907-141019

- **Expediente Nº: E/02564/2019**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 4 de febrero de 2019 la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación en relación a la notificación de una brecha de seguridad realizada por AIR EUROPA LÍNEAS AÉREAS, S.A. relativa al acceso no autorizado a la información de contacto y tarjetas bancarias que afecta a 489000 interesados y un volumen de 1500000 registros.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

1. AIR EUROPA aporta un informe de auditoría realizado por IBM X-FORCE IRIS y fechado a 20 de diciembre de 2018 con las siguientes manifestaciones:

   En el apartado de "Antecedentes del Incidente" se manifiesta:

   > *"En octubre de 2018, GLOBALIA fue informada por las compañías de las tarjetas de crédito de que un gran número de tarjetas de crédito, unas 4000, habían sido utilizadas para cometer fraude. Los datos robados incluían datos personales y financieros de los clientes de GLOBALIA que realizaron reservas y modificaciones en AirEuropa.com. Los datos no incluían datos de viaje ni de pasaporte."*

   Manifestaciones en el resto del documento de auditoría:

   a. "E*l primer acceso confirmado a la red de GLOBALIA por parte del atacante tuvo lugar a través de la pasarela de acceso CITRIX mediante el uso de credenciales válidas para una cuenta desconocida el día 12 de mayo de 2018."*

   b. "*Tras este acceso inicial, el atacante comprometió una serie de sistemas de GLOBALIA e IRIS considera que el atacante siguió accediendo a los sistemas y cuentas de GLOBALIA al menos hasta el 11 de agosto de 2018.*"

   c. "*Aunque IRIS no ha logrado confirmar cómo logró el atacante exfiltrar información de la red de GLOBALIA o qué fue exfiltrado, habida cuenta de la limitación de registros, lo que sí ha confirmado IRIS es que el atacante había recopilado al menos 488847 tarjetas de crédito únicas"*

d. *“A partir de la muestra de 4939 tarjetas de crédito únicas ya declaradas fraudulentas, se encontraron 1185 en la recopilación anteriormente mencionada.”*

e. *“El atacante visualizó y archivó en SNMIDSRVPRD02 al menos 2651 números de tarjeta únicos, CVVs, fechas de vencimiento y nombres de titular de la tarjeta.”*

f. “*En total el atacante comprometió al menos 12 sistemas y un mínimo de 2 cuentas de servicio en apoyo de su operación*”

g. “*Para el acceso inicial, el atacante se aprovechó de la falta de Doble Autenticación (2FA) de la pasarela de acceso CITRIX para conseguir acceder a la red por vez primera”*

h. *“Todo sistema expuesto a Internet, como CITRIX, VPN y Office365, debería tener ejecutada Autenticación Multifactorial.”*

i. *“Asimismo, las investigaciones posteriores de las cuentas comprometidas por el atacante, como la cuenta de servicio GLOBALIA\EJP, reveló que utilizaba una contraseña que no cumplía los requisitos de complejidad y longitud en línea con la práctica óptima del sector, cosa que habría hecho que al atacante le resultara más fácil comprometer esta cuenta.”*

j. *“Aunque IRIS no logró confirmar los datos relativos al modo en que el atacante exfiltró información debido a la limitación de registros, algunos datos de la investigación indican el momento en que pudieron tomarse los datos y desde dónde. Habida cuenta de que la mayoría de los datos sensibles que fueron recopilados por el atacante fue encontrada o transferida al servidor SNMIDSRVPRD02, y que el servidor también contaba con el único mecanismo viable de persistencia, es probable que el atacante usara SNMIDSRVPRD02 como servidor de pruebas desde el que exfiltrar información. De igual forma, un análisis estadístico de los registros del cortafuegos reveló que el mayor número de conexiones a la dirección IP controlada por el atacante, 5.8.18[.]50, desde los sistemas de GLOBALIA, tuvo lugar entre el 14 de mayo y el 4 de junio, con un pico del 19 al 21 de mayo, lo que indica que el atacante se puso manos a la obra. Visto el volumen de actividad, es posible que también tuviera lugar la exfiltración de los datos durante estos marcos temporales, aunque el hecho de que el atacante accediera a archivos específicos relacionados con las tarjetas de crédito posteriormente, en junio, podría indicar que la exfiltración también tuvo lugar posteriormente en el mismo mes.”*

k. “*Para mantener el acceso a la red, el atacante usó herramientas públicamente disponibles, de código abierto, como Metasploit, para establecer puertas traseras en los sistemas que se comunicaban con la dirección IP controlada por el atacante 5.8.18[.]50.*”

l. “N*o se observó más actividad maliciosa referente al mismo atacante o actor de amenazas tras el 11 de agosto de 2018”*

m. *“La dirección IP controlada por el atacante fue bloqueada el 15 de noviembre.”*

n. *"Se observó una configuración de registros irregular en los sistemas analizados, de forma que únicamente algunos sistemas almacenaban archivos de registros archivados localmente; por ejemplo, los scripts ejecutados por Powershell se registraban únicamente en algunos sistemas.*

