DOCUMENTACIÓN DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Área de Sistemas de la Información y Ciberseguridad

077 Medidas Adicionales Para El Tratamiento de Categorías Especiales de Datos Personales y/o Información Confidencial/Sensible

AUTOR: **Área de Sistemas de la Información y Ciberseguridad**

FECHA DE CREACIÓN: **20 de agosto de 2018**

ÚLTIMA VERSIÓN: 25 de septiembre de 2019

ÍNDICE

INTRODUCCIÓN 3

A.1. DEFINICIONES 3

A.2. CUÁNDO SE PUEDEN TRATAR DATOS 4

A.3. PERIODOS DE CONSERVACIÓN 4

A.4. MEDIDAS A APLICAR POR EL PERSONAL DE IFEMA 5

B. PRODUCTOS PARA LA RECOGIDA Y TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS PERSONALES Y/O INFORMACIÓN SENSIBLE 5

C. WEBS SIEMPRE POR HTTPS 6

D. CLOUD PÚBLICAS 6

E. ENVÍOS POR EMAIL 7

F. UNIDAD S: 7

G. SOPORTES EXTRAÍBLES 8

H. CIFRAR CATEGORÍAS ESPECIALES DE DATOS PERSONALES Y/O INFORMACIÓN SENSIBLE 8

H.1. COMPRESIÓN CON CONTRASEÑA 8

H.2. CIFRAR CON OFFICE 11

I. ALMACENAR DATOS EN PAPEL 11

J. MINIMIZACIÓN DEL TRATAMIENTO DE DATOS 12

INTRODUCCIÓN

El objetivo de este documento, el cual forma parte de la Política de Seguridad de IFEMA, es establecer las Normas que los empleados y usuarios colaboradores de IFEMA deben seguir cuando tengan acceso a información que pueda resultar sensible y/o confidencial para la Institución, así como en los casos en los que se traten categorías especiales de datos personales.

A.1. DEFINICIONES

"**INFORMACIÓN CONFIDENCIAL**" O "**INFORMACIÓN SENSIBLE**"

Tendrá la consideración de "**Información Confidencial**" o "**Información Sensible**", toda información que abarca conocimientos técnicos o científicos, datos empresariales relativos a clientes y proveedores, planes comerciales, estudios, estrategias de mercado, así como cualquier información susceptible de generar un beneficio de cualquier tipo para la Institución.

TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS PERSONALES

Las "**categorías especiales de datos personales**" representan aquellos datos de carácter personal que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Ejemplos de categorías especiales de datos personales son los siguientes:

- Los que revelen el origen étnico o racial,
- las opiniones políticas,
- las convicciones religiosas o filosóficas,
- la afiliación sindical,
- el tratamiento de datos genéticos,
- los datos biométricos dirigidos a identificar de manera unívoca a una persona física (imágenes faciales o datos dactiloscópicos),
- datos relativos a la salud,
- la orientación sexual,
- los de personas vulnerables, en particular niños,

- las condenas e infracciones penales.

A los efectos del establecimiento de estas medidas de seguridad, entrarán dentro de las categorías especiales de datos personales aquellos tratamientos realizados con la finalidad de elaborar perfiles. Se entenderá como elaboración de perfiles, toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

A.2. CUÁNDO SE PUEDEN TRATAR DATOS

IFEMA puede tratar categorías especiales de datos personales únicamente en los casos en que sea pertinente y necesario para el fin para el que esos datos fueron recogidos.

Además, IFEMA deberá recabar el consentimiento expreso del interesado siempre que se traten categorías especiales de datos personales. Todos los consentimientos deberán guardarse y almacenarse a fin de demostrar que IFEMA trata este tipo de datos de forma legítima.

No obstante, deben cumplirse estrictamente las condiciones que se indican a continuación para no vulnerar los derechos de los titulares y tampoco incurrir en infracciones reglamentarias sancionables.

- Conocimiento de la Secretaría General de IFEMA, junto con su visto bueno desde el punto de vista reglamentario. Porque algunas categorías especiales de datos personales no se pueden tratar ni siquiera contando con el consentimiento de sus titulares.
- Conocimiento del Departamento de Sistemas Corporativos y Seguridad de la Información junto con su visto bueno desde el punto de vista técnico de la seguridad, de la viabilidad y de las medidas técnicas de seguridad necesarias.
- Adopción de todas las medidas reglamentarias, técnicas y de seguridad para el tratamiento de datos sensibles de carácter personal.
- Adopción de las medidas adicionales descritas en el presente documento.

A.3. PERIODOS DE CONSERVACIÓN

Las categorías especiales de datos personales se conservarán mientras sean imprescindibles para cumplir con la finalidad para la que fueron recogidos. Este plazo

deberá ser el menor posible para garantizar que los datos sean exactos y se mantengan actualizados.

Una vez cumplida la finalidad para la que fueron recabados, los datos personales deberán eliminarse de las bases de datos, excepto que exista una obligación legal de conservarlos durante un tiempo determinado (por ejemplo, legislación laboral, legislación de lucha contra el fraude, o cualquier otra que sea de aplicación) IFEMA conservará los datos personales durante el tiempo que establezca la normativa en cuestión.

Los plazos de conservación aplicables a cada caso dependerán del tipo de dato y de su finalidad.

A.4. MEDIDAS A APLICAR POR EL PERSONAL DE IFEMA

Este documento representa una postura de mínimos, por lo que, en cualquier momento, tanto Secretaría General y/o el Departamento de Sistemas Corporativos y Seguridad de la Información pueden decidir incorporar otras medidas adicionales que resulten más restrictivas con el fin de dotar mayor seguridad a los datos personales que son objeto de tratamiento.

A continuación, se detallan las normas, directrices, propuestas y medidas de nivel alto de aplicación obligatoria al trabajo con categorías especiales de datos. Estas normas son de obligado cumplimiento para todo el personal que esté autorizado para tratar datos sensibles de IFEMA:

1. Personal contratado directamente por IFEMA.
2. Personal contratado por empresas de trabajo temporal para prestar sus servicios en IFEMA.
3. Personal de empresas de servicios contratadas por IFEMA.
4. Personal de empresas colaboradoras con IFEMA.

Todas las personas relacionadas anteriormente se encuentran obligadas por ley a cumplir lo establecido en este documento y están sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

B. PRODUCTOS PARA LA RECOGIDA Y TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS PERSONALES Y/O INFORMACIÓN SENSIBLE

Para la recogida y tratamiento de categorías especiales de datos y/o información sensible deben usarse siempre productos que estén respaldados por una empresa solvente y comprometida con los asuntos de seguridad y protección de datos de modo que demuestren que están en disposición de proporcionar medidas de seguridad suficientes y conforme a la normativa.

No están permitidos productos, módulos, plugins, apps, etc. de origen opensource o no determinado, pese a lo atractivo de su funcionamiento y lo competitivo de su coste. Estos son criterios que nunca deben prevalecer frente a la seguridad de los datos sensibles.

C. WEBS SIEMPRE POR HTTPS

Las webs que capturan categorías especiales de datos o contengan información sensible deben publicarse únicamente por https en su totalidad, empleando para ello un certificado digital válido, moderno y procedente de una Autoridad de Certificación de confianza. Es decir, el acceso a dichas webs debe ser seguro y cifrado.

Por tanto, no está permitido publicar este tipo de webs por http sin cifrado ni con un certificado digital auto firmado ni que provoque advertencias en los navegadores.

D. CLOUD PÚBLICAS

La recogida y tratamiento de categorías especiales de datos y/o contengan información sensible debe realizarse siempre en sistemas seguros. Por tanto, no deben emplearse para estos fines sistemas cuya ubicación no es bien conocida, que se encuentra directamente en países que carecen de garantía alguna en materia de protección de datos o que utilizan sistemas de hosting cuestionables en relación con la seguridad de la información.

El uso de cloud públicas (esto es, sistemas de almacenamiento en la nube) para almacenar categorías especiales de datos y/o información sensible tampoco está permitido. Este tipo de webs están orientadas a la accesibilidad y al uso cada vez más rápido y sencillo, tienen diseños muy conseguidos, un coste reducido, etc. Y, aunque se ubiquen en países de la Unión Europea o aquellos con un nivel equivalente de protección[1], su propia naturaleza pública plantea dudas para almacenar en ellas datos sensibles, junto con los demás datos del resto de usuarios de dichas webs, a los que cabe considerar como auténticos desconocidos y cuyos datos pueden ser de todo tipo, incluso contener virus y malware.

Tampoco ayuda en materia de seguridad que las cloud públicas, con el fin de dar un servicio más rápido, permiten compartir las categorías especiales de datos y/o información sensible muy fácilmente, con operaciones muy sencillas. Esta amenaza (a que se desvelen los datos sensibles con tanta facilidad) constituye un riesgo que no se debe asumir nunca con este tipo de datos.

Por último, las condiciones de uso de las cloud públicas están siempre recogidas en textos complejos, muy largos, que conducen fácilmente al equívoco y a la confusión, y

[1] Son países con un nivel equiparable de protección los siguientes: Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Estados Unidos (aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU.) y Japón.

que no cumplen con los principios de protección de datos recogidos por la normativa en esta materia. Además, pueden cambiarlos inadvertidamente y, en estas condiciones, no se deben almacenar categorías especiales de datos y/o información sensible .

E. ENVÍOS POR EMAIL

Los envíos por email de categorías especiales de datos y/o información sensible siempre deben ir cifrados. No está permitido que las contraseñas empleadas para el cifrado estén escritas en los propios envíos junto con los datos cifrados. Dichas contraseñas se comunicarán por teléfono a la persona autorizada para tratar con los datos sensibles.

Es obligatorio cifrar las categorías especiales de datos y/o información sensible que se adjunten a los emails porque se pierde su control una vez abandonan los sistemas de IFEMA. El cifrado contribuye a que sólo el destinatario autorizado pueda acceder a dichos datos.

Los procedimientos para cifrar categorías especiales de datos y/o información sensible para adjuntarlos en un email están recogido en el apartado H.

F. UNIDAD S:

Las categorías especiales de datos personales y/o información sensible se almacenarán en la unidad S: en una carpeta con los permisos restringidos al máximo. Así, solo deberán tener acceso a estos archivos aquellos usuarios que con motivo de sus labores profesionales deben acceder a la información.

La unidad S: es el lugar más adecuado para guardar los datos de IFEMA. Cuenta con medidas que garantizan la disponibilidad y la integridad de los datos, así como medidas generales de confidencialidad por las que sólo ciertos usuarios pueden acceder a dicha unidad.

Es obligatorio permitir el acceso a las categorías especiales de datos y/o información sensible únicamente a los usuarios autorizados e impedirlo a los demás. Por tanto, para garantizar la confidencialidad de las categorías especiales de datos y/o de la información sensible , en primer lugar, se copiarán dichos datos en carpetas concretas de la unidad S. A continuación, se solicitará a la CIO que configure el acceso permitido al contenido de dichas carpetas sólo a los usuarios autorizados y que impida el acceso al resto.

G. SOPORTES EXTRAÍBLES

No está permitido guardar datos sensibles sin cifrar en soportes extraíbles tales como pendrives USB, CDs, DVDs o cualquier otro dispositivo extraíble, dado el riesgo que supone que dichos soportes puedan ser accedidos por personas no autorizadas. Las

categorías especiales de datos y/o información sensible se cifrarán como se indica en el apartado H.

No está permitido dejar dispositivos extraíbles desatendidos en una mesa o incluso conectados a un PC sin la debida supervisión, aunque se encuentren en su interior, en el lector de discos. Porque de nada sirve bloquear el PC en estos casos: al final los datos que contienen los pendrives o los discos pueden acabar en manos de personas no autorizadas.

H. CIFRAR CATEGORÍAS ESPECIALES DE DATOS PERSONALES Y/O INFORMACIÓN SENSIBLE

El responsable de la custodia, envío u otros tratamientos de los archivos con categorías especiales de datos personales y/o información sensible deberá cifrarlos de modo que no se pueda acceder a dichos datos sin autorización de su superior dentro del departamento al que pertenezca o del responsable de Seguridad de la Chief Information Office. El cifrado también se conoce como encriptación.

Para enviar categorías especiales de datos y/o información sensible a un destinatario autorizado se cifrarán utilizando uno de los métodos de cifrado con contraseña que se describen en los apartados siguientes.

Las contraseñas se escogerán aleatoriamente y estarán formadas por números, letras en mayúsculas y minúsculas y caracteres especiales. No está permitido emplear contraseñas débiles, triviales o palabras que se encuentren en los diccionarios. La longitud de las contraseñas será como mínimo de 8 caracteres.

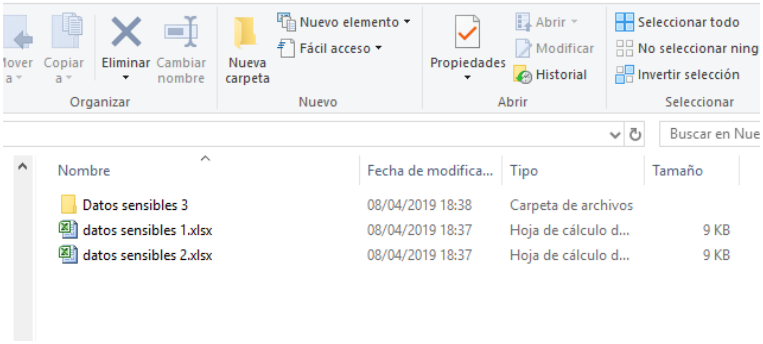
Los archivos cifrados y sus contraseñas no deben estar juntos, por tanto, tampoco está permitido que formen parte del mismo envío, con el fin de evitar que dicho contenido sea desvelado a personas no autorizadas. Tras enviar archivos cifrados por email a otra persona autorizada, la contraseña se dirá por teléfono al destinatario.

Precaución: el extravío de la contraseña de cifrado implica la pérdida definitiva del contenido de los archivos que protege.

H.1. COMPRESIÓN CON CONTRASEÑA

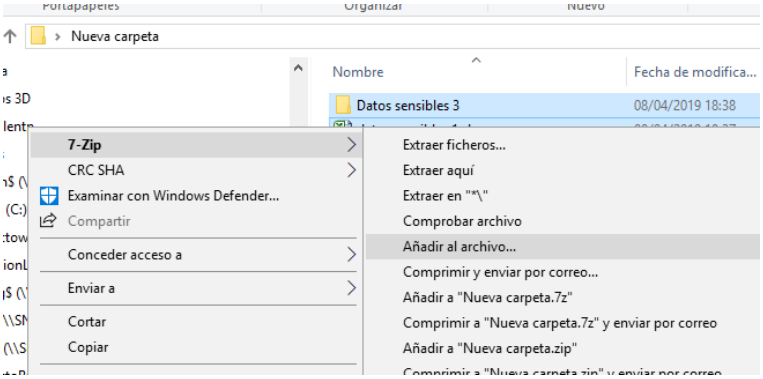
El procedimiento para cifrar un conjunto de archivos con datos sensibles consiste en incluirlos en un fichero zip con contraseña. A continuación se describen los detalles:

Sean estos archivos y carpeta con datos sensibles

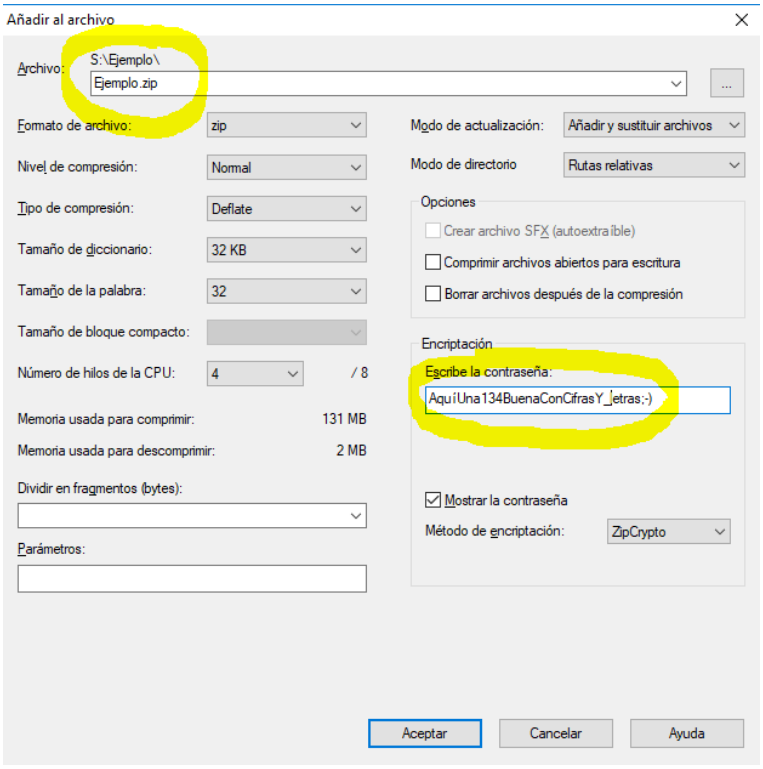


Se seleccionan los que es necesario cifrar.

A continuación, se pulsa el botón derecho del ratón y se escoge la opción “7-zip” y “Añadir al archivo…” como indica el ejemplo

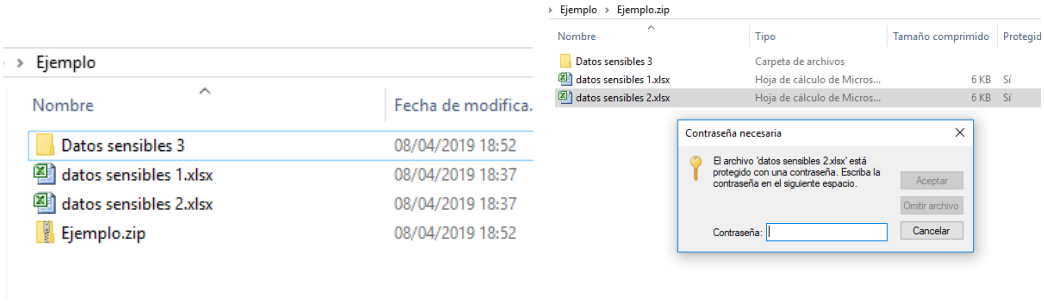


Se especifica un nombre adecuado para el archivo zip y una contraseña de cifrado, sin la cual, será imposible acceder al contenido de dicho archivo zip.



Los archivos originales ya no es necesario guardarlos aparte porque se encuentran más seguros dentro del fichero Ejemplo.zip: están protegidos con la contraseña que se empleó para cifrarlos.

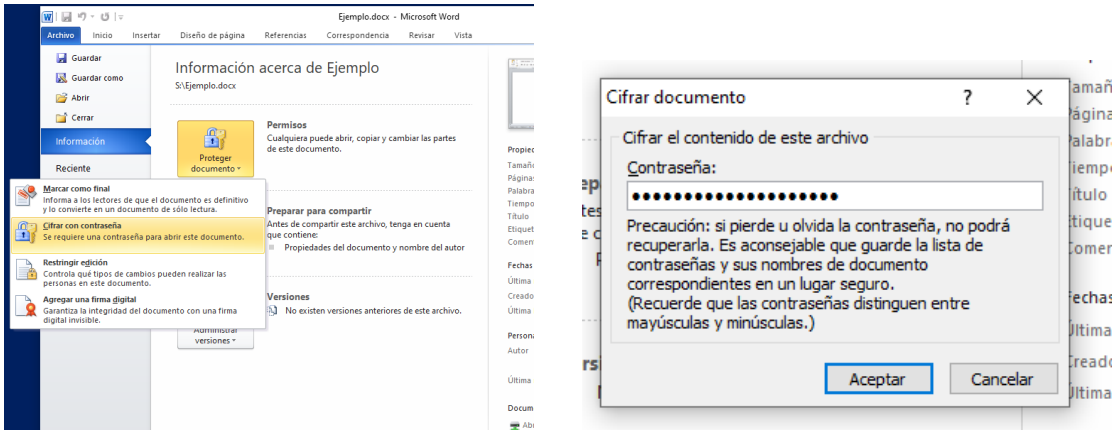
Para acceder al contenido del archivo .zip, es necesario volver a introducir la misma contraseña con la que se protegió, como se ve en la figura de la derecha a continuación.



H.2. CIFRAR CON OFFICE

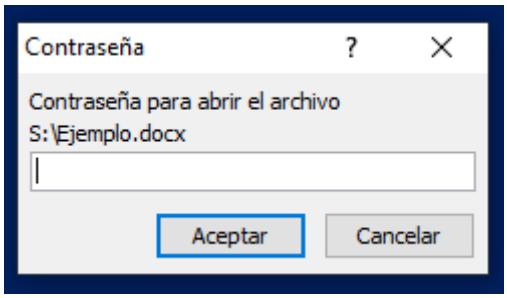
Los documentos generados con Office (Word, Excel, PowerPoint,…) se pueden cifrar individualmente con una contraseña para cada archivo. A continuación se describe el procedimiento.

Se selecciona, sucesivamente, las siguientes opciones desde el menú principal: Archivo -> Información -> Proteger documento -> Cifrar con contraseña, como se observa en la figura de la izquierda.



A continuación, se introduce dos veces la misma contraseña de cifrado, como se ve en la figura de la derecha.

Para abrir el archivo cifrado es necesario introducir cada vez la misma contraseña, como se indica a continuación.



I. ALMACENAR DATOS EN PAPEL

En primer lugar, advertir que el uso de papel debe ser excepcional cuando se trate información sensible o categorías especiales de datos personales, puesto que representa una política interna de IFEMA el uso cada vez más restringido de este soporte.

Los datos en papel deben almacenarse de forma que sólo las personas autorizadas puedan acceder a ellos. Estarán archivados en lugares tales como armarios de seguridad y bajo un control de acceso a los mismos.

Nunca se dejarán los datos en papel en las mesas o en cualquier otro lugar en que puedan ser accedidos por personas no autorizadas.

Medidas concretas aplicables cuando en soporte papel:

Los usuarios serán responsables de los soportes y documentos no automatizados (papel) que estén bajo su custodia. El archivo de los soportes o documentos en formato papel se realizará de acuerdo con los siguientes criterios:

1. Cada departamento establecerá los criterios y procedimientos de archivo de aquellos soportes o documentos que contengan datos de carácter personal o información sensible.
2. En caso de que, para el ejercicio de determinadas funciones deban manejarse soportes papel o, en cualquier caso, siempre que temporalmente se manejen dichos soportes en papel, éstos deberán conservarse siempre en archivadores o armarios bajo llave, o en cualquier caso deberán disponer de mecanismos que obstaculicen su apertura, y ordenados para facilitar su consulta en caso necesario.
3. Cuando los documentos que contengan datos de carácter personal o información sensible no se encuentren debidamente archivados en los dispositivos de almacenamiento indicados anteriormente, por estar en proceso de revisión o de tramitación, el personal autorizado que esté a cargo de dichas actividades deberá custodiarlos e impedir en todo momento el acceso no autorizado a los datos. Los puestos de trabajo se mantendrán libres de documentación que contenga datos de carácter personal sin vigilancia, especialmente encima de las mesas. Se deberá mantener encima de la mesa únicamente la documentación necesaria para las funciones que se estén desempeñando en cada momento y bajo custodia. Se tomarán medidas para salvaguardar la documentación en caso de que sea necesario abandonar momentáneamente el puesto de trabajo por cualquier causa.
4. Cuando se haya terminado de utilizar aquellos soportes o documentos no automatizados que contengan datos de carácter personal o información sensible, se deberá llevar a cabo su destrucción, de tal forma que resulten inaccesibles.

J. MINIMIZACIÓN DEL TRATAMIENTO DE DATOS

Sólo se obtendrán, procesarán y guardarán los datos necesarios que sean imprescindibles para la realización de la finalidad perseguida y para la que se han obtenido los consentimientos. En el caso de categorías especiales de datos, tiene que estar absolutamente justificado el tratamiento de tales datos.

A continuación, un ejemplo ilustrativo: tampoco tiene sentido recabar datos de dirección postal si sólo están previstos los envíos por medios electrónicos, debido a que IFEMA estaría tratando más datos de los necesarios e imprescindibles para prestar el servicio.

Otro ejemplo ilustrativo sería pedir información sobre el sexo o la orientación religiosa de un visitante cuando ello no fuera relevante para permitir el acceso a una feria.

Las categorías especiales de datos que sean necesarios para una ocasión en particular, una vez hayan cumplido su cometido, se deben eliminar. Por ejemplo, si recabamos las preferencias de menú para la asistencia a un acto, no tiene sentido luego conservarlas una vez transcurrido el acto. En particular, si hemos recabado datos para evitar ciertos alimentos que revelan datos de salud tales como alergias o intolerancias.