- **Expediente N.º: EXP202207523**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: D. ***A.A.A.*** (en adelante, la parte reclamante) con fecha 27 de junio de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra DIRECCIÓN GENERAL DEL CATASTRO con NIF S2826053G (en adelante, el CATASTRO). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que en la página web oficial de la sede electrónica del CATASTRO, en el apartado -generar certificaciones-, al introducir un DNI cualquiera se autocompletaban campos con el nombre de la persona, apellidos y su dirección, todo ello sin necesidad de registrarse en la sede electrónica. Que estos hechos se pusieron a disposición de la administración competente (Dirección General del Catastro) el día 26 de junio de 2022 y, en el momento de presentarse esta denuncia, persistía dicha incidencia. Además, el reclamante tiene indicios de que esta situación ha operado durante más de 6 meses. Afirma que la URL del formulario era accesible a través del buscador Google.

En fecha 17 de julio de 2022 se recibe en esta Agencia nuevo escrito de la parte reclamante en el que se nos aporta una captura de pantalla realizada con un móvil donde aparece un formulario que cuelga de la sede electrónica del catastro y con un ejemplo de consulta realizada para un número de DNI, apareciendo el campo nombre y apellidos cumplimentado. La captura de pantalla se hizo el 28 de junio de 2022 y se aporta como prueba de los hechos denunciados en la reclamación presentada por esta misma parte en fecha 27 de junio de 2022.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación al CATASTRO, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones

Públicas (en adelante, LPACAP), fue aceptado en fecha 12 de julio de 2022, tal y como consta en la certificación que obra en el expediente.

Con fecha 29 de julio de 2022 se recibe en esta Agencia escrito de respuesta indicando que *"1. Descripción detallada y cronológica de los hechos ocurridos.*
El 26 de junio se recibe incidencia en el buzón de la sede electrónica notificando una posible vulnerabilidad en el apartado –generar certificaciones- de la sede electrónica del catastro.
A raíz de la incidencia se revisa el apartado referido y no se encuentra ninguna anomalía, por lo que se solicita más información al usuario. El día 28 se le pregunta por los pasos realizados en el acceso referido y el usuario contesta ese mismo día detallando los mismos.
En ese momento, se procede a investigar el comportamiento y se realiza una primera corrección, eliminando el acceso directo a la página problemática el día 1 de julio.
Posteriormente esto se comunica al remitente de la incidencia el día 6 de julio.
2. Especificación detallada de las causas que han hecho posible el incidente.
Una de las opciones que se ofrece en la sede electrónica es la generación de certificaciones con tasa de acreditación catastral. Este servicio únicamente es accesible para usuarios registrados, cuya identificación
se realiza en la página de acceso a la sede registrada y se verifica en todas y cada una de las páginas. Esta página en concreto tiene una opción de autocompletar los datos de nombre y apellidos cuando se introduce el NIF del solicitante, para facilitar la cumplimentación del formulario por parte del usuario registrado.
El incidente sucedió porque en el buscador de Google, al buscar "generación certificaciones catastro", el tercer link que aparecía era una URL directa a la siguiente página:
******URL.1***
Al acceder a dicho enlace, aunque no se mostraban datos protegidos (ya que se comprobaba si tenía permisos para verlos) dejaba ver el formulario vacío, y si se ponía en el campo del NIF un NIF valido, se refrescaba esa parte de la página mostrando nombre y apellidos asociados con ese NIF.
Esto no se detectó en pruebas previas porque la verificación consistía en asegurar que no se mostraban datos al usuario que no estuviera autorizado, pero no se comprobaba que tampoco cumplimentara los campos del formulario.
3. Número de personas afectadas por la violación de la seguridad de los datos personales.
La función de autocompletar el nombre y apellidos a partir del NIF se ofrece tras la autenticación previa, y no genera una petición al sistema.
Como no se ha ofrecido ningún dato protegido almacenado en Catastro (titularidad de los inmuebles, o valor catastral de los mismos), no existe constancia en la base de datos de dichos accesos.
Para estimar el alcance del problema con esa limitación, se ha revisado en las tablas accedidas las consultas realizadas desde la implantación de esta funcionalidad (año 2016) y se han encontrado 575 consultas de datos de los que no consta autenticación previa. Se trata de una cantidad no elevada para ese periodo
4. Categoría de los datos personales involucrados.
A este respecto cabe informar que tras introducir el NIF, se autocompletan los campos de nombre y apellidos, pero no se proporciona ningún dato protegido específico del Catastro (titularidad de los inmuebles, o valor catastral de los mismos).
5. Posibles consecuencias para las personas afectadas.