Los registros de auditoría son importantes durante una incidencia de seguridad para reconstruir las actividades del atacante…

…

Por consiguiente, se recomienda revisar la política actual de auditoría y retención y aplicarla uniformemente en todo el entorno. Si no se emplea ya, también se recomienda valorar la posibilidad de centralizar la recopilación de registros en una plataforma exclusiva, como un producto de Gestión de Incidencias e Información de Seguridad (SIEM), …"

o. *"Aunque no ha sido posible determinar exactamente la fuente de la infección de los sistemas en alcance, una de las hipótesis más probables es que los sistemas se vieran infectados por una segregación insuficiente entre el entorno de oficina y el entorno de producción gestionando los datos de las tarjetas de pago."*

p. *"Bloquear y supervisar el tráfico de salida a direcciones IP externas sospechosas es una buena forma de detectar un comportamiento anormal que se origine en la red.*

…

En este incidente hemos visto servidores críticos, como ST-CONEXFLOW, comunicarse con direcciones IP externas que no se hallaban relacionadas con ningún sistema de pago, ni tampoco estaban justificadas por otras necesidades comerciales."

q. *"Durante la investigación, IRIS observó diversos sistemas con funcionamiento más largo de un año, con lo que los sistemas operativos no contaban con parches para un periodo tan largo."*

2. Se aporta un calendario de tareas técnicas acometidas para el cierre de la brecha y las mejoras de protección implantadas que ha tenido en consideración, según manifestación de AIR EUROPA, las medidas y recomendaciones emitidas por IBM tras el análisis del incidente de seguridad. Este calendario alberga tareas comprendidas entre el 14 de noviembre de 2018 y el 13 de febrero de 2019 y se clasifican en los siguientes grupos:

   a. Actualización de servidores PCI.

   b. Restricción reglas de firewall.

   c. Bloqueo y registro de IP maliciosa.

   d. Limpieza de usuarios locales entorno PCI.

   e. Cambios de contraseña.

      - Se fuerza una política de contraseñas compleja con una longitud mínima de 8 caracteres, uso de números, caracteres especiales,

mayúsculas y minúsculas, expiración en 90 días y no repetición de las 3 últimas.

f. Antivirus.

g. Aplicación SIEM. El incidente ocurrió estando en proceso de integración del software SIEM WAZUH.

h. Parcheo de vulnerabilidades y actualización de servidores involucrados en el incidente.

i. Instalación agente Carbon Black.

j. Cifrado de las comunicaciones internas PCI. Se aplican medidas para cifrar todas las comunicaciones internas que no lo estaban dentro del entorno PCI.

k. Replataformado de servidores PCI.

l. Configuración TOMCAT. El servidor TOMCAT arrancaba con permisos de administración. Se cambia para usar un usuario propio.

3. AIR EUROPA manifiesta que ha recibido únicamente 20 comunicaciones de clientes debidas, en su mayoría, a incomodidades derivadas de la cancelación de la tarjeta por su entidad bancaria, sin que manifestaran ningún tipo de daño económico sufrido, y a través de las cuales solicitan mayor información. Que únicamente 3 de ellas manifestaban haber sufrido algún tipo de perjuicio económico fruto de la utilización, por terceros, de los datos personales obtenidos a través del ataque. Desde AIR EUROPA se ha dado respuesta atendiendo los requerimientos de información solicitados por los interesados.

4. Aporta análisis de riesgos respecto de las medidas de seguridad en el tratamiento de los datos de venta online a pasajeros de AIR EUROPA el cual consiste en un documento de una página que analiza 9 riesgos.

5. Aporta análisis de riesgos efectuado respecto de la necesidad o no de notificación a esta Agencia y a los interesados. En este análisis se manifiesta:

   a. El art. 34.3 del GDPR establece tres excepciones a la obligación de notificar a los interesados:

      - Respecto al 34.3.a):

        "*En relación a los sistemas de AIR EUROPA, no existían medidas específicas, como el cifrado o la tokenización, que protegiese los datos a los que accedieron los atacantes. Sin embargo, la información a la que accedieron los atacantes no incluye información sensible como categorías especiales de datos personales, direcciones postales o números de teléfono, número de pasaporte o DNI o fecha de nacimiento. Esta información sensible no se almacena junto con la información de tarjetas bancarias como medida de seguridad. Como resultado, es muy difícil identificar individuos únicos dentro del conjunto de datos.*"

      - Respecto al 34.3.b):

"…una vez identificado el incidente por las entidades bancarias, estas y los emisores de las tarjetas bancarias comprometidas procedieron a bloquear e informar de dicho bloqueo a los interesados de manera que los datos comprometidos quedasen inutilizados…"

Se aporta modelo de comunicación realizado por la entidad Bankinter a sus clientes.

