el dispositivo son seguros y no están disponibles para otros en caso de robo o utilización por parte de otra persona. Esto se puede lograr con el cifrado de los datos.

Coste para el entrevistado

Los encuestados que utilicen dispositivos móviles interactivos para participar en las encuestas pueden incurrir en gastos de conexión, de itinerancia o de consumo de datos al hacerlo. Si es posible, el investigador debe diseñar el estudio para que el sujeto no incurra en coste alguno. De no ser posible, el investigador debe estar dispuesto a compensar los costes a los encuestados. Cuando los entrevistados a través de dispositivos móviles interactivos se añadan a una base de datos del panel de la investigación o del muestreo, la cuestión del coste y la compensación se deben acordar durante la fase de inscripción.

Diseño adecuado

Cuando se contacta con los encuestados que se sabe están utilizando dispositivos móviles interactivos, el investigador debe asegurarse de que la encuesta se presenta en un formato adecuado y optimizado para cualquier dispositivo que los participantes podrían utilizar. También se debe dar a los entrevistados la oportunidad de dejar el estudio.

Política de privacidad

Debido a las limitaciones de espacio que presentan las pantallas de los dispositivos móviles, pueden ser difícil mostrar una política de privacidad completa. Los investigadores deben

aplicar una solución apropiada y tomar las medidas adecuadas para reducir al mínimo los costes y maximizar la comodidad de acceso a la información relevante. Por ejemplo, los investigadores deben proporcionar un enlace web a su política de privacidad con la URL (dirección web) más corta posible, y proporcionar un número de teléfono gratuito y/o una dirección postal.

Datos de localización y GPS

En la actualidad los dispositivos interactivos móviles y teléfonos inteligentes permiten capturar datos adicionales tales como información en tiempo real sobre su ubicación. La Guía de ESOMAR sobre la **Recolección pasiva de datos** aborda esta cuestión. El investigador debe contar con el permiso del entrevistado antes de procesar dicha información.

5. CUESTIONES DE METODOLOGÍA

5.1. Muestra *online*

Hay un gran número de maneras diferentes de buscar muestras online y éstas requieren diferentes tipos de consentimiento (ver **sección 2.3** sobre políticas de privacidad). Los datos personales de los miembros de un panel son almacenados por el proveedor del panel, mientras que otros tipos de muestreo normalmente no requieren que los datos personales sean retenidos por el proveedor de servicios de investigación. Si la intención es almacenar datos personales de los individuos, se ha de obtener el consentimiento apropiado ya sea antes o en el momento de la recolección.

5.2. Paneles de acceso

Esta sección se encuentra en revisión y se incluirá aquí cuando esté completa. Mientras tanto, consulte la guía existente, **26 preguntas**, que está siendo actualizada.

5.3. Detalles técnicos

El **Código de conducta ICC/ESOMAR** (artículos 4d y e) exige a los investigadores que ofrezcan todos los detalles técnicos de la metodología utilizada para la realización de un proyecto; pero la investigación online puede tener complejas metodologías y estrategias de muestreo. Esto hace que sea aún más importante que los detalles técnicos se presenten de tal forma que el estudio se pueda replicar.

La **Guía ESOMAR sobre los derechos y responsabilidades mutuos de investigadores y clientes** establece los requisitos para la presentación de informes técnicos de proyectos de investigación previstos en el Código ICC/ESOMAR. Esta guía se aplica a todos los proyectos de investigación, incluyendo la investigación online.

6. DEFINICIONES Y FUENTES DE INFORMACIÓN ÚTILES

Tres conceptos clave – los investigadores, los datos personales y el consentimiento – se tratan a continuación a los efectos de esta guía:

Investigador: se define en el Código Internacional ICC/ESOMAR como cualquier individuo u organización que lleva a cabo un proyecto de investigación de mercado o actúa como consultor en el mismo, incluyendo a aquellas personas que trabajan en las organizaciones de los clientes.