Si alguien consiguió acceder de esta forma e introdujo un NIF completo válido, pudo obtener el nombre y apellidos correspondientes a ese NIF. No obstante, se desconocen los posibles usos de esta información.
6. Descripción detallada de las acciones tomadas para solucionar el incidente y minimizar su impacto sobre las personas afectadas.
En cuanto se detectó el problema se quitó el acceso directo a esa página.
Para corregirlo, ahora se comprueba que si el usuario no tiene permisos para ver los datos, no se muestra tampoco el formulario, indicando que su sesión ha caducado, y forzando así que se tenga que autenticar. Esta página solo está autorizada para que la vean los usuarios registrados con la autorización adecuada, de no ser este tipo de usuario no se mostrará el formulario.
Por otro lado también se ha añadido en todas las páginas de la Sede Electrónica del Catastro el metadato facilitado por Google para identificar a la Dirección General del Catastro como propietaria y así poder solicitarle que borre de la cache y retire del resultado del buscador cualquier página que le indiquemos.
Para ésta en concreto también se ha añadido el metadato para que no la indexe el buscador y no aparezca nunca como resultado de una búsqueda.

7. Medidas de seguridad de los tratamientos de datos personales adoptadas con anterioridad al incidente, así como la documentación acreditativa del Análisis de Riesgos que ha conllevado la implantación de dichas medidas de seguridad y, en su caso, copia de las Evaluaciones de Impacto de los tratamientos donde se ha producido la violación de seguridad de los datos personales.
Las medidas de seguridad para los tratamientos de datos personales actualizadas se informan en el estado del cumplimiento del Esquema Nacional de Seguridad de la Dirección General del Catastro según la guía CCN-STIC-824, recogido en la herramienta INES, apartado 3.7 Protección de la información, subapartado 1. Datos de carácter personal.
En todo caso, se adjunta la última Declaración de Aplicabilidad completa, de marzo 2021, en la que se refleja lo relativo a los tratamientos de datos personales en la dimensión de confidencialidad (C).
8. Copia del Registro de Actividad de los tratamientos donde se ha producido el incidente.
Con carácter general los tratamientos de la Sede Electrónica del Catastro, exceptuando las descargas masivas de información, se encuadran en la actividad E00127105-002 del Registro de Actividades de Tratamiento (RAT). Se adjunta el citado fichero RAT de la Dirección General del Catastro.
9. Si la violación de seguridad ha sido comunicada a las personas afectadas, indique el canal utilizado, fecha de la comunicación y detalle del mensaje enviado. En caso negativo, indicar los motivos.
Como consecuencia del bajo número de posibles afectados desde 2016 (575 consultas de datos de los que no consta autenticación previa, lo que descartaría una actuación masiva de consulta por algún tipo de medio automatizado), unido a la categoría de datos personales involucrados (nombre y apellidos previa introducción de un DNI válido registrado en la Base de Datos de Catastro), no confieren a la brecha de seguridad un nivel de impacto suficiente sobre los afectados para que constituya un riesgo probable para sus derechos y libertades, por lo que no se estaría en el supuesto del artículo 34 del RGPD, para notificar dicha brecha a los afectados
10. Indique si la violación de seguridad ha sido notificada a esta Autoridad de Control. En caso contrario, indique los motivos por los que la violación de seguridad no ha sido

notificada a esta Autoridad de Control antes del transcurso de 72 horas desde que se haya tenido constancia de ella. Puede obtener información sobre la gestión y notificación de brechas de seguridad en el siguiente enlace de la Agencia: ******URL.2***
Tal y como se ha respondido en el aparatado anterior, el bajo número de posibles afectados desde 2016 (575 consultas de datos de los que no consta autenticación previa, lo que descartaría una actuación masiva de consulta por algún tipo de medio automatizado), unido a la categoría de datos personales involucrados (nombre y apellidos previa introducción de un DNI válido registrado en la Base de Datos de Catastro), no confieren a la brecha de seguridad un nivel de impacto suficiente sobre los afectados para que constituya un riesgo probable para sus derechos y libertades, por lo que no se estaría en el supuesto del artículo 33 del RGPD, para notificar dicha brecha a esa Agencia.
11. Medidas que piensa adoptar para que no se vuelva a producir un incidente similar en el futuro.
Para todas las páginas que tienen características de autenticación previa, se ha implementado la siguiente funcionalidad: se comprueba que si el usuario no tiene permisos para ver los datos, no se muestra la página solicitada, diciéndole que su sesión ha caducado, forzando así que se tenga que autenticar.
Por otro lado también se han añadido en todas nuestras páginas el metadato facilitado por google para poder solicitarle que borre de la cache del buscador cualquier URL nuestra que le pidamos…"

TERCERO: Con fecha 18 de agosto de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

En fecha 18 de agosto de 2022 se recibe en esta Agencia un nuevo escrito de la parte reclamante, con número de registro de entrada REGAGE22e00035737498, en el que se hace constar que en el acuerdo de admisión a trámite se señaló por esta Agencia que los datos autocompletados en el formulario eran nombre y apellidos vinculados con el NIF introducido; no obstante, afirma que esta Agencia había obviado el elemento más gravoso expuesto en la reclamación original, que se trataba del campo domicilio también autocompletado en el formulario.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

En fecha 29 de julio de 2022 y con número de registro de entrada REGAGE22e00032983383, se recibe escrito de contestación al traslado de la reclamación efectuado por esta Agencia. De su análisis se extrae:

1. Afirman que el 26 de junio de 2022 recibieron la incidencia en el buzón de la sede electrónica notificando dicha vulnerabilidad, que se solicitó al usuario más información en fecha 28 de junio de 2022, contestando el usuario a la petición este mismo día. Que en ese momento se procede a investigar los hechos y se realiza una primera corrección, eliminando el acceso directo a la página

problemática el día 1 de julio de 2022. Posteriormente se comunica al remitente en fecha 6 de julio de 2022.

