- Procedimiento Nº: PS/00179/2020

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha de 04/02/2019 la Directora de la Agencia Española de Protección de Datos acuerda iniciar actuaciones de investigación en relación a la notificación de una brecha de seguridad realizada por AIR EUROPA LÍNEAS AÉREAS, S.A., con CIF ***CIF.1** (en lo sucesivo AIR EUROPA), relativa al acceso no autorizado a la información de contacto y tarjetas bancarias que afecta a 489.000 interesados y un volumen de 1.500.000 registros.

No obstante, en fecha 28/02/2020, se acordó abrir nuevas actuaciones de investigación a AIR EUROPA e incorporar a éstas la documentación que integraban las actuaciones previas del expediente E/02564/2019, que se declararon caducadas.

La notificación de brecha de seguridad se efectuó en fecha 28/11/2018 y el 22/01/2019 como notificación inicial y completa.

Posteriormente, el 22/01/2019 se efectúa otra notificación para corregir información aportada, según manifiesta AIR EUROPA, a discrepancias entre el acuse de recibo emitido por la sede electrónica de esta Agencia y los datos efectivamente introducidos en el formulario online. Las tres notificaciones contienen, entre otra, la siguiente información:

- Que en fecha 27/11/2018 se intentó en repetidas ocasiones notificar de manera inicial a esta Agencia a través del formulario habilitado al efecto en sede electrónica pero el procedimiento online de notificación imposibilitó la presentación por dicho medio, procediéndose a la presentación de manera inicial y presencial en fecha 28/11/2018.
- Responsable del tratamiento: AIR EUROPA cuyos datos se han incluido en el apartado de Entidades Investigadas.
- Fecha de detección de la brecha: ***FECHA.1**
- Medios de detección de la brecha: AIR EUROPA recibe una notificación por parte del Banco Popular relativo a un potencial incidente de seguridad, lo que determina la activación del plan de respuestas ante incidentes por parte de AIR EUROPA, el día 17/10/2018.
- Fecha de inicio de la brecha: 12/05/2018
- Brecha resuelta a 17/11/2018.
- Justificación de la notificación tardía: N/A
- Resumen del incidente: el incidente de seguridad ha comportado el acceso no autorizado a información de tarjetas bancarias, numeración, fecha de

caducidad y CVV que se podría haber utilizado para la comisión de operaciones fraudulentas. Si bien todas las identificadas fueron canceladas antes de que conste que se haya producido algún perjuicio para los interesados.

En algunos casos (aproximadamente 2500) la identidad de los titulares de las tarjetas bancarias también ha sido comprometida.

- Tipología: Brecha de confidencialidad (acceso no autorizado).
- Medio por el que se ha materializado la brecha: Hacking y malware.
- Contexto: Externa (acción intencionada)
- Que antes de la brecha se aplicaron las siguientes medidas preventivas:

  Seguridad en la red:

  Equipo humano propio con experiencia superior a 10 años en gestión y administración de redes, LAN y WAN.

  La empresa ha diseñado y facilitado formación a los empleados sobre el uso de las herramientas puestas a su disposición conforme a la legislación vigente.

  AIR EUROPA utiliza ***1.-[……]***.

  De forma periódica ***(XXX)*** se ejecuta un programa de evaluación de vulnerabilidades para monitorizar potenciales brechas de seguridad en vulnerabilidades conocidas.

  Adicionalmente a los sistemas de firewall que permiten gestionar y bloquear accesos no autorizados, se dispone de un ***2.-[……].***

  Para proteger la navegación del usuario se dispone de un ***3.-[……].***

  Protección de la información y controles de acceso:

  El acceso a los sistemas de información requiere la identificación y autenticación de todos los usuarios ***4.-[……] (XX).***

  *El **XX*** está conectado con el sistema ***5.-[……]***.

  Existe una política de renovación de contraseñas por la cual se ven obligados a cambiar la misma cada ***XXX***.

  La política de ***6.-[……]***.

  Las políticas de gestión de permisos de acceso a las aplicaciones ***7.-[……]*** permitiendo aplicar el principio de mínimo privilegio.