Datos personales designa cualquier información sobre una persona física identificada o identificable, es decir, un particular en lugar de una empresa u otra entidad comparable. Una persona identificable es una persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un número de identificación o las características físicas, fisiológicas, mentales, económicas, culturales o sociales.

Datos personales sensibles son cualquier información sobre el origen racial o étnico, salud o vida sexual, antecedentes penales, opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical de una persona. En los Estados Unidos de América, la información personal relacionada con la salud, sobre ingresos u otra información financiera, identificadores financieros y documentos emitidos por el gobierno o de identidad financiera también se consideran datos sensibles.

Consentimiento, significa el acuerdo libre e informado por parte del interesado para la recolección y tratamiento de sus datos personales. En la investigación de mercado, este consentimiento se puede basar en el hecho de que el entrevistado proporciona voluntariamente respuestas para un estudio una vez que se le ha proporcionado información clara sobre la naturaleza de los datos recogidos, el fin para el cual serán utilizados y la identidad de la persona u organización que recibirá los datos personales. El entrevistado podrá retirar su consentimiento en cualquier momento negándose a cooperar en una entrevista o proyecto de investigación.

Consentimiento inequívoco se utiliza en la directiva de la Unión Europea sobre procesamiento de datos personales en general. Sin embargo, dado que el término "consentimiento inequívoco" no está reconocido fuera de la UE, en esta guía se utiliza el término "consentimiento".

Legislación clave

La Directiva de la UE sobre protección de datos (oficialmente **Directiva 95/46/EC** relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos) regula el tratamiento de datos personales dentro de la UE. Todos los 27 Estados miembros de la UE han incorporado la Directiva y aprobado su propia legislación nacional de protección de datos.

La Directiva de la UE sobre privacidad y comunicaciones electrónicas (oficialmente 2009/136/EC) requiere el consentimiento previo para las comunicaciones comerciales electrónicas no solicitadas, e incluye los mensajes de texto SMS y otros mensajes electrónicos recibidos a través de cualquier terminal fijo o móvil. También requiere el consentimiento del usuario final para el almacenamiento de *cookies* en su ordenador después de haber recibido información clara y completa sobre los efectos y la función de las *cookies*. Esta Directiva endurece la Directiva existente sobre la protección de la intimidad en comunicaciones electrónicas (2002/58/EC) y su impacto dependerá de la implementación que realicen los estados miembros de la UE en sus leyes nacionales, exigida para el año 2011, así como de la influencia de la Comisión Europea.

Canadá — Ley de protección de la información personal y documentos electrónicos PIPEDA

Información personal es la información sobre una persona identificable, pero no incluye el nombre, título o dirección de negocios o número de teléfono de un empleado de una organización.

Nota: la Ley de protección de la información personal y documentos electrónicos PIPEDA (Personal Information Protection and Electronic Documents Act) considera que una dirección de correo electrónico de trabajo es información personal. La información personal sensible no está definida en la ley.

Leyes federales de los Estados Unidos de América

Las leyes de protección de datos en los EE.UU. a nivel federal son específicas del sector, ya que en la actualidad no existe una sola ley nacional sobre privacidad que sea exhaustiva y que se aplique a todas las organizaciones del sector privado.

Hay dos leyes sobre privacidad específicas que se aplican a ciertas organizaciones en los sectores financiero y sanitario: la **Ley Gramm-Leach-Bliley** (GLB) y **Ley de portabilidad y responsabilidad del seguro médico** HIPPA (Health Insurance Portability and Accountability Act).

Cuando se investiga sobre niños, se aplica la Ley para la protección de la privacidad de los niños online (**COPPA**, por sus siglas en inglés).

Leyes estatales de Estados Unidos relativas a las violaciones de la seguridad de datos

Ley 1386 del Senado de California (California Senate Bill 1386) – primera ley sobre notificación de violaciones de seguridad en los Estados Unidos de América – define la información personal como:

El nombre propio de una persona, o la combinación de la primera inicial y su apellido con uno o más de los siguientes datos, cuando el nombre o los datos no estén cifrados:

1. Número de la seguridad social.
2. Número de licencia de conducción o número de la tarjeta de identificación del Estado de California.
3. Número de cuenta, número de la tarjeta de crédito o débito, en combinación con cualquier código de seguridad requerida, código de acceso o clave que permita el acceso a la cuenta financiera de una persona.

Fuentes de información útiles

Los siguientes documentos y organizaciones proporcionan material útil y pertinente para el investigador online:

ACE: (Association Collaborative Effort): ha desarrollado un conjunto actualizado de definiciones de los conceptos clave de la búsqueda en internet;

AMSRO: Código sobre la privacidad en la investigación de mercado y social, y Principios sobre privacidad en la investigación de mercado y social;

COPPA: Ley para la protección de la privacidad de los niños online (Children's Online Privacy Protection Act);

CASRO: Código de normas y principios éticos para las encuestas de investigación (Code of Standards and Ethics for Survey Research), Sección 3. Investigación a través de internet;

ADM: Declaración para el territorio de la República Federal de Alemania en relación con el Código Internacional ICC/ESOMAR de investigación social y de mercados y sus guías;

DMA: Código de prácticas para las comunicaciones comerciales dirigidas a niños en internet;

Directrices para las encuestas online (Alemania) suscritos por ADM, ASI, BVM, DGOF;

MRS: Código y directrices para la investigación con niños y jóvenes;

Programas Safe Harbour entre EE.UU. y la Unión Europea, y entre EE.UU. y Suiza: con el fin de armonizar los distintos enfoques de privacidad de los EE.UU. y la UE y proporcionar un medio eficiente para que las organizaciones estadounidenses cumplan con la Directiva de la UE al transferir datos personales desde la UE a los EE.UU., el Departamento de Comercio de EE.UU., en colaboración con la Comisión Europea, ha desarrollado el programa legal SafeHarbour para proporcionar la información que una organización debería tener para evaluar y unirse al programa;

Comisión Europea: modelos de contratos para la transferencia de datos personales desde la UE;

ISO 26362:2009: comunicado de prensa sobre los paneles de acceso en la investigación de mercado y opinión — Vocabulario y requisitos de servicio;

ISO 20252:2006: investigación de Mercado, social y de opinión — Vocabulario y requisitos de servicio.

Orientación adicional

Los miembros que tengan dudas acerca de la aplicación de la Guía en circunstancias especiales pueden solicitar consejos contactando con el Comité de Estándares Profesionales, professional.standards@esomar.org o ESOMAR, Eurocenter 2 planta 11, Barbara Strozzilaan 384, 1083 HN Ámsterdam, Países Bajos.

Equipo del proyecto

John O Brien, consultantto ESOMAR Professional Standards Committee (Chair Project Team)
Reg Baker, COO, Market Strategies
Diane Bowers, ESOMAR Professional Standards Committee member and President of CASRO
Mike Cooke, Global Director, Online Development, GfK NOP
Jonathan Jephcott, Executive Vice President, Views Net, Synovate
Kathy Joe, Director, Professional Standards and Public Affairs, ESOMAR
Kees de Jong, CEO, Survey Sampling International
Peter Milla, Consultantto CASRO
Adam Phillips, Chair of ESOMAR Professional Standards Committee and Legal Committee
Reneé Smith, Chief Research Officer, Kantar
David Stark, Vice President, Compliance and Privacy Officer, GfK
Kevin Umeh, Past CEO at Cint USA

Apéndice 1 — Fundamentos clave del Código ICC/ESOMAR

1. Los investigadores de mercado deben cumplir con todas las leyes nacionales e internacionales pertinentes.
2. Los investigadores de mercado se han de comportar de una forma ética y no hacer nada que pueda dañar la reputación de la investigación de mercado.
3. Los investigadores de mercado tendrán especial cuidado cuando lleven a cabo una investigación con niños y jóvenes.
4. La colaboración de los entrevistados es voluntaria y se ha de basar en información adecuada y no engañosa sobre el propósito general y la naturaleza del proyecto, dada al obtener su acuerdo para participar, además del respeto a todos los términos pactados.
5. Los derechos de los entrevistados como personas deberán ser respetados por los investigadores de mercado y no se verán perjudicados o afectados negativamente como resultado directo de su cooperación en un proyecto de investigación de mercado.
6. Los investigadores de mercado nunca permitirán que los datos personales que recogen durante un estudio de mercado se utilicen para ningún otro propósito que no sea la investigación de mercado.
7. Los investigadores de mercado deberán asegurarse de que los proyectos y actividades sean diseñados, llevados a cabo, reportados y documentados con exactitud, transparencia y objetividad.
8. Los investigadores de mercado se ajustarán a los principios reconocidos de competencia leal.

Apéndice 2 — Ejemplo de política de privacidad

El ejemplo siguiente proporciona un marco de referencia para una política de privacidad. El texto no debiera tratarse como un texto exhaustivo o al día con todas las leyes nacionales o locales. Es responsabilidad del investigador asegurarse de que su política cumple con los requisitos nacionales en vigor en un momento dado y en los países en los que estén trabajando.

La política se divide en tres partes principales: la principal será una exposición clara sobre cómo se protegerá la privacidad y se utilizarán los datos; en segundo lugar, una introducción general que describe el propósito y los principios generales, y, por último, una sección detallada cubriendo todos los aspectos sobre cómo el investigador trata los datos personales.

Ejemplo:

Nivel 1

Gracias por participar en nuestro proyecto de investigación.

1. Prometemos proteger su intimidad y tratar de forma confidencial la información que nos proporcione.

2. La información que proporcione será utilizada únicamente con fines de investigación.
3. No revelaremos su información personal a terceros sin su consentimiento.
4. Nunca intentaremos venderle nada y nunca venderemos sus datos personales a nadie. Ese no es nuestro negocio. No somos agentes de *marketing* telefónico ni promotores de ventas. Somos investigadores de mercado interesados únicamente en sus opiniones y su conducta.
5. Sus decisiones sobre la participación en un estudio, responder a preguntas específicas o dejar de participar serán respetadas sin preguntas.

Haga clic aquí para obtener más información acerca de la investigación de mercados (Nivel 2)
Haga clic aquí para obtener una declaración completa de nuestras políticas de privacidad (Nivel 3)

Nivel 2

Su privacidad es importante para nosotros.

La investigación de mercados, social y de opinión cumplen una importante función en la sociedad. Las empresas y los gobiernos toman mejores decisiones a través de las encuestas de investigación. Como participante de la encuesta, sus opiniones ayudan a las empresas a desarrollar productos nuevos, perfeccionar los existentes y mejorar el servicio al cliente. Las organizaciones políticas y gobiernos también se apoyan en estudios de investigación para avanzar leyes y políticas que el público quiere o necesita.

Cuando usted participa en una investigación llevada a cabo por nuestra empresa, puede estar seguro de que protegeremos su intimidad. Ocasionalmente, puede que volvamos a contactar con usted para validar sus respuestas. Nunca vamos a engañarle sobre nosotros mismos o nuestras actividades.

Hemos desarrollado rigurosos estándares de privacidad que están recogidos en nuestra política de privacidad detallada. Varios miembros del equipo profesional de nuestra compañía pertenecen a ESOMAR, la organización mundial para facilitar una mejor investigación de mercados, consumidores y sociedades. ESOMAR establece las normas profesionales a las que se adhiere nuestra firma, y que también protegen su privacidad.

Si usted tiene alguna pregunta o preocupación sobre privacidad, por favor póngase en contacto con nuestro Director de Privacidad por correo electrónico escribiendo a (insertar dirección de correo electrónico), por teléfono llamando al (insertar el número de teléfono gratuito) o por correo postal en la siguiente dirección: (indicar la dirección postal).

Nivel 3

Política de privacidad

Fecha de creación: (insertar la fecha)

Última revisión: (insertar la fecha)

Nota para investigadores: algunos estados de EE.UU. requieren políticas de privacidad para *websites* que incluyan la información anterior. Es una buena práctica incluir la fecha de la última revisión para que los consumidores estén informados sobre cuándo hacen cambios sustanciales en sus declaraciones de privacidad las empresas.

1. La información que recogemos

Cuando nuestra empresa lleva a cabo investigaciones online, nuestras invitaciones y cuestionarios nos identifican claramente y explican el propósito o propósitos de nuestro contacto.

Cuando contactamos con usted, por lo general lo hacemos con uno de los siguientes objetivos:

1. Para invitarle a participar en un estudio;
2. Para realizar una entrevista con usted como parte de un estudio;
3. Para validar las respuestas que usted nos facilitó en una entrevista reciente;
4. Para actualizar y asegurarnos de que sus datos son correctos *(sólo aplicable a paneles de investigación).*

De manera ocasional podemos contactar con usted con uno de los siguientes propósitos:

1. Para notificarle si ha resultado ganador de un sorteo que nosotros hemos patrocinado (en el caso de que exista un incentivo);
2. Para solicitar su permiso para utilizar su información personal con un propósito que no fuese descrito cuando nos facilitó su información personal por primera vez.

Cuando participe en nuestra investigación, es posible que le preguntemos por sus opiniones personales, e información demográfica como su edad y composición del hogar. Usted puede negarse a responder a determinadas preguntas o dejar de participar en un estudio en cualquier momento. Si usted se une a nuestro panel de investigación en internet, puede rescindir su membresía en cualquier momento siguiendo las instrucciones de baja que incluimos en cada correo electrónico que le enviemos.

Nunca invitamos deliberadamente a niños menores de (*insertar edad dependiendo de los códigos de la industria y las leyes nacionales pertinentes*) a participar en estudios de investigación sin tomar medidas para garantizar el consentimiento paterno correspondiente.

2. Confidencialidad de sus respuestas e información de contacto

Combinamos sus respuestas a un estudio concreto con las respuestas de todos los demás participantes y facilitamos dichas respuestas combinadas al cliente que encargó el estudio. Nunca facilitaremos deliberadamente sus respuestas individuales, excepto en las situaciones que se describen a continuación.

Sus respuestas pueden ser recolecciones, almacenadas o procesadas por nuestras compañías afiliadas o proveedores de servicios no afiliados, tanto dentro como fuera de (*insertar el país donde se ubica la empresa*). Están obligados por contrato a mantener de forma confidencial cualquier tipo de información que recojan y nos revelen, o que nosotros recojamos y les revelemos, con normas y prácticas de seguridad equivalentes a las nuestras.

Además de mantener la confidencialidad de sus respuestas durante un estudio, nunca venderemos, compartiremos, alquilaremos o transferiremos de cualquier forma intencionada su nombre, dirección, número de teléfono o dirección de correo electrónico a nuestros clientes, otras empresas de investigación de mercado, empresas de *marketing* directo o cualquier otra organización.

Las únicas excepciones en que podemos revelar su información personal o respuestas a terceros son las siguientes:

1. Cuando usted solicita o consiente en que compartamos su información identificativa y las respuestas individuales con terceros para un fin determinado;
2. Cuando, de acuerdo con las directrices de ESOMAR, suministramos las respuestas a un tercero que está obligado contractualmente a mantener la confidencialidad sobre la información revelada y sólo la utiliza con fines de investigación o estadísticos;
3. En el caso raro – aunque posible – de que la información esté sujeta a ser revelada como consecuencia de citaciones judiciales o gubernamentales, órdenes judiciales, peticiones o para requisitos legales o reglamentarios similares.

3. Uso de *cookies*, archivos de registro y otras tecnologías en nuestro sitio web

Las *cookies* son pequeños archivos de texto almacenados en un ordenador por un sitio web que le asigna una ID de usuario numérica y contiene cierta información sobre su navegación online. Utilizamos *cookies* en el sitio web de nuestra encuesta para ayudarnos a ofrecerle una mejor experiencia y proporcionar funciones de control de calidad y evaluación. No se almacena información personal en ninguna de las *cookies* que utilizamos.

(Aplicable a paneles de investigación) Algunas de las *cookies* que utilizamos en este sitio son necesarias para identificarle como un miembro válido de nuestro panel y proteger el acceso a su perfil e información de cuenta. Las opciones de privacidad de su navegador deben estar configuradas para admitir las *cookies* de (*inserte la URL del sitio web*), de lo contrario usted no podrá registrarse en el panel de (*inserte la URL del sitio web*) o acceder al Área de Miembros de este sitio. Si lo desea, puede ajustar la configuración de privacidad de su navegador para borrar las *cookies* al salir de los sitios web, o cuando usted cierre el navegador.

Este sitio utiliza objetos locales compartidos de Flash (LSO), también conocidos como "*cookies* de Flash", para almacenar algunas de sus preferencias, mostrar contenido basado en lo que usted ha visto, personalizar su visita, combatir el fraude que pone en riesgo la calidad de la investigación, o para realizar un seguimiento sobre su conducta y actividades durante múltiples visitas al sitio web. Usamos las cookies de Flash estrictamente con fines de investigación.

Las *cookies* de Flash son diferentes de las *cookies* del navegador, debido a la cantidad y al tipo de datos almacenados y cómo se almacenan los datos. Las últimas versiones de los navegadores populares permiten a los usuarios de internet gestionar las *cookies* de Flash utilizando la configuración de privacidad del navegador o descargando de complementos.

Si su navegador no dispone de estas características, usted puede gestionar la privacidad y la configuración de almacenamiento de las *cookies* de Flash o desactivar su uso por completo visitando el sitio web de Macromedia, el fabricante de Flash Player, en el siguiente enlace:

Adobe Flash Player — administrador de configuración:http://www.macromedia.com/support/documentation/es/flashplayer/help/settings_manager.html

Nota: se recomienda a los investigadores en la UE que consulten la sección 4.1.1 en relación con la legislación comunitaria y los posibles requisitos para la solicitud de

consentimiento para almacenar *cookies*, excepto cuando sea estrictamente necesario para la prestación de un servicio expresamente solicitado.

(Aplicable a la investigación de seguimiento de la conducta) Utilizamos *cookies* opcionales, tanto para navegador como basadas en Flash, (*insertar "aplicaciones de software" si es aplicable a su panel*) para realizar investigaciones sobre publicidad y sitios web. Estas *cookies* sólo están disponibles para los miembros de nuestro panel que han aceptado expresamente participar en nuestro programa de investigación de seguimiento de la conducta. Las *cookies* realizan un registro de ciertos anuncios online y páginas web que usted ve, incluyendo la frecuencia con que el contenido online que estamos midiendo es visto por su ordenador. Sólo medimos un pequeño número de anuncios o sitios web a través de este programa de investigación y la información que recogemos se utiliza estrictamente con fines de investigación. Usted no recibirá ningún mensaje o comunicación comercial como resultado de su participación en esta investigación. Todos los detalles acerca de este programa están a su disposición mientras permanezca identificado en nuestro sitio web, incluyendo instrucciones sobre cómo detener su participación en cualquier momento.

Al igual que la mayoría de sitios web, recogemos cierta información automáticamente y la almacenamos en archivos de registro. Esta información incluye las direcciones IP (protocolo de internet), tipo de navegador, proveedor de servicios de internet (ISP), páginas referentes/de salida, sistema operativo, marca de fecha/hora y datos de navegación. Utilizamos esta información para analizar tendencias, administrar nuestro sitio, rastrear los movimientos de los usuarios por nuestro sitio y recopilar información demográfica sobre el conjunto de nuestra base de usuarios. Como protección contra el fraude, podemos vincular esta información recolección automáticamente a la información enviada a través de (*insertar URL de la empresa de investigación*).

(Aplicable a ID de dispositivo) Las tecnologías de identificación de dispositivos asignan un identificador único al ordenador del usuario para identificar y rastrear el equipo. (*insertar nombre de la empresa*) no utiliza la tecnología de identificación de dispositivos (también conocido como identificación de la máquina o huella digital) para recopilar información personal o realizar un seguimiento de las actividades online de los usuarios de ordenadores. Usamos la tecnología para ayudar a nuestros clientes a garantizar la integridad de los resultados de la investigación. La tecnología analiza información y datos obtenidos del navegador de su ordenador y de otros puntos de datos públicos, incluyendo por ejemplo los ajustes técnicos de su equipo, las características de su equipo y la dirección IP de su ordenador. Estos datos son utilizados para crear un identificador único asignado a su ordenador. El identificador único es un identificador alfanumérico que conservamos. No conservamos la información analizada por la tecnología para crear el identificador único. La tecnología no interrumpe o interfiere en el uso o el control de su ordenador y no altera, modifica o cambia la configuración o funcionalidad de su equipo.

En cumplimiento de nuestros esfuerzos para ayudar a los clientes en la protección y garantizar la integridad de los resultados de la encuesta, nosotros:

a. podemos vincular o asociar su identificador único con usted y con cualquier información que usted nos proporcione;

b. podemos compartir su identificador único con nuestros clientes y con otros proveedores de muestras o paneles, y

c. podemos recibir u obtener un identificador único vinculado a usted de terceros, incluyendo sin limitación a proveedores de muestras o de paneles o a clientes de nuestra empresa.

Cualquier identificador (o identificadores) único vinculado a un individuo específico será protegido de acuerdo con esta política de privacidad. Utilizaremos y distribuiremos la tecnología de una manera profesional y ética, y de acuerdo con nuestra política de privacidad, comunicaciones y/o divulgaciones hechas por nuestra empresa, así como con las leyes aplicables y normas de la industria.

En el caso de que descubramos o nos enteremos de cualquier conducta no ética en relación con el uso de la tecnología, o que la tecnología se esté utilizando de una manera incompatible con las declaraciones y/o revelaciones que hayamos hecho a los entrevistados, o en violación de las leyes y normas aplicables, tomaremos medidas inmediatas para prohibir tal conducta y garantizar la correcta administración de la tecnología.

4. Seguridad de la información personal

Informamos a nuestros empleados sobre nuestras políticas y procedimientos relativos a la confidencialidad, seguridad y privacidad, y hacemos hincapié en la importancia de cumplir con ellos. Nuestros procedimientos de seguridad concuerdan con las normas comerciales generalmente aceptadas para proteger la información personal.

Podemos transferir información personal a compañías afiliadas o proveedores de servicios no afiliados con fines relacionados con la investigación, tales como procesamiento de datos y la realización de sorteos de premios u otros incentivos. Pedimos a estas empresas que protejan toda la información personal de una manera que concuerde con las medidas de nuestra empresa y según lo estipulado por la ley. Seguimos los estándares aceptados por la industria para proteger la información personal que se nos envía, durante la transmisión y una vez que la recibimos.

5. Exactitud de la información personal

(insertar nombre de la empresa) se esfuerza por mantener la información personal en su poder o bajo su control y que utiliza de forma continua, exacta, completa, actualizada y relevante, basada en la información más reciente de que disponemos. Confiamos en usted para ayudarnos a mantener su información personal precisa, completa y actualizada respondiendo a nuestras preguntas con honestidad.

6. Acceso a información personal

Nota para los investigadores: en Europa, Australia, Canadá, Nueva Zelanda y otras jurisdicciones que tienen leyes de privacidad exhaustivas, los individuos tienen derecho legal a acceder a su información personal almacenada por organizaciones, con sujeción a ciertas condiciones. Los derechos de acceso de los particulares también se aplican a las empresas estadounidenses que participan en el programa Safe Harbour de Estados Unidos y la Unión Europea.

Para solicitar el acceso a la información personal que tenemos sobre usted, es necesario que usted presente su solicitud por escrito a la dirección de correo electrónico o dirección postal que se muestra a continuación (en Cómo contactar con nosotros). Usted puede acceder a su información personal y corregirla, modificarla o eliminarla donde sea inexacta, excepto en los siguientes supuestos:

1. Cuando al facilitar acceso a su información personal es probable que se revele información personal sobre otros;
2. Cuando al comunicar la información podría revelar información comercial confidencial sobre (*insertar nombre de la empresa*) o sus clientes.
3. Cuando la carga o coste de facilitar el acceso sean desproporcionados en relación a los riesgos para su privacidad en el caso de que se trate.

Haremos todo lo posible para proporcionarle su información personal solicitada dentro de los 30 días desde la recepción su solicitud de acceso. Si no podemos atender su solicitud, le proporcionaremos una explicación escrita de por qué hemos tenido que rechazar su solicitud de acceso.

7. Notificación de cambios sustanciales a esta política

Si hacemos un cambio importante en esta política o nuestras prácticas de privacidad, publicaremos un aviso destacado en este sitio durante 30 días naturales antes de la implementación del cambio material y describiremos cómo podrán ejercer cualquier opción pertinente los individuos. Inmediatamente después de implementar el cambio, haremos constar en la introducción de esta política cuándo fue revisada por última vez.

8. Cómo contactar con nosotros

Las preguntas sobre esta política, las quejas acerca de nuestras prácticas y las solicitudes de acceso deben ser remitidas al Director de Privacidad de (*insertar nombre de la empresa*) a través de e-mail, escribiendo a (*insertar la dirección de correo electrónico*), o por correo postal enviando su carta a (*insertar la dirección postal*).

Investigaremos todas las quejas y trataremos de resolver las que encontremos justificadas. Si es necesario, modificaremos nuestras políticas y procedimientos para que otras personas no experimenten el mismo problema.

(Nota para los investigadores: si su empresa participa en el programa de privacidad TRUSTe u otro servicio de control de credenciales de privacidad por terceros, menciónelo aquí. TRUSTe, por ejemplo, ofrece un servicio de resolución de conflictos que exige que sus miembros lo incluyan en sus políticas de privacidad).

ESOMAR
Eurocenter 2
Barbara Strozzilaan 384
1083 HN Ámsterdam
Países Bajos
Tel +31 20 664 2141
Fax +31 20 664 2922
E-mail professional.standards@esomar.org
www.esomar.org

“La investigación de mercados, que incluye la investigación social y de opinión, consiste en recopilación e interpretación sistemáticas de información sobre personas u organizaciones, utilizando métodos estadísticos y analíticos y técnicas de las ciencias sociales aplicadas para obtener nuevas percepciones o aportar elementos de apoyo a la toma de decisiones.
La identidad de los entrevistados no se revelará al usuario de la información sin el consentimiento específico de aquéllos, ni los entrevistados serán contactados para acciones de venta como resultado directo de haber facilitado información.”

Definición de investigación de mercados contenida en el Código internacional ICC/ESOMAR

ESOMAR es la organización mundial que busca posibilitar una mejor investigación de mercados, consumidores y sociedades.
Con 5000 miembros en más de 100 países, el objetivo de ESOMAR es promocionar el valor de la investigación de mercados y de opinión esclareciendo los problemas reales y logrando una toma de decisiones efectiva.
Para facilitar este diálogo continuo, ESOMAR crea y gestiona un amplio programa de eventos temáticos específicos para la industria, publicaciones y comunicaciones, y promociona activamente la autorregulación y la práctica del Código en todo el mundo.