- Respecto al 34.3.c):

"*…es prácticamente imposible identificar de forma única a los interesados a partir de este conjunto de datos, ya que no dispone de los datos de contacto de los mismos.*

Por lo tanto si se determina que debe realizarse una notificación a los interesados, AIR EUROPA tendría que realizar una comunicación pública en lugar de notificaciones individuales. Desde AIR EUROPA se entiende que en este momento resulta más gravoso para los intereses generales y los de los interesados realizar una comunicación pública, al no existir ningún beneficio derivado de esa comunicación."

b. Que, según la metodología de análisis de la AEPD el resultado cuantitativo no superaría el umbral establecido para dicha notificación (30 vs 40) mientras que el umbral cualitativo sí se vería superado. Sin embargo y teniendo en cuenta lo anterior, AIR EUROPA ha decidido no notificar a los interesados argumentando que el incidente no es susceptible de suponer un alto riesgo para los derechos y libertades de los mismos.

c. Que en aquellos casos en que se pudiera observar un alto riesgo podrían aplicarse una o más excepciones de las recogídas en el art. 34 RGPD. En este sentido aplicarían las previstas en el art. 34.3 a) y b).

Con fecha 14 de noviembre de 2019, AIR EUROPA remite a esta Agencia la siguiente información y manifestaciones:

1. Que el 100% del capital social de AIR EUROPA pertenece a GLOBALIA CORPORACIÓN EMPRESARIAL, S.A. Que en AIR EUROPA existe un equipo responsable de los sistemas de información encabezado por la figura del CIO. A nivel operativo las funciones relacionadas con el aprovisionamiento de infraestructura y administración de los sistemas de información y comunicaciones son provistas por GLOBALIA SISTEMAS Y COMUNICACIONES S.L.U., sociedad que pertenece en un 100% a GLOBALIA CORPORACIÓN EMPRESARIAL, S.A.
2. Aporta copia firmada de contrato de asistencia y gestión en el área de sistemas de información y comunicaciones fechado a 31 de octubre de 2009 entre AIR EUROPA LINEAS AÉREAS, S.A.U. y GLOBALIA SISTEMAS Y COMUNICACIONES, S.L.U. donde se manifiesta, entre otros:
    a. Que GLOBALIA SISTEMAS asistirá a AIR EUROPA en las áreas de sistemas de información y telecomunicaciones.

b. Que el servicio a prestar por GLOBALIA SISTEMAS tendrá un carácter integral, de forma que permita a AIR EUROPA la externalización total de los servicios en las áreas de sistemas de información y comunicaciones.

c. Que GLOBALIA SISTEMAS realizará por propia iniciativa las gestiones y tareas oportunas para le desarrollo de las prestaciones anteriormente identificadas. No obstante lo anterior, GLOBALIA SISTEMAS someterá a la aprobación de AIR EUROPA los proyectos a desarrollar y rendirá cuentas de las gestiones en el curso de reuniones organizadas, de mutuo acuerdo, con una periodicidad no superior a la trimestral.

3. Aporta copia firmada de novación al contrato de encargado de tratamiento de datos personales fechado a 31 de octubre de 2019, según el cual, GLOBALIA SISTEMAS Y COMUNICACIONES, S.L.U. es el encargado del tratamiento y AIR EUROPA LINEAS AÉREAS, S.A.U. es el responsable del tratamiento.

4. Aporta copia del Plan de Respuesta ante Incidentes de Ciberseguridad de GLOBALIA con fecha de entrada en vigor del 5 de julio de 2019 en su primera versión según indica el control de versiones del documento y la portada del documento.

5. Que el informe forense de FOREGENIX es un informe que requieren por norma los bancos en nombre de las entidades de pago que son miembros del PCI Council (como sería el caso de VISA) a las entidades afectadas por un incidente, con el fin de evaluar lo ocurrido en relación con el cumplimiento respecto del estándar PCI DSS (“Payment Card Industry Data Security Standard”)

6. Que el informe forense de FOREGENIX tiene un objeto muy específico y está orientado en el marco de identificar el volumen de tarjetas identificadas como comprometidas, lo cual determina por norma general la compensación económica que el PCI Council pueda requerir a la entidad afectada por el incidente.

   Aporta informe forense de FOREGENIX fechado a enero de 2019 y basado en la investigación iniciada en fecha 25 de octubre de 2018 el cual contiene las siguientes manifestaciones, entre otras:

   a. “*La investigación realizada por FOREGENIX identificó pruebas concluyentes de violación en AIR EUROPA”*

   b. *“La investigación de FOREGENIX identificó más de 2,7 millones de números de tarjeta únicos que habían sido extraídos de los sistemas de bases de datos por el atacante. Aunque algunos de los datos de las tarjetas estaban encriptados mientras estaban en reposo dentro del entorno de la empresa, el atacante consiguió utilizar herramientas de descifrado presentes en los sistemas para obtener daros de texto claros.”*

   c. *“La intrusión probablemente tuvo su origen en sistemas inseguros disponibles a través de internet. FOREGENIX identificó varios dispositivos que no se habían parcheado con regularidad…”*

   d. “Resumen de posibles causas y lista de vectores de ataque:

Host- El sistema tiene acceso de red/Internet sin restricciones. El código del atacante consiguió conectarse directamente el servidor C&C.

Host- Sistema no parcheado/mantenido. Múltiples sistemas comprometidos no habían sido parcheados durante más de 6 meses.

Red- Sin segmentación de redes. Aunque había ACLs y segmentos, el atacante pudo "pivotar" la entrada en el CDE a través de servidores que tenían acceso a los servidores PCI.

Red- Sin monitorización de seguridad. Se hallaron múltiples indicadores que podrían haber advertido de la violación a AIR EUROPA antes del momento de su detección."

e. Existen pruebas de violación del entorno de datos de los titulares de las tarjetas.

f. "E*l ataque comenzó al acceder el atacante al entorno PCI desde un servidor no adecuadamente segmentado en el ámbito PCI".*

g. "El atacante tenía una conexión sistemática con un host externo. Debido a la falta de registro, FOREGENIX no identificó todas las transmisiones de datos fuera de la red. Sin embargo, sí visualizó cómo el atacante creaba varios archivos y posteriormente los comprimía en un solo archivo. Esta acción se realizaba frecuentemente inmediatamente antes de la transmisión/exfiltración de datos."

h. Posible exposición de tipos de datos, entre otros; nombre del titular de tarjeta, dirección de titular de tarjeta, fecha de vencimiento.

i. Que el número total de tarjetas expuestas son 2722692, no siendo ése el número de tarjetas que están en riesgo.

7. Que, en relación al motivo de la no detección de la brecha hasta el 16 de octubre de 2018 a pesar de que el ataque se inició el 12 de mayo de 2018, AIR EUROPA manifiesta que la brecha se produjo como consecuencia de una APT, un ataque dirigido y sofisticado, planificado y ejecutado de una forma profesional y alevosa.

   Así mismo manifiesta que:

   "el ataque sufrido por la Sociedad es un tipo de "*ataque […] diseñado para perdurar en el tiempo y conseguir evadir todas las medidas de seguridad de las plataformas más usuales"* tal y como describe el INCIBE en un artículo publicado en su portal a fecha 16 de junio de 2016 y firmado por A.A.A.. Es, por tanto, un tipo de ataque sigiloso y que busca como fin último filtrar información sensible de una organización y borrar las huellas a la finalización, lo que los hace extremadamente difíciles de detectar"

8. Manifiesta que las fechas clave del proyecto de elaboración del Plan Director de Seguridad (PDS) son:

   a. Julio 2019: definición del alcance preliminar de los servicios de negocio que se evaluarán para el desarrollo del PDS.

   b. 11 de septiembre de 2019: reunión de lanzamiento.

   c. 31 de enero de 2019: cierre de proyecto.

d. 3 de febrero de 2020: entrada en vigor del PDS.

9. Aporta un documento con título “Procedimiento de actualizaciones críticas y de seguridad” y manifiesta que este procedimiento se viene aplicando de forma habitual desde antes del incidente.

   a. En este documento se manifiesta en el apartado de servidores Windows, subapartado de Instrucciones para sistemas con función de servidor (web servers, servidores de bases de datos, etc).

      “…*se actualizan 2 veces al año. Manualmente cada 6 meses en producción.”*

   b. En este documento se manifiesta en el apartado de servidores NO Windows, subapartado de Instrucciones para servidores backend Solaris.

      “*Son actualizados manualmente en producción cada 6 meses.”*

   c. En este documento se manifiesta en el apartado de servidores NO Windows, subapartado de Instrucciones para resto de servidores (Apache, Linux, etc).

      “*bajo demanda en producción. No está establecida como tarea periódica.”*

10. Aporta el Manual de Seguridad de la Información de AIR EUROPA con fecha de última modificación del documento el 31 de octubre de 2013 siendo el objeto de este documento responder a la obligación establecida en el artículo 9 de la Ley Orgánica 15/1999.

11. Manifiesta que “*resulta relevante manifestar, como dato importante a efectos de ratificar la inexistencia de perjuicios efectivos relevantes, que el número de reclamaciones recibidas por parte de usuarios de la Compañía que pudieran estar relacionados con el incidente ha sido muy pequeño (2 reclamaciones en total sin solicitud de compensación). Ello confirma el análisis de que los atacantes no han podido conseguir información sensible o relevante y que, con la información que pudieran haber sustraído, la existencia de numerosas medidas de seguridad técnicas y organizativas en toda la cadena de procesos (incluyendo las entidades intervinientes en los servicios de pago) ha hecho que esa información no se pueda haber utilizado para causar perjuicios graves.*”

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD) determina lo siguiente, respecto a las actuaciones previas de investigación:

"1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en la Sección 2.ª del Capítulo I del Título VII de esta ley orgánica y no podrán tener una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa o como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.3 de esta ley orgánica."

III

Por su parte, el artículo 25 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) en su apartado 1.b) establece que:

"1. En los procedimientos iniciados de oficio, el vencimiento del plazo máximo establecido sin que se haya dictado y notificado resolución expresa no exime a la Administración del cumplimiento de la obligación legal de resolver, produciendo los siguientes efectos:

(…) b) En los procedimientos en que la Administración ejercite potestades sancionadoras o, en general, de intervención, susceptibles de producir efectos desfavorables o de gravamen, se producirá la caducidad. En estos casos, la resolución que declare la caducidad ordenará el archivo de las actuaciones, con los efectos previstos en el artículo 95".

En el presente supuesto el cómputo de los doce meses de duración máxima de las actuaciones previas E/02564/2019 se inició el día 4 de febrero de 2019 y, actualmente, aún están pendientes de finalización, por lo que deben declararse caducadas.

Todo ello de conformidad con la interpretación que al respecto ha realizado la Audiencia Nacional en su Sentencia de 19 de julio de 2013, en la que establece que "*el hecho de que tras la denuncia se acordara por el Director de la Agencia Española de Protección de Datos no incoar actuaciones inspectoras y no iniciar procedimiento sancionador, para a continuación, en respuesta al recurso de reposición formalizado por el denunciante contra tal acuerdo, resolver su estimación y ordenar a la Subdirección General de Inspección de Datos que se procediera a realizar actuaciones de inspección, no enerva aquella conclusión*". Esto es, que las

actuaciones previas de investigación deben entenderse caducadas si transcurridos doce meses desde el día inicial del cómputo no se ha procedido a dictar y notificar acuerdo de inicio de procedimiento sancionador.

IV

No obstante, el artículo 95.3 de la citada LPACAP, determina que:

"La caducidad no producirá por sí sola la prescripción de las acciones del particular o de la Administración, pero los procedimientos caducados no interrumpirán el plazo de prescripción.

En los casos en los que sea posible la iniciación de un nuevo procedimiento por no haberse producido la prescripción, podrán incorporarse a éste los actos y trámites cuyo contenido se hubiera mantenido igual de no haberse producido la caducidad. En todo caso, en el nuevo procedimiento deberán cumplimentarse los trámites de alegaciones, proposición de prueba y audiencia al interesado."

Al respecto la Audiencia Nacional considera (Sentencia de 10 de julio de 2013) que "*declarada la caducidad de las actuaciones previas de investigación iniciadas por la Agencia Española de Protección de Datos, tal circunstancia no supone obstáculo alguno para que dicha entidad proceda a iniciar o reiniciar otras actuaciones previas de investigación sobre los mismos hechos, siempre y cuando no hubiere transcurrido el plazo de prescripción de la infracción administrativa objeto de investigación*".

En consecuencia, dado que los hechos objeto de investigación no se encuentran prescritos, se dan instrucciones a la Subdirección General de Inspección de Datos para que inicie nuevas actuaciones de investigación.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: ABRIR nuevas actuaciones de investigación e incorporar a estas nuevas actuaciones la documentación que integra las actuaciones previas que se declaran caducadas mediante el presente acto.

TERCERO: NOTIFICAR la presente Resolución a **AIR EUROPA LINEAS AEREAS S.A.** y ***DE OFICIO.***

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

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