  Prevención:

  AIR EUROPA inició hace unos meses un proceso destinado a confeccionar un Plan Director de Seguridad con objeto de tener un escenario más amplio de amenazas y definir una estratega más eficaz. ***8.-[……].***

- Que las categorías de datos afectados son datos básicos e información sobre tarjetas bancarias como el número, fecha de caducidad y CVV.
- Que no hay categorías especiales de datos afectados.
- Que le número aproximado de registros de datos afectados son 1.500.000

- Que el perfil de los sujetos afectados son clientes siendo el número aproximado de personas afectadas 489.000.
- Que la naturaleza del impacto potencial sobre los sujetos es el fraude.
- Que las posibles consecuencias es la divulgación a terceros/difusión en internet y que los datos pueden ser explotados con otros fines.
- Que cataloga la severidad de las consecuencias como “Media”.
- Que las medidas tomadas para solucionar la brecha y minimizar el impacto fue:
    - Realización de una investigación preliminar.
    - Contratación de una empresa forense ******EMPRESA.1*** para la prestación de soporte y ayuda en el análisis del incidente.
    - Contratación de empresa especialista en análisis y resolución de incidencias ******EMPRESA.2.***
    - Seguimiento de tareas y planificación de mejoras y acciones a implantar en los sistemas con el fin de ir “cerrando puertas” y disminuir el riesgo.
    - Revisión del conjunto de las medidas de seguridad y refuerzo de las mismas.
    - Cronología de las actuaciones seguidas descritas en documentos adjuntos.
- Que los interesados no serán informados por los siguientes motivos:
    - Únicamente se tiene constancia de 11 peticiones de información por parte de clientes en relación a este evento y se está dando respuesta a todos ellos. Se desconoce la existencia de otros afectados.
    - Que se han adoptado las medidas de protección técnicas y organizativas apropiadas que garantizan que ya no existe la probabilidad de que se materialice ningún riesgo para los derechos y libertades de los interesados afectados por la violación de seguridad.
    - Que entienden que en este momento resulta más gravoso para los intereses generales y los de los interesados realizar una comunicación pública ya que no disponen de información de contacto de todas las personas afectadas.
- Se aportan documentos adjuntos que contienen, entre otras, las siguientes manifestaciones:
    - Que de forma inmediata tras el conocimiento de la brecha se contrató a la compañía especializada en brechas de seguridad y análisis forense y ******EMPRESA.3.***
    - Se contrató a la empresa ******EMPRESA.2*** con el propósito de analizar el alcance, conjuntamente con ******EMPRESA.3***, y aplicar las medidas necesarias para corregir la incidencia.
    - Que el alcance de la brecha no es todavía conocido de forma completa. El incidente de seguridad ha comportado el acceso no autorizado. Se

realiza esta notificación de forma preliminar para ir aportando la información que se dispone hasta el momento.

- Que se adoptaron una serie de medidas de índole técnico que se llevaron a cabo poniendo el foco en primer lugar en actividades de contención y seguidamente en actividades preventivas.
- Que después de haber analizado la información que AIR EUROPA cree haber sido comprometida, resulta muy poco probable que únicamente se hayan visto afectados interesados españoles. Sin embargo, AIR EUROPA no se encuentra actualmente en posición de identificar las nacionalidades específicas de todos los interesados afectados.
- Cronología de las actuaciones seguidas:
  - ******FECHA.1***. AIR EUROPA recibe una notificación por parte de VISA (Banco Popular) relativa a un potencial incidente de seguridad lo que determina la activación del Plan de Respuestas ante Incidentes (PRI) el día 17 de octubre de 2018.
  - 18/10/2018. Como parte del PRI se contacta con la empresa ******EMPRESA.3*** para la prestación de soporte y ayuda en el análisis forense del incidente cuya contratación tuvo lugar el 22 de octubre de 2018.
  - 24/10/2018 al 31/10/2018. Recogida de evidencias e información necesaria.
  - 05/11/2018 al 08/11/2018. Análisis de la información recogida. El día 8/11 se confirma por el analista forense la existencia de una brecha.
  - 08/11/2018. Se contacta con ******EMPRESA.2*** con el objetivo de reforzar los equipos internos de seguridad y trabajar conjuntamente con ******EMPRESA.3***.
  - 09/11/2018. Comienzan los trabajos de ******EMPRESA.2*** para ir “cerrando puertas” y disminuir el riesgo progresivamente.
  - 14/11/2018. Se inician las tareas de revisión del conjunto de medidas de seguridad y, según proceda, reforzar las mismas.

    Por parte de ******EMPRESA.2*** y el equipo forense se identifica que desde un servidor se está contactando con una IP no reconocida.
  - 15/11/2018. AIR EUROPA recibe instrucciones concretas desde el equipo forense con 8 medidas destinadas a contener el problema. Con el apoyo del equipo de ******EMPRESA.2*** se asigna prioridad máxima a las tareas de contención.
  - 17/11/2018. Confirmación por parte de ******EMPRESA.2*** y ******EMPRESA.3*** de que la brecha está contenida.
  - 23/11/2018. Se confirma por parte de ******EMPRESA.2*** la realización del 90% de las acciones de contención y protección y que las tareas pendientes quedan a finalizar en los próximos

días. Se confirma la efectividad de las medidas de monitorización en tiempo real que se siguen desplegando para garantizar la detección de cualquier intrusión.

SEGUNDO: la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

Con fecha 01/04/2019, AIR EUROPA remite a esta Agencia la siguiente información y manifestaciones:

1. Se aporta un informe de auditoría realizado por ******EMPRESA.4*** y fechado a 20/12/2018 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 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* ******ARCHIVO.1*** *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* ***9.-[…….]*** *para conseguir acceder a la red por vez primera*"

   h. *"Todo sistema expuesto a Internet,* ***10.-[…….]****."*

   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* ******ARCHIVO.1****, y que el servidor también contaba con el único mecanismo viable de persistencia, es probable que el atacante usara* ******ARCHIVO.1*** *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,* ******IP.1****, 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* ***11.-[…….]*** *en los sistemas que se comunicaban con la dirección IP controlada por el atacante* ******IP.1****.*"

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), …"

a. *"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* ***12.-[…….]****."*

b. *"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 **13.- [……],** comunicarse con direcciones IP externas que no se hallaban relacionadas con ningún sistema de pago, ni tampoco estaban justificadas por otras necesidades comerciales."*

a. *"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 ******EMPRESA.2*** tras el análisis del incidente de seguridad. Este calendario alberga tareas comprendidas entre el 14/11/2018 y el 13/02/2019 y se clasifican en los siguientes grupos:

   a. Actualización de ***XXX XXX***.

   b. Restricción reglas de firewall.

   c. Bloqueo y registro de ******IP.2***.

   d. Limpieza de usuarios locales ***XXX XXX***.

   e. Cambios de contraseña.

      - ***14.- [……].***

   f. Antivirus.

   g. Aplicación ***15.-[……]***.

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

   i. Instalación ***XXX XXX***.

   j. 16.-[……].

   k. Replataformado de ***XXX XXX***.

   l. Configuración ***17.-[……]***.

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 na 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,* ***18.-[……]****. 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 recogidas en el art. 34 RGPD. En este sentido aplicarían las previstas en el art. 34.3 a) y b).

Con fecha 14/11/2019, 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 31/10/2009 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 el 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 31/10/2019, 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 05/07/2019 en su primera versión según indica el control de versiones del documento y la portada del documento.
5. Que el informe forense de ******EMPRESA.3*** 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 ***19.-[……].***
6. Que el informe forense de ******EMPRESA.3*** 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 ******EMPRESA.3*** fechado a enero de 2019 y basado en la investigación iniciada en fecha 25/10/2018 el cual contiene las siguientes manifestaciones, entre otras:

a. "*La investigación realizada por* ******EMPRESA.3*** *identificó pruebas concluyentes de violación en AIR EUROPA"*

b. *"La investigación de* ******EMPRESA.3*** *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* ***20.-[…….]****, el atacante consiguió utilizar herramientas de* ***21.-[…….]*** *para obtener datos de texto claros."*

c. *"La intrusión probablemente tuvo su origen en sistemas inseguros disponibles a través de internet.* ******EMPRESA.3*** *identificó varios dispositivos que no se habían parcheado con regularidad…"*

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

22.-[…….]

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

b. "E*l ataque comenzó al acceder el atacante al* ***XXX XXX*** *desde un servidor no adecuadamente segmentado en el* ***XXX XXX****".*

c. *"El atacante tenía una conexión sistemática con un host externo.* ***23.-, ***EMPRESA.3 […….]****. Sin embargo, sí visualizó cómo el atacante creaba varios archivos y posteriormente los comprimía en un solo archivo.* ***24.-[…….]."***

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

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

2. Que, en relación al motivo de la no detección de la brecha hasta el ******FECHA.1*** a pesar de que el ataque se inició el 12/05/2018, 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"

1. 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.

2. 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 ***25.-[…….].***

      "26.-[…….]"

   b. En este documento se manifiesta en el apartado de ***27.-[…….].***

   c. En este documento se manifiesta en el ***28.-[…….]."***

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

4. 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.*"

Con fecha 04/06/2020 AIR EUROPA remite a esta Agencia la evaluación de impacto del tratamiento de *"Venta a clientes por canales alternativos".*

TERCERO: Con fecha 23/06/2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción de los artículos 32.1 y 33 del RGPD, tipificadas conforme a lo dispuesto en el artículo 83.4.a) del citado RGPD.

CUARTO: Notificado el citado acuerdo de inicio, el reclamado presento ante la AEPD escrito solicitando copia del expediente y ampliación del plazo concedido para la presentación de alegaciones, que fue concedido en cinco días más.

El 16/07/2020 el reclamado presentó escrito de alegaciones en el que, en síntesis, manifestaba que no era cierto que no se hubiese notificado la brecha de seguridad sino que una vez que se tuvo indicios fundados de que el ciberataque sufrido había afectado a un considerable número de datos se procedió a su notificación; que el reclamado en todo momento ha contestado a los requerimientos formulados por la AEPD; la improcedencia de la infracción del artículo 33 del RGPD puesto que la notificación fue efectuada; la falta de motivación y de responsabilidad apreciada por la AEPD; que en las resoluciones dictadas por la AEPD relativas a brechas de seguridad menos sofisticados que la analizada fueron la mayor parte de ellas archivadas siempre que se acreditaran medidas de seguridad técnicas con anterioridad al incidente y se adoptaban medidas paliativas con posterioridad como ocurre en el presente caso; su

disconformidad con la graduación de la sanción ante la posible infracción del artículo 32.1 del RGPD por la no concurrencia de agravantes y la existencia de atenuantes que no han sido considerados en el acuerdo de inicio.

QUINTO: Con fecha 23/11/2020, el instructor del procedimiento acordó la apertura de un período de práctica de pruebas, practicándose las siguientes:

Dar por reproducidos a efectos probatorios todos los documentos obtenidos y generados por los Servicios de Inspección y el Informe de actuaciones previas de Inspección que forman parte del expediente E/01909/2020.

Dar por reproducidos a efectos probatorios, las alegaciones al acuerdo de inicio PS/00179/2020 presentadas por el reclamado y la documentación que a ellas acompaña.

Solicitar al reclamado en referencia a fecha anterior al inicio de la brecha producida:

- Descripción (incluyendo el nombre de los servidores y las bases de datos incluidos en ellos) los distintos entornos de sistemas desde el punto de vista de la seguridad, donde almacenan datos de clientes y de sus tarjetas bancarias, incluyendo al menos, los datos de dirección postal, números de teléfono, números de pasaporte, DNI, fecha de nacimiento, nombre del titular de la tarjeta, PAN de la tarjeta, fecha de caducidad de la tarjeta y su código CVV.

Asimismo, indicación de tipos de datos que se almacenan dentro de cada entono/servidor/base de datos y aporte documentación que acredite las medidas de seguridad aplicadas encaminadas a aislar los distintos entonos entre sí.

- Para cada una de los entornos, servidores y bases de datos identificados en el apartado anterior, aporte captura de pantalla donde se visualice, para 50 registros, todos los datos almacenados junto con la explicación de su significado.

Teniendo en cuenta el documento de Análisis de Riesgos entregado a esta Agencia con nombre *"Documento_3__PIA_Venta_on_line.pdf",* y las medidas de seguridad aplicadas antes del inicio de la brecha, aportación de la siguiente información y documentación en vigor a fecha anterior al inicio de la brecha:

• Motivo por el que no se incluyeron en el análisis de riesgos ***29.-[…….].***

• Motivo por el que no estaban adoptando ***30.-[…….]***:

31.-[…….].

32.-[…….]

El 02/12/2020, el reclamado presento ante la AEPD escrito de ampliación del plazo concedido para la aportación de pruebas que le fue concedido en cinco días más.

El 16/12/2020 el reclamado dio respuesta a la información solicitada cuyo contenido obra en el expediente.

SEXTO: El 05/02/2021 fue emitida Propuesta de Resolución en el sentido de que por la Directora de la Agencia Española de Protección de Datos se sancionara al reclamado, por infracción de los artículos 32.1 y 33 del RGPD, tipificadas en el artículo

83.4 del RGPD, con multas de 500.000 € (quinientos mil euros) y 100.000 € (cien mil euros), respectivamente.

El 10/02/2021, el reclamado presento ante la AEPD escrito de ampliación del plazo concedido para la presentación de alegaciones, que fue concedido en dos días más.

El 25/02/2021 el reclamado presente escrito en el que alegaba en síntesis: la importancia para el reclamado supone tanto el incidente producido como la protección de los datos de carácter personal de todos sus clientes; la indefensión causada ante la falta de consideración de las pruebas presentadas al último requerimiento de información de la AEPD; la impugnación expresa de la totalidad del informe de la empresa Foregenix; la improcedencia de la sanción impuesta por presunta infracción del artículo 33 del RGPD y, subsidiariamente, su prescripción; disconformidad con la imputación de infracción del artículo 32 del RGPD en relación con las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo y la improcedencia del uso de los informes forenses como prueba de que Air Europa no contaba con medidas de seguridad adecuadas; la falta de proporcionalidad en el análisis de las circunstancias agravantes tenidas en cuenta por la AEPD para la graduación de la sanción impuesta como consecuencia de la presunta infracción del artículo 32.1 del RGPD y la existencia de circunstancias atenuantes que no han sido consideradas a la hora de establecer la cuantía de la sanción y la disparidad de criterios en relación a anteriores procedimientos sancionadores similares.

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

HECHOS PROBADOS

PRIMERO: El 29/11/2018 se recibe en la AEPD escrito del reclamado señalando que el ******FECHA.1*** había recibido notificación del Banco Popular relativa a un incidente de seguridad provocando la activación del plan de respuestas ante incidentes el 17/10/1018.

SEGUNDO: El 18/01/2019 el reclamado aporto notificación completa a través del formulario habilitado en la sede electrónica de la AEPD, aportando documentos anexos relativos a Medidas preventivas aplicadas con anterioridad al incidente; Medidas de contención e información adicional y Justificación para no informar a los interesados afectados por el incidente.

TERCERO: El reclamado en fecha 01/04/2019 ha aportado: Informe técnico forense elaborado por ******EMPRESA.2*** en relación con la incidencia comunicada a la AEPD en el que se analiza la incidencia producida y recomendaciones; señalando *que "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"* y que *"El primer acceso confirmado a la red de GLOBALIA por parte del atacante tuvo lugar a través* ***33.-[……]*** *para una cuenta desconocida el día 12 de mayo de 2018."*Informe elaborado por el equipo técnico del reclamado el que se identifican las tareas técnicas

acometidas para el cierre de la brecha y las mejoras de protección implantadas, atendiendo a las recomendaciones de IBM; análisis de riesgo respecto de las medidas de seguridad en el tratamiento de los datos de venta online a pasajeros de Air Europa; el análisis de riesgos efectuado por la Sociedad respecto de la necesidad o no de notificación a la AEPD y a interesados acerca de la brecha de seguridad experimentada.

CUARTO: El reclamado en fecha 14/11/2019 ha aportado Informe forense de ***EMPRESA.3** de enero de 2019 basado en investigaciones realizadas y el análisis de las posibles causas, señalando entre otras que *"La investigación realizada por **EMPRESA.3 identificó pruebas concluyentes de violación en AIR EUROPA*"; copia del contrato de asistencia y gestión de sistemas de información y comunicaciones de 31/10/2009 entre GLOBALIA SISTEMAS Y COMUNICACIONES, S.L.U. y el reclamado en el que ostentan la condición de responsable y encargado del tratamiento respectivamente; copia el Plan de Respuesta ante Incidentes de Ciberseguridad de GLOBALIA de 05/07/2019 y Manual de Seguridad de la Información de fecha 31/10/2013

QUINTO: El 04/06/2020 el reclamado ha aportado Evaluación de impacto del tratamiento de *"Venta a clientes por canales alternativos"*.

SEXTO: El reclamado ha aportado en periodo de pruebas documentos relativos a medidas que tenía implantadas con anterioridad al incidente de seguridad declarado.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

El artículo 58 del RGPD, *Poderes*, señala:

"2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

(…)"

El RGPD establece en el artículo 5 de los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de *"integridad y confidencialidad".*

El artículo señala que:

"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»)".

(…)

Por otra parte, el artículo 4 del RGPD, *Definiciones*, establece en sus apartados 7, 8 y 12:

"(…)

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

(…)

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione 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;

(…)"

Asimismo, el artículo 24, *Responsabilidad del responsable del tratamiento,* establece que:

"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento".

Y el artículo 25, *Protección de datos desde el diseño y por defecto,* señala que;

"1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa

probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo".

Por tanto, para subsanar una violación de seguridad el responsable del tratamiento debe ser capaz de reconocerla y la consecuencia de tal violación es que el responsable del tratamiento no puede garantizar el cumplimiento de los principios relativos al tratamiento de los datos personales, tal como se establece en el artículo 5 del RGPD.

La seguridad de los datos personales viene regulado en los artículos 32, 33 y 34 del RGPD.

III

El RGPD define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las

precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

En el artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control.

En este mismo sentido se señala en los Considerandos 85 y 86 del RGPD:

(*85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.*

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

IV

En primer lugar, se imputa al reclamado la vulneración del artículo 32.1 del RGPD, que señala:

"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".

El Considerando (83) señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

De las actuaciones practicadas y documentación aportada al expediente se ha verificado que las medidas de seguridad que contaba la entidad investigada en relación con los datos que sometía a tratamiento, no eran las más adecuadas para garantizar la seguridad y confidencialidad de los datos personales en el momento de producirse el incidente o quiebra.

Como señala igualmente el *Considerando 39*:

"…Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

Hay que señalar que las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos ya que no es posible asegurar el derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales. Para garantizar estos tres factores de la seguridad son necesarias medidas tanto de índole técnica como de índole organizativo.

Por tanto, los análisis de riesgos de seguridad en la información deben centrarse en la capacidad de garantizar la confidencialidad, integridad, disponibilidad de los sistemas y servicios de tratamiento, tal como lo contempla también dicho artículo.

Uno de los requerimientos que establece el RGPD para responsables y encargados del tratamiento que realizan actividades de tratamiento con datos personales es la necesidad de llevar a cabo un análisis de riesgos de la seguridad de la información con el fin de establecer las medidas de seguridad y control orientadas a cumplir los principios de protección desde el diseño y por defecto que garanticen los derechos y libertades de las personas.

Se hace necesario señalar que en el presente caso a la luz de los informes emitidos por las empresas ******EMPRESA.2*** *y* ******EMPRESA.3*** acreditan vulnerabilidades graves de los sistemas del reclamado, comprometiendo la confidencialidad e integridad de la seguridad de la información provocando un acceso no autorizado que desemboco y provoco una transmisión ilícita de datos.

Como consta en el Informe de ******EMPRESA.2*** de 20/12/2018, *"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"* que *"El primer acceso confirmado a la red de GLOBALIA por parte del atacante tuvo lugar* ***34.-[……]*** *para una cuenta desconocida el día 12 de mayo de 2018"* y prosigue que tras el acceso inicial, sirviéndose ***35.-[……],*** el hacker comprometió una serie de sistemas de GLOBALIA continuando el acceso hasta como mínimo el 11/08/2018; que se ha confirmado que el atacante había recopilado 488847 tarjetas de crédito únicas; que comprometió al menos 12 sistemas y un mínimo de 2 cuentas de servicio en apoyo de su operