TRATAMIENTO DE LA CONFIDENCIALIDAD EN LAS OPERACIONES ESTADÍSTICAS DE EUSTAT

EUSKAL ESTATISTIKA ERAKUNDEA
INSTITUTO VASCO DE ESTADISTICA
Donostia-San Sebastián, 1
01010 VITORIA-GASTEIZ
Tel.: 945 01 75 00
Fax: 945 01 75 01
E-mail: eustat@eustat.eus
www.eustat.eus

Presentación

El mantener el secreto estadístico de los suministradores (hogares, individuos, empresas, administraciones y otros), la confidencialidad de la información que facilitan y la utilización de ésta con fines exclusivamente estadísticos deben garantizarse plenamente dentro de la actividad estadística. Esta salvaguarda responde al derecho a la privacidad que asiste a todos los ciudadanos por la propia Constitución, y que está garantizada en las leyes estadísticas, y en concreto en la Ley Estadística Vasca, la cual hace referencia al Secreto Estadístico y a la protección de datos individualizados (Cap. IV de la Ley 4/1986, de 23 de abril, de Estadística de la Comunidad Autónoma de Euskadi).

Tanto el mantener el secreto estadístico de los suministradores como la confidencialidad de los datos individualizados, sustenta toda la credibilidad de una organización estadística y, por ello, ha de estar presente en todas las fases del quehacer estadístico. Esta tarea ha de comenzarse por la fase de recogida de los datos directamente de los suministradores, adaptándose dicha salvaguarda y protección en los diferentes métodos de recogida, bien sea personal o por medios telefónicos o telemáticos. También habrá de inspirar el tratamiento de la información a través de las diferentes fases de validación, extrapolación y explotación de la misma, finalizando con la protección de los datos en la difusión estadística.

El Código de Buenas Prácticas de la Estadísticas Europeas, adoptado por Comité del Sistema Estadístico Europeo el 16 de noviembre de 2017, en su principio quinto, establece la necesidad de impartir al personal orientaciones e instrucciones sobre la protección de la confidencialidad estadística a lo largo de todos los procesos estadísticos, y de que la política de confidencialidad esté a disposición del público.

Este último aspecto es el que inspira el desarrollo de este documento, cuya finalidad es informar tanto al suministrador como al usuario de la estadística, así como al público en general, del tratamiento de la confidencialidad dentro de las operaciones estadísticas que lleva a cabo el EUSTAT y de las normas que rigen este aspecto en cada una de las fases de la producción estadística.

Este documento se desarrolla en tres apartados; el primero de ellos agrupa las recomendaciones seguidas para la salvaguarda de la confidencialidad en la fase de recogida de los datos; en el segundo, aparecen las normas y observaciones a seguir en la fase de producción; y un tercer apartado donde se detallan las normas aplicadas en la difusión de ficheros y tablas.

Por último, se incluye un glosario de términos relacionados con el ámbito de la protección de datos estadísticos y las principales referencias en cuanto al marco legal y recomendaciones técnicas sobre las que se sustenta esta actuación, y que conforman la base y principios por los que se rige en esta materia la Organización Estadística Vasca y sus Organismos.

Vitoria-Gasteiz, agosto de 2021

Josu Iradi Arrieta

Director General

Tratamiento de la confidencialidad en la recogida de información

En sentido estricto, la recogida de información abarca los trabajos de campo necesarios para la obtención de la información estadística de los informantes.

No obstante, en la actualidad, la implantación de nuevos sistemas de automatización implica que procesos como la depuración, grabación y codificación de los datos se realizan de forma simultánea a la recogida de información.

Por lo tanto, las medidas y procedimientos para la protección y preservación de la confidencialidad descritos en este apartado abarcarán también a dichos procesos en aquellos casos en los que éstos sean implícitos al proceso de recogida.

Deber de salvaguardar el secreto estadístico por parte del personal

El secreto estadístico es un deber jurídico que obliga a todo el personal estadístico y también a las personas físicas o jurídicas que tengan conocimiento de la información estadística individualizada y a los órganos de las administraciones públicas con competencia en materia de función pública estadística a no difundir, ni directa ni indirectamente, datos individuales o individualizados de los suministradores de la información.

El secreto estadístico implica también la prohibición de utilizar para finalidades distintas de las estadísticas los datos obtenidos directamente de los informantes por los servicios estadísticos. Es decir, estos datos no pueden ser utilizados para finalidades distintas de las estadísticas.

Todo el personal que lleva a cabo la recogida de la información, así como cualquier otra función dentro de EUSTAT, debe firmar una cláusula de confidencialidad (Artículo 15 de la Ley Vasca de Estadística).

Esta cláusula de confidencialidad es asumida tanto por el personal contratado directamente por Eustat como por el personal subcontratado para la recogida.

Derechos y deberes del informante

Las personas o entidades tienen obligación de suministrar la información estadística que les sea requerida con independencia de su naturaleza física o jurídica, pública o privada.

A quien se le vayan a solicitar datos se le debe informar previamente y de forma expresa, precisa e inequívoca de:

- La existencia del tratamiento, la finalidad de la recogida de los datos y de los posibles destinatarios de la información.
- Las consecuencias si se niega a facilitar los datos solicitados.
- La posibilidad de ejercitar los derechos de acceso, rectificación, oposición y limitación, sujeto a excepciones.

Estos requerimientos se comunican **por carta** (preferentemente mediante correo electrónico) a los suministradores de información anticipadamente, y se recuerdan en la fase de la recogida de datos **a través del encuestador** y/o mediante clausulas informativas en el propio **cuestionario** (de preferencia, a través del canal web).

Medidas físicas y técnicas para la protección de datos en la fase de recogida de información

Estas medidas afectan al personal contratado para la recogida y a los sistemas automáticos de recogida de información.

- Uso del **carnet de encuestador.** Personal e intransferible; éste debe ser presentado por el encuestador en el momento de la recogida de datos. Le habilita para la recogida y le obliga a guardar el secreto estadístico.
- **Salvaguarda de la información**. El personal de campo debe guardar por tiempo indefinido la **máxima reserva** y no emitir al exterior datos de carácter personal o sujetos a secreto estadístico, salvo que esté debidamente autorizado.

- **Formatos y soportes**. Solo utilizar informes en formato papel, que contengan datos de carácter personal o sujetos a secreto estadístico, en caso excepcional. Éstos se deben mantener en lugar seguro y fuera del alcance de terceros. Todos los soportes que contienen este tipo de información son devueltos y guardados en lugar seguro tras la finalización de las tareas que han originado el uso temporal de los mismos.

- **Accesos autorizados.** A través de un servicio de identificación seguro (llave de seguridad usb, identificador de usuario y contraseña, mensaje/app en teléfono móvil, …) se permite el acceso del personal autorizado a los sistemas de recogida automática y grabación de datos (tablet, portátil, ordenador personal). La asignación de estos accesos (llave USB, usuario y contraseña, …) se realiza de forma individual y para una operación estadística concreta. Además, el volcado y recuperación de la información desde los dispositivos portátiles requiere de un acceso específico que permite realizar este tipo de acción.

  En general, el uso y asignación de los accesos estará regulado por la normativa expresada en la Política de Seguridad y el Documento de Seguridad de EUSTAT, desarrollados en cumplimiento del *Real Decreto 3/2010*, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y del *Real Decreto 1720/2007*, de 21 de diciembre, por el que se aprueba el Reglamento de protección de datos de carácter personal, respectivamente.

- **Registro de incidencias**. El personal de campo deberá notificar al responsable cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos (pérdida de listados y/o soportes de almacenamiento electrónico, sospecha de uso indebido del acceso autorizado por otras personas, recuperación de datos, etc.).

- **Recogida de datos a través de Internet**. La información estadística recogida directamente a través de cuestionarios web, se deposita directamente en la Bases de datos de EUSTAT, que dispone de un entorno propio y diferenciado para los datos estadísticos, dentro de la infraestructura de nube híbrida del Gobierno Vasco.

Tratamiento de la confidencialidad en la producción estadística

El proceso de producción estadística abarca todas las fases, desde la recogida hasta su difusión, por cualquiera de los canales establecidos. Estas fases pueden abarcar tratamientos de validación, imputación, extrapolación, explotación y almacenamiento. La normativa y directrices de protección de los datos y preservación de la confidencialidad en este proceso, se centrará principalmente en los protocolos de seguridad establecidos para el acceso, tratamiento y almacenaje de ficheros que contienen datos protegidos ya sean Datos de Carácter Personal o Datos Estadísticos. Dicha normativa se halla pormenorizada en la Política de Seguridad y el Documento de Seguridad desarrollados por EUSTAT.

Deber de salvaguardar el secreto estadístico por parte del personal

Todo el personal de EUSTAT ha de firmar una cláusula de confidencialidad, así como un compromiso de cumplimiento de la normativa que se establece en la Política de Seguridad y el Documento de Seguridad.

De igual forma, las empresas contratadas para de recogida de datos, su tratamiento y/o desarrollo de aplicativos, deberán firmar una cláusula de confidencialidad de los datos manejados.

En los contratos que se celebran con otras empresas, figuran las siguientes cláusulas:

Específicas en función del servicio:

- Definición de los trabajos contratados, finalidad de los mismos e instrucciones para su realización.
- Instrucciones para la destrucción o devolución al contratante de los soportes que contengan datos protegidos.

- Medidas de seguridad que, de acuerdo con la naturaleza de la información tratada, ha de implantar la empresa contratada para la realización de los trabajos.

Genéricas:

- Compromiso de la empresa contratada de que únicamente tratará los datos conforme a las instrucciones recibidas de Eustat, que no los aplicará o utilizará con un fin distinto al que figura en el contrato, ni los comunicará, ni siquiera para su conservación, a terceras personas.

- Compromiso de la empresa contratada de que los trabajos se realizarán bajo las medidas de seguridad especificadas.

- Compromiso de la empresa contratada de que, una vez cumplida la relación contractual, se destruirá o devolverá al contratante cualquier soporte que contuviera datos protegidos.

- Cláusula de responsabilidad, para el caso de que la empresa contratada destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato.

No se permitirá la transferencia de datos recabados con una finalidad estadística a ficheros administrativos.

Medidas físicas y técnicas para la protección de datos en el proceso de producción estadística

Estas medidas afectan tanto al personal de EUSTAT, como al contratado para el procesamiento y almacenamiento de la información, así como al desarrollo de los sistemas y aplicativos informáticos utilizados en esta fase este proceso.

- **Puertas de acceso** a las plantas de EUSTAT. Eustat, como medida de seguridad adicional, tiene establecido un sistema específico (tarjetas) de entrada a sus dependencias, que exclusivamente permite acceder a las mismas a las personas que trabajan en el Instituto.

- Medidas en el **puesto de trabajo.** Durante ausencias prolongadas del puesto físico de trabajo, éste debe mantenerse limpio de documentación y material. Para ello, debe hacerse el debido uso de los cajones y armarios provistos de llave, manteniéndolos cerrados durante el periodo de ausencia. Además, el ordenador personal deberá estar apagado o en estado de "Bloqueado por el usuario", para evitar accesos indebidos al contenido del mismo.

- **Ficheros y soportes.** Todas las entradas y salidas de ficheros y soportes de datos protegidos hacia y desde las dependencias del Instituto, están controladas por un estricto protocolo de actuación que garantiza el registro y el seguimiento de la información, así como el almacenamiento centralizado de todos los datos en entornos seguros y de acceso restringido.

- Acceso físico a los servidores **Centro de Proceso de Datos** (Batera). Se requiere que el acceso a este tipo de dependencias u otras que almacenen datos protegidos se realice mediante un sistema informatizado de registro y control de acceso. Por defecto, el acceso estará cerrado de forma permanente y sólo se permitirá el acceso y permanencia a dichas dependencias al personal autorizado.

- **Envío de datos individualizados**. Cualquier envío de los datos individualizados se realizará por la persona autorizada y utilizando las aplicaciones puestas a disposición para ello (incorporarán transmisión por un medio seguro o un sistema de encriptación electrónico).

- **Accesos autorizados.** El personal sólo accede a los datos y recursos protegidos que necesita para su trabajo cotidiano. Este acceso se controla mediante la asignación de un usuario y contraseña o llave de seguridad USB, únicos e intransferibles y que permiten el acceso a unos recursos y datos determinados.

- El **acceso** a datos reales **para pruebas** de aplicativos informáticos en desarrollo dentro del Instituto requerirá de una autorización especial y se realizará bajo las siguientes condiciones:

    - Los datos reales serán sometidos a un proceso que permita la disociación de los datos, de tal modo que se imposibilite la asociación de la información obtenida con una persona concreta.

- Si los datos no se disocian, deberá asegurarse el nivel de seguridad correspondiente a la naturaleza de los datos que se van a manejar.

- **Ficheros temporales** que se creen tendrán las mismas medidas de seguridad que correspondan a los ficheros maestros de los que proceden sus datos. En general, su creación y gestión se regirá por las siguientes normas:

    - Sólo se podrán generar ficheros temporales cuando sean para su uso exclusivo en procesos específicos y relacionados con el trabajo de la unidad usuaria.

    - Estos ficheros no podrán ubicarse en unidades locales de PCs, ni se permitirá su salida fuera de la unidad usuaria, ni podrán ser copiados en soportes informáticos (ni siquiera para ser almacenados) o en la nube interna de gobierno.

    - Una vez que estos ficheros hayan dejado de ser útiles para la finalidad con la que se crearon, serán borrados por el usuario que los creó.

- **Registro de incidencias** Cada vez que un usuario detecte una incidencia que pudiera afectar a la seguridad de los datos, lo notificará al Centro de Proceso de Datos. Este centro será el encargado del mantenimiento del registro de incidencias de seguridad y anotará toda la información relevante que afecte a datos protegidos.

Tratamiento de la confidencialidad en la difusión estadística

Las tablas, gráficos, ficheros, documentos y publicaciones derivados de cualquier operación estadística y distribuidos por los canales y medios de comunicación establecidos conforman la difusión de cualquier operación estadística. Descartada la posibilidad de cualquier identificación individual directa gracias a la estricta aplicación de la Ley de Estadística Vasca en cumplimiento del secreto estadístico y de la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, las medidas y criterios para la protección de los datos en esta fase de la difusión estadística de los datos, están encaminados a evitar identificaciones indirectas de individuos o entidades a partir de la publicación de análisis o explotaciones muy detallados, que puedan derivar en la revelación de información sensible o confidencial sobre los mismos.

Estas medidas y directrices, de control de desvelamiento estadístico, dependerán en gran medida del formato en el que se difunda la información y del carácter general o específico de ésta. Nos centraremos principalmente en las medidas de carácter general de aplicación en la difusión de tablas y microdatos.

Directrices generales de protección para la difusión de tablas

- Se evitará publicar celdas con frecuencias pequeñas en aquellos cruces de variables dónde intervenga alguna variable sensible y además la tabla se refiera a un área geográfica inferior a 10.000 habitantes.

- Se evitará publicar celdas con magnitudes o variables numéricas dónde se pueda derivar de forma fácil la contribución o contribuciones de alguna de las unidades estadísticas (individuos, familias, establecimientos, empresas, ...) que aportan valor a la celda. Esto se produce en presencia de pocos contribuyentes o cuando existen contribuciones dominantes a la celda.

- Para evitar la aparición de dichas celdas se podrán aplicar criterios de sensibilidad y técnicas de recodificación de variables y/o métodos de supresión de celdas que protejan la tabla de forma adecuada y preserven la mayor cantidad de información posible.

Directrices generales de protección para la difusión de Microdatos.

- Los ficheros de microdatos que se difundan no incluirán en ningún caso identificadores directos de registro ni datos de carácter personal (*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*).

- En general, los ficheros de microdatos que se difundan no presentarán identificadores geográficos que hagan referencia a **áreas menores de 10.000** habitantes. Por tanto, para **áreas geográficas de tamaño inferior a dicho límite, no se distribuirán ficheros de microdatos**.

- El detalle del resto de variables incluidas en el fichero de microdatos dependerá del nivel geográfico aportado y de la sensibilidad de la propia variable, permitiendo una mayor desagregación conceptual cuanto más grande sea el ámbito geográfico difundido y menor el grado de sensibilidad de la variable.

- Como **protección adicional** se podrán aplicar técnicas de perturbación de microdatos o intercambio de registros, modificando variables cuantitativas en pequeñas cantidades aleatorias y/o intercambiando atributos de forma controlada entre registros de áreas geográficas próximas, respetando en todo caso las distribuciones (medias, totales, …) por territorio histórico.

Normativa relacionada (Leyes de estadística y Protección de datos)

Ley 4/1986, de 23 de abril, de estadística de C. A. de Euskadi.

Leyes de los Planes Vascos de Estadística 1989-1992, 1993-1996, 1997-2000, 2001-2004, 2005-2008, 2010-2012, 2014-2017 y, el actualmente vigente, ley 8/2019, de 27 de junio, del Plan Vasco de Estadística 2019-2022.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Glosario de términos

Criterios de sensibilidad

Reglas aplicadas para la detección de celdas sensibles en tablas de frecuencias y/o magnitud. Estas reglas pueden estar basadas en el número de contribuciones a la celda (regla del valor umbral) o en el valor de las contribuciones dominantes de la celda (reglas de dominancia). La primera detecta celdas con frecuencias pequeñas y la segunda con aportaciones dominantes al valor de la celda. En ambos casos estas celdas son potencialmente “peligrosas” de cara a su difusión ya que pueden contener o derivar en la revelación de información sensible.

Datos de carácter personal

Toda información numérica, alfabética, gráfica, fotográfica, acústica, biométrica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento y transmisión, concerniente a personas físicas identificadas o identificables (tales como nombre, apellidos, estado civil, sexo, edad, domicilio, número de la seguridad social, número de matrícula del empleado, D.N.I., número de teléfono, etc.)

Datos estadísticos

Toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a unidades estadísticas (personas físicas o jurídicas, entes u organismos públicos, etc.) recogida con fines estadísticos y sujeta por lo tanto a las normas que rigen el secreto estadístico.

Identificaciones indirectas

Inferencia de la identidad de una unidad de la población incluida en un archivo difundido de microdatos, por otros medios diferentes a la identificación directa (nombre, apellidos, dirección, D.NI. número de la seguridad social, número de matrícula, número de teléfono, …).

Información sensible

Hace referencia a la información considerada como estrictamente confidencial. Información y características referentes a la salud, raza, religión, ideología, afiliación, finanzas, etc., se consideran de carácter sensible y requieren de una protección especial.

Intercambio de registros o permutación

Es un método de control de la revelación aplicado a los microdatos, que consiste en intercambiar los valores de algunas variables que figuran en registros apareados por medio de una variable clave representativa. En la literatura, este método es a veces denominado “transformación multidimensional”. Se trata de una técnica de transformación que garantiza (bajo ciertas condiciones) la preservación de un conjunto de estadísticos, como los promedios, las varianzas y las distribuciones univariantes.

Métodos de supresión de celdas

Aplicado a los datos tabulados, los métodos de supresión de celdas comprenden la **supresión primaria** y la **supresión complementaria (secundaria**).

La supresión primaria consiste en no publicar el valor de ninguna celda reveladora, dicho de otra manera, de no presentar sus valores en la tabla y de reemplazarlos por un símbolo, (P.ej: “x”, ó “s”,…) para indicar la supresión. Según la definición de criterio de sensibilidad serán celdas reveladoras y, por lo tanto, deben ser objeto de una supresión primaria, aquellas cuyo valor es bajo en tablas de frecuencias, y las celdas cuyo valor es bajo o que presentan un caso de **dominancia,** en las tablas de variables cuantitativas.

Para lograr el grado deseado de protección de las celdas reveladoras, a veces, es necesario suprimir celdas adicionales, que hacen necesario recalcular el valor de la supresión primaria: entonces se habla de **supresión complementaria (secundaria)**. El criterio de selección de las celdas complementarias suprimidas debe ser elegido prudentemente, con el fin de garantizar el nivel deseado de protección y al mismo tiempo suprimir la menor cantidad posible de información.

Microdatos

Es un conjunto de registros individualizados que contienen información sobre individuos o entidades económicas determinadas.

Tablas

Explotaciones sintéticas de datos estadísticos dónde interviene una o más variables (categóricas o numéricas) y que presentan información agregada sobre los individuos o entidades económicas objeto de estudio.

Técnicas de perturbación

Procedimientos que implican la modificación sistemática de datos (a veces en pequeñas cantidades aleatorias), de manera que las cifras no sean lo suficientemente precisas como para revelar información sobre casos individuales.

Variable sensible

Variable numérica o categórica que contiene información sensible.