2. En relación con las causas que motivaron el incidente, afirman que sucedió porque el formulario quedó expuesto en internet accesible desde el buscador Google, y que al rellenarse el campo NIF con un dato válido se refrescaban los campos nombre y apellidos que correspondían al NIF introducido, no detectándose esta anomalía en las pruebas previas que se habían realizado porque la verificación consistió en asegurar que no se mostraban datos catastrales al usuario que no estuviera autorizado, pero no se comprobaba que tampoco cumplimentara los campos del formulario .
3. En relación con las personas afectadas, afirman que tras revisar los logs internos se han detectado 575 consultas desde que se activó el formulario en 2016.
4. En relación con las categorías de datos afectadas afirman que se autocompletaban los campos nombre y apellidos únicamente.
5. En relación con las acciones tomadas para solucionar el incidente, afirman que para corregirlo se ha forzado a que el usuario esté autenticado para que se pueda mostrar el formulario, y que este formulario solo se muestra a usuarios registrados autorizados.
6. En relación con nuestra solicitud de las medidas existentes, Análisis de Riesgos y Evaluación de Impacto, nos afirman que la relación de medidas implantadas son las especificadas en el Esquema Nacional de Seguridad (ENS), aportando documento con la Declaración de Aplicabilidad con fecha de marzo de 2021 (se trata del documento que recoge las medidas seleccionadas e implantadas de entre las especificadas en el Anexo II del ENS). No aportan ni Análisis de Riesgos ni Evaluación de Impacto.
7. Aportan el Registro de Actividades de Tratamiento (RAT).
8. En relación con la comunicación de la violación a los afectados y la notificación a esta Agencia, afirman que teniéndose en cuenta el bajo número de posibles afectados (575) y que solo afectaba a la tipología de datos nombre y apellidos, *no confiere riesgo para los derechos y libertades de las personas afectadas* por lo que no procede la notificación a esta Agencia y comunicación a los afectados. No obstante, en el transcurso de esta investigación se utiliza la herramienta de la AEPD “Asesora BRECHA” obteniéndose el resultado siguiente: *“EL RESPONSABLE DEBE NOTIFICAR SIN DILACIÓN INDEBIDA LA BRECHA DE DATOS PERSONALES A LA AEPD”*, conclusión obtenida utilizando los siguientes datos de entrada introducidos:
    - *El incidente ha afectado a la confidencialidad.*
    - *El incidente ha sucedido por un fallo, ausencia o vulneración de medidas de seguridad.*
    - *Existe la probabilidad de que la brecha suponga algún riesgo sobre los derechos y libertades de las personas, habiéndose producido la pérdida de control de los datos personales de las personas afectadas en las 575 consultas detectadas.*

    Por otro lado, en relación con la obligación de comunicar la violación a los afectados, se utiliza en el transcurso de esta investigación la herramienta de la AEPD “Comunica-Brecha RGPD” obteniéndose el resultado:” NO *SERÍA NECESARIO COMUNICAR LA BRECHA DE SEGURIDAD A LOS AFECTADOS”*, y a partir de los siguientes datos de entrada introducidos:

- *Las personas no se verán afectadas o pueden encontrar algunos inconvenientes muy limitados y reversibles que superarán sin ningún problema.*
- *No hay constancia de la materialización de daños y la probabilidad de materialización es baja.*
- *Los datos afectados son nombre, apellidos y dirección postal.*
- *Se han visto afectados unas 575 personas.*

1. Afirman que como medida implantada para que el incidente no vuelva a ocurrir se ha forzado para que el usuario esté autenticado en la sede y tenga los permisos adecuados para acceder a este formulario.

En fecha 21 de septiembre de 2022 se realiza requerimiento de información a la Dirección General del Catastro, marcado por la siguiente línea de investigación:

- Obtener información del tipo de usuario autenticado en sede que sí tendrían acceso al formulario una vez implantadas las medidas correctivas.
- Obtener confirmación sobre si el campo domicilio también se autocumplimentaba al introducir el campo NIF y por lo tanto también fue un dato personal filtrado en la violación de seguridad.
- Solicitar los Análisis de Riesgos para la actividad de tratamiento “Base de datos del catastro – SIGECA”.
- En relación con el ENS:
  - Obtener información sobre la dimensión del nivel de seguridad de los sistemas de información sobre los que se apoya la actividad de tratamiento anterior.
  - Obtener aclaración del por qué se utiliza el mecanismo de autenticación en sede electrónica basado en “Número de NIF + Número de soporte del DNI + Referencia Catastral del Titular” en lugar del certificado digital (método de autenticación más seguro y recomendado por el ENS en las medidas de seguridad).
  - Obtener la copia de la última auditoría del ENS realizada obligatoria según el propio ENS.

En fecha 5 de octubre de 2022 y con números de registro de entrada REGAGE22e00044314252 y REGAGE22e00044314408 se recibe respuesta al requerimiento de información anterior. Del análisis de esta respuesta se extrae:

1. Afirman que el formulario está accesible exclusivamente para usuarios registrados en sede *del tipo “Gerencia*” con objeto de que un funcionario habilitado pueda obtener la certificación catastral solicitada por el ciudadano a través de este formulario. Afirman que la función de autocompletar sigue estando activa para facilitar la funcionalidad.
2. Nos confirman que también se autocompletaba el domicilio de la persona para la que se hubiera introducido el NIF.
3. En relación con el Análisis de Riesgos solicitado, únicamente se nos aporta un documento que se ha obtiene al hacer uso de la herramienta “Evalúa Riesgo RGPD” de la AEPD. Del análisis de este documento se concluye:
   a. El documento tiene fecha de obtención el 5 de octubre de 2022 a las 13:48 horas.
   b. En este se indica una valoración de *Riesgo Intrínseco Alto* y una valoración de *Riesgo Residual Bajo*.

c. En el pie del propio documento se incluye el texto por parte de la herramienta: "*Este informe tiene carácter de documento de soporte a la realización de la gestión del riesgo, y en ningún caso la sustituye, ni reemplaza a las obligaciones de responsables y encargados*".

4. En relación con la información solicitada sobre la adecuación al ENS:
   a. Afirman que la categoría del Sistema de Información Catastral (SIC) que sirve de base a los tratamientos de datos afectados por la violación de seguridad es la correspondiente a NIVEL MEDIO.
   b. Afirman que el mecanismo existente de autenticación en sede electrónica basado en el conocimiento de los datos: ***(…)*** (opción de autenticación menos segura que el certificado electrónico recomendado por el ENS) fue implementado a raíz de *la Orden HFP/1423/2021 de 20 de diciembre, por la que se modificó la Orden EHA/2219/2010, de 29 de julio, por la que se aprueba el sistema de firma electrónica de clave concertada para actuaciones en la sede electrónica asociada de la Dirección General del Catastro.* Afirman que dicha orden se aprobó con el espíritu de ofrecer las mayores facilidades posibles al amparo del Real Decreto 463/2020, de 14 de marzo, por el que se declaró el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19.
   c. Aportan un documento con un informe de adecuación al ENS realizado por la empresa "GMV Soluciones Globales Internet S.A.U" en diciembre de 2017. Este documento resume las actuaciones a realizar para la consecución de los objetivos marcados por la Dirección General del Catastro según la Guía de Seguridad CCN-STIC-806 (Adecuación al Esquema Nacional de Seguridad).

QUINTO: Con fecha 5 de mayo de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del Artículo 5.1.f) del RGPD tipificada en el Artículo 83.5 del RGPD, por la presunta infracción del Artículo 32 del RGPD y del Artículo 33 del RGPD tipificadas en el Artículo 83.4 del RGPD.

SEXTO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), la parte reclamada presentó escrito de alegaciones en el que manifestaba:

> *PRIMERA. - En relación a su manifestación de la página 11 del citado escrito: "La exposición en la internet pública de un formulario al que solo se debía acceder previa identificación del usuario en sede electrónica no cumple con las mínimas medidas de seguridad razonables. Este formulario permitía que al rellenarse el campo NIF con un valor válido se autocompletaban de manera automática los campos nombre, apellidos y domicilio de la persona a la que hacía referencia esta NIF.*
> *En consecuencia, la exposición de dicho formulario no garantiza la confidencialidad, integridad y disponibilidad de los sistemas y servicios del tratamiento ni la finalidad del tratamiento".*
> *A este respecto, se considera que el incidente pudo afectar de una manera muy residual únicamente a la confidencialidad, al proporcionarse una*

información que no se debía ofrecer (nombre, apellidos y domicilio de la persona a la que correspondía dicho NIF).
No obstante, en ningún caso afectó a la integridad porque no se alteraron los datos existentes en el Catastro al ser una función de Consulta. Tampoco a la disponibilidad, pues el servicio de la Sede Electrónica del Catastro no se vio interrumpido temporal o permanentemente por el incidente, tal y como se desprende de lo dispuesto en las páginas 9 y 13 de su escrito.

"SEGUNDA.- En relación a su manifestación de la página 13 del citado escrito: "En el presente supuesto, el CATASTRO no notificó la brecha de seguridad en el plazo establecido en el RGPD a tal efecto, con las informaciones establecidas en el artículo 33 del RGPD; puesto que, consideró que no existió riesgo para los derechos y libertades de las personas afectadas, para ello han tenido en cuenta el volumen de datos filtrados (575 consultas), la tipología de datos (nombre, apellidos y dirección) y el tiempo que lleva el formulario en producción (desde 2016)".
En primer lugar, habiendo realizado la evaluación del riesgo a través de la herramienta Asesora-Brecha de esa Agencia Española de Protección de Datos, el resultado obtenido, relativo a una brecha de seguridad en un tratamiento de datos personales en el que se ha visto comprometida la confidencialidad de los datos y se han mitigado los posibles riesgos de dicha pérdida de confidencialidad, no viéndose afectada la integridad y la disponibilidad de los datos, ha sido que "no es necesario notificar la brecha de datos personales a la AEPD".
Se acompaña imagen del resultado obtenido:
Además, una vez se tuvo conocimiento por parte de este Centro Directivo de la brecha de seguridad, fueron inmediatamente aplicadas medidas para su subsanación, mitigándose así los posibles riesgos de pérdida de confidencialidad. Se quitó igualmente el acceso directo a la página web donde se generó la incidencia, por medio del buscador de Google "generación certificaciones catastro". También, y para corregirlo, se comprobó que, si el usuario no tenía permisos para ver los datos, no se mostraba tampoco el formulario, indicando que su sesión había caducado, y forzando así que se tuviera que autenticar. Además, esta página sólo se encuentra autorizada para que la vean los usuarios registrados con la autorización adecuada.
Por otro lado, también se añadieron en todas las páginas de la Sede Electrónica del Catastro el metadato facilitado por Google para identificar a la Dirección General del Catastro como propietaria y así poder solicitarle que borrase de la cache y retirara del resultado del buscador cualquier página que se indicara.
Para ésta en concreto, también se añadió el metadato para que no indexara el buscador y no apareciera nunca como resultado de una búsqueda.
En segundo lugar, cabe informar que, al introducir el NIF, la opción de autocomplementar existente anteriormente, cuyo fin era facilitar la cumplimentación de formularios a los usuarios registrados, autocompletaba los campos de nombre, apellidos y domicilio, pero no proporcionaba ningún dato protegido específico del Catastro (titularidad de los inmuebles, o valor catastral de los mismos).
Para concluir, se adjunta tabla que muestra el volumen de accesos a la Sede Electrónica del Catastro por año desde 2016 en el que se puede apreciar el

volumen de la brecha (575 consultas)frente al volumen anual de accesos a la sede constituyendo un 0,0000841247655% del total.

Años	***Visitas a Sede***
2016	*70.005.043*
2017	*77.011.004*
2018	*78.827.767*
2019	*126.926.632*
2020	*170.807.374*
2021	*159.930.772*
Total	***683.508.592***

SÉPTIMO: Con fecha 9 de junio de 2023 se formuló propuesta de resolución, en la que se estimó la alegación relativa a la no obligación de no notificar la brecha de seguridad, de conformidad con el artículo 33 del RGPD, y se proponía imponer a la DIRECCIÓN GENERAL DEL CATASTRO, con NIF S2826053G, por una infracción del Artículo 5.1.f) del RGPD y del Artículo 32 del RGPD, tipificadas en los Artículo 83.5 del RGPD y Artículo 83.4 del RGPD, respectivamente, una sanción de apercibimiento por cada una de las infracciones.

OCTAVO: Notificada la propuesta de resolución, en fecha 27 de diciembre de 2023, se dicta nota por la Directora de la Agencia Española de Protección de Datos; en la que, siguiendo el criterio de este organismo en relación con este tipo de supuestos, considera que concurren en el presente expediente sancionador, tramitado a la DIRECCIÓN GENERAL DEL CATASTRO, las siguientes infracciones, a las que corresponden las siguientes sanciones:

- Sanción de apercibimiento por la infracción del Artículo 5.1.f) del RGPD tipificada en el Artículo 83.5 del RGPD.
- Sanción de apercibimiento por la infracción del Artículo 32 del RGPD tipificada en el Artículo 83.4 del RGPD.
- Sanción de apercibimiento por la infracción del Artículo 33 del RGPD tipificada en el Artículo 83.4 del RGPD.

NOVENO: De acuerdo con el artículo 90.2 Ley 39/2015, de 1 de octubre, del Procedimiento administrativo común de las Administraciones Públicas, se le notificó a la DIRECCIÓN GENERAL DEL CATASTRO dicha nota con fecha 28 de diciembre de 2023, a fin de que en el plazo de 15 días pudieran alegar cuanto consideraran en su defensa de la infracción del artículo 32 del RGPD y presentar los documentos e informaciones que considere pertinentes, de acuerdo con el artículo 89.2 de la LPACAP.

DÉCIMO: Notificada la citada nota conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) y dentro del plazo concedido, la parte reclamada ha presentado escrito de alegaciones considerando que no resulta procedente la sanción de apercibimiento por la vulneración del artículo 33 del RGPD propuesta.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: Consta acreditado en el expediente que en la página web oficial de la sede electrónica del CATASTRO, en el apartado -generar certificaciones-, al introducir un DNI cualquiera se autocompletaban campos con el nombre de la persona, apellidos y su dirección, todo ello sin necesidad de registrarse previamente en la sede electrónica.

SEGUNDO: Consta acreditado en el expediente que se han detectado 575 consultas de datos de los que no consta autenticación previa, desde que se activó el formulario en 2016.

TERCERO: Consta probado en el expediente que la tipología de los datos afectados son nombre y apellidos, así como el domicilio de la persona de la que se hubiera introducido el NIF.

CUARTO: Consta acreditado en el expediente que al utilizar la herramienta Asesora-Brecha, no se tuvo en cuenta que el riesgo de suplantación o usurpación de la identidad conlleva un riesgo para los derechos y libertades de las personas afectadas.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II

En relación con la imputación del artículo 32 del RGPD, la entidad reclamada señaló alegó lo siguiente en su escrito de alegaciones al acuerdo de inicio:

> *PRIMERA. - En relación a su manifestación de la página 11 del citado escrito: "La exposición en la internet pública de un formulario al que solo se debía acceder previa identificación del usuario en sede electrónica no cumple con las*

mínimas medidas de seguridad razonables. Este formulario permitía que al rellenarse el campo NIF con un valor válido se autocompletaban de manera automática los campos nombre, apellidos y domicilio de la persona a la que hacía referencia esta NIF.
En consecuencia, la exposición de dicho formulario no garantiza la confidencialidad, integridad y disponibilidad de los sistemas y servicios del tratamiento ni la finalidad del tratamiento".
A este respecto, se considera que el incidente pudo afectar de una manera muy residual únicamente a la confidencialidad, al proporcionarse una información que no se debía ofrecer (nombre, apellidos y domicilio de la persona a la que correspondía dicho NIF).
No obstante, en ningún caso afectó a la integridad porque no se alteraron los datos existentes en el Catastro al ser una función de Consulta. Tampoco a la disponibilidad, pues el servicio de la Sede Electrónica del Catastro no se vio interrumpido temporal o permanentemente por el incidente, tal y como se desprende de lo dispuesto en las páginas 9 y 13 de su escrito.

En contestación a dicha alegación, esta Agencia Española de Protección de Datos debe recordar que el artículo 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante brecha de seguridad) como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

En consecuencia, en el presente caso consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haberse expuesto en la internet pública un formulario al que solo se debía acceder previa identificación del usuario en sede electrónica.

Si bien y con independencia de ello, cuando en el acuerdo de inicio se habla de confidencialidad, integridad y disponibilidad se refiere a los sistemas y servicios del tratamiento, así como la finalidad del tratamiento.

El artículo 32 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de determinar y establecer las medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo en función del estado de la técnica, los costes de aplicación y, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

Es decir, el objetivo de dichas medidas de seguridad técnicas y organizativa debe ser garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales objeto de tratamiento.

Por todo lo expuesto, se desestimó la alegación.

Respecto a la imputación del artículo 33 del RGPD, la entidad reclamada se señala en su escrito de alegaciones a la nota de la Directora de fecha 27 de diciembre de 2023, según el orden expuesto, lo siguiente:

En respuesta a las alegaciones presentadas a la nota de la Directora por la entidad reclamada se señala, según el orden expuesto, lo siguiente:

> "*PRIMERA. - En relación a su manifestación de la página 13, párrafo primero del citado escrito:*
>
> *"Dicho lo anterior, como consecuencia de la brecha de seguridad sufrida en relación con las personas afectadas, la Dirección General del Catastro afirma que tras revisar los logs internos se han detectado 575 consultas desde que se activó el formulario en 2016, lo cual no quiere decir que se produjeran más consultas, aunque no se hayan podido detectar".*
>
> *A este respecto, parece que la resolución sugiere que se han podido producir más consultas de las 575 detectadas tras revisar los logs internos. En este punto, esta Dirección General puede confirmar positivamente que no ha habido más consultas que las reflejadas y que son las 575 de las que ya se informó en su día a esa Agencia. La herramienta de traza proporciona información de todos los accesos realizados, no pudiendo existir ningún acceso que no quede reflejado y contabilizado."*

En contestación a lo alegado, esta Agencia Española de Protección de Datos debe resaltar que 575 consultas al formulario es más que suficiente para que exista un riesgo para los derechos y libertades de las personas físicas, a los efectos de lo preceptuado en el artículo 33 del RGPD.

> *"SEGUNDA. - En relación a su manifestación de la página 13, párrafos segundo y cuarto del citado escrito:*
>
> *"Se accedió a datos de nombre, apellidos y dirección postal, pero el consultante también conocía el NIF de los titulares de los datos; por lo que, sí existió riesgo para los derechos de las personas dado que existió riesgo de suplantación de la identidad".*
>
> *"Además, dependiendo de la situación de los titulares de los datos personales, esta pérdida de confidencialidad pudo generar mayores riesgos para los derechos y libertades de las personas."*
>
> *Esta Dirección General entiende que pudo existir este riesgo. No obstante, se consideró inicialmente que habría sido residual. De igual forma que en la propia Sede Electrónica del Catastro no es suficiente con conocer el nombre y el código NIF para suplantar la identidad en los procedimientos, esto es práctica estándar en toda la administración digital, y en procesos equivalentes en el sector privado.*
>
> *Además, cabe reiterar, como ya se información en escritos anteriores que, una vez se tuvo conocimiento por parte de este Centro Directivo de la brecha de seguridad, fueron inmediatamente aplicadas medidas para su subsanación, mitigándose así los posibles riesgos de pérdida de confidencialidad. Se quitó igualmente el acceso directo a la página web donde se generó la incidencia, por medio del buscador de Google "generación certificaciones catastro".*

También, y para corregirlo, se comprobó que, si el usuario no tenía permisos para ver los datos, no se mostraba tampoco el formulario, indicando que su sesión había caducado y forzando así que se tuviera que autenticar. Además, esta página sólo se encuentra autorizada para que la vean los usuarios registrados con la autorización adecuada.

Por otro lado, también se añadieron en todas las páginas de la Sede Electrónica del Catastro el metadato facilitado por Google para identificar a la Dirección General del Catastro como propietaria y así poder solicitarle que borrase de la cache y retirara del resultado del buscador cualquier página que se indicara.
Para ésta en concreto, también se añadió el metadato para que no indexara el buscador y no apareciera nunca como resultado de una búsqueda.".

En contestación a dicha alegación, esta Agencia Española de Protección de Datos se alegra de que la Dirección General reconozca "… *que pudo existir este riesgo…"* así como las medidas adoptadas inmediatamente para su subsanación y corrección, intentando así mitigar los posibles riesgos de pérdida de confidencialidad.

"*TERCERA. - En relación a su manifestación de la página 13, párrafo quinto del citado escrito:*

"A mayor abundamiento, hay que poner de manifiesto que CATASTRO sólo ha aportado el resultado que, indica, ha obtenido de la herramienta "asesora-brecha", pero no aporta qué información ha introducido para que se llegara a tal resultado."

En relación a este punto, cabe indicar que los parámetros introducidos en la evaluación del riesgo a través de la herramienta Asesora-Brecha de esa Agencia Española de Protección de Datos y que arrojan el resultado según el cual "no es necesario notificar la brecha de datos personales a la AEPD", son los recogidos en el Anexo 1."

En contestación a lo alegado y en relación con los parámetros utilizados en la herramienta Asesora-Brecha, mencionar que en el apartado relativo al riesgo para los derechos y libertades de las personas afectadas, en el momento de su cumplimentación, se hizo caso omiso al apartado de ayuda, en el que consta literalmente:

Ayuda:

Existe riesgo para los derechos y libertades de las personas afectadas cuando pueda producirse un daño o perjuicio físico, material o inmaterial para las personas físicas cuyos datos se han visto afectados en la brecha.

Por ejemplo:

- Afecta a derechos fundamentales como:
  - La libertad de expresión,
  - La libertad de pensamiento,
  - La libertad de circulación,
  - La no discriminación,
  - La libertad de conciencia y de religión.
  - El derecho a la vida
- Produce:
  - Pérdida de control sobre sus datos personales
  - Restricción de derechos
  - Usurpación de identidad
  - Pérdidas financieras
  - Daño para la reputación
  - Pérdida de confidencialidad de datos sujetos a secreto profesional
- Conlleva una reversión no autorizada de la pseudonimización
- Otro perjuicio económico o social

En el presente caso, es evidente que se accedieron a datos de nombre, apellidos y dirección postal, pero que, además, el consultante también conocía el NIF de los titulares de los datos; por lo que, sí existió riesgo para los derechos de las personas dado que existió riesgo de suplantación o usurpación de la identidad.

En consecuencia, se desestiman las alegaciones presentadas.

III
Artículo 5.1.f) del RGPD

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"1. Los datos personales serán:
(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

En el presente caso, consta que los datos personales de la parte reclamante, obrantes en la base de datos del CATASTRO, fueron indebidamente expuestos a terceros, vulnerándose el principio de confidencialidad.

Según consta en el expediente, la violación de seguridad sufrida por la Dirección General del Catastro estuvo ocasionada por la exposición en la internet pública de un formulario al que solo se debía acceder previa identificación del usuario en sede electrónica.

Este formulario permitía que al rellenarse el campo NIF con un valor válido se autocompletaba de manera automática los campos nombre, apellidos y domicilio de la persona a la que hacía referencia esta NIF.

El CATASTRO no ha respetado el principio de confidencialidad, puesto que, a dicho formulario sólo se accedía previa identificación en sede electrónica, y se autocompletaba automáticamente rellenando el campo NIF con un valor válido, exponiéndose de manera automática los campos relativo al nombre, apellidos y domicilio de la persona a la que correspondía dicho NIF.

IV
Tipificación de la infracción del artículo 5.1.f) del RGPD

La citada infracción del artículo 5.1.f) del RGPD supone la comisión de la infracción tipificada en el artículo 83.5 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que:

"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"

V
Artículo 32 del RGPD

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

En el presente caso, en el momento de producirse la brecha de seguridad, no consta que el CATASTRO dispusiese de medidas de seguridad razonables en función de los posibles riesgos estimados.

La exposición en la internet pública de un formulario al que solo se debía acceder previa identificación del usuario en sede electrónica no cumple con las mínimas medidas de seguridad razonables. Este formulario permitía que al rellenarse el campo NIF con un valor válido se autocompletaban de manera automática los campos nombre, apellidos y domicilio de la persona a la que hacía referencia esta NIF.

En consecuencia, la exposición de dicho formulario no garantiza la confidencialidad, integridad y disponibilidad de los sistemas y servicios del tratamiento ni la finalidad del tratamiento.

Ha quedado constatado en el expediente, que la exposición indebida del formulario en internet no fue detectada en las pruebas previas del sistema, esto fue debido a que las pruebas realizadas consistieron en verificar que no se mostraban datos catastrales a los usuarios no autenticados en sede, pero no se comprobaba que tampoco se cumplimentara de forma automática los campos del formulario, evidenciando que las pruebas realizadas para la puesta en funcionamiento de la funcionalidad no fueron suficientes o adecuadas.

Tras el conocimiento de la violación de seguridad se adoptaron las siguientes medidas:

- Se fuerza a que el usuario esté identificado en la sede electrónica y con los permisos de “gerencia” habilitados para poder mostrarse el formulario.

- Para todas las páginas que tienen características similares al formulario se implementa la funcionalidad por la que se comprueba que si el usuario que intenta acceder no tiene permisos adecuados no se le muestra la página, indicando que su sesión ha caducado y forzando así que se tenga que autenticar con los permisos correctos.

- Se añaden en todas las páginas un metadato facilitado por Google para poder solicitarle la eliminación de la cache del buscador cualquier URL solicitada.

VI
Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de la infracción tipificada en el artículo 83.4 del RGPD que bajo la rúbrica “*Condiciones generales para la imposición de multas administrativas*” dispone:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)”*

A este respecto, la LOPDGDD, en su artículo 71 *“Infracciones*” establece que *“Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*”.

A efectos del plazo de prescripción, el artículo 73 “*Infracciones consideradas graves*” de la LOPDGDD indica:

“En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> *(…)*
> *f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.*

VII
Artículo 33 del RGPD

El artículo 33 "*Notificación de una violación de la seguridad de los datos personales a la autoridad de control*" del RGPD dispone:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo".

En el presente supuesto, el CATASTRO no notificó la brecha de seguridad en el plazo establecido en el RGPD a tal efecto, con las informaciones establecidas en el artículo 33 del RGPD; puesto que, consideró que no existió riesgo para los derechos y libertades de las personas afectadas, para ello han tenido en cuenta el volumen de datos filtrados (575 consultas), la tipología de datos (nombre, apellidos y dirección) y el tiempo que lleva el formulario en producción (desde 2016).

No obstante, en el transcurso de esta investigación se hace uso de la herramienta de la AEPD "Asesora Brecha" con los siguientes datos de entrada y obteniendo como resultado la "Obligación de notificar la violación de seguridad":

- El incidente ha afectado a la confidencialidad.

- El incidente ha sucedido por un fallo, ausencia o vulneración de medidas de seguridad.
- Existe la probabilidad de que la brecha suponga algún riesgo sobre los derechos y libertades de las personas ya que se ha producido la pérdida de control de los datos personales de las personas afectadas en las 575 consultas detectadas.

En relación con las personas afectadas, el CATASTRO afirma que tras revisar los logs internos se han detectado 575 consultas desde que se activó el formulario en 2016.

Se accedió a datos de nombre, apellidos y dirección postal, pero el consultante también conocía el NIF de los titulares de los datos; por lo que, sí existió riesgo para los derechos de las personas dado que existió riesgo de suplantación de la identidad.

Por otro lado, los consultantes no estaban logados por lo que se desconoce quiénes accedieron a los datos, así como la situación particular de los titulares de los datos personales a los que se accedieron.

Además, dependiendo de la situación de los titulares de los datos personales, esta pérdida de confidencialidad pudo generar mayores riesgos para los derechos y libertades de las personas.

VIII
Tipificación de la infracción del artículo 33 del RGPD

La citada infracción del artículo 33 del RGPD supone la comisión de la infracción tipificada en el artículo 83.4 del RGPD que bajo la rúbrica “Condiciones generales para la imposición de multas administrativas” dispone:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)”

A este respecto, la LOPDGDD, en su artículo 71 “Infracciones” establece que “Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica”.

A efectos del plazo de prescripción, el artículo 73 “Infracciones consideradas graves” de la LOPDGDD indica:

“Se consideran graves y prescribirán a los dos años las infracciones que supongan una
vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

"(…)
r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679. (…)",

IX
Sanción por la infracción de los artículos 5.1 f), 32 y 33 del RGPD

El Artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD apartado 7 establece:

"Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro."

Asimismo, el artículo 77 "Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados: ...

> *c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local…*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

A la vista de lo expuesto se procede a emitir la siguiente

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a la DIRECCIÓN GENERAL DEL CATASTRO, con NIF S2826053G, por una infracción del artículo 5.1.f) del RGPD tipificada en el artículo 83.5 del RGPD por una infracción del Artículo 32 del RGPD y del Artículo 33 del RGPD tipificadas en el Artículo 83.4 del RGPD, una sanción de apercibimiento por cada una de las infracciones.

SEGUNDO: NOTIFICAR la presente resolución a la DIRECCIÓN GENERAL DEL CATASTRO.

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso

contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-21112023

Mar España Martí
Directora de la Agencia Española de Protección de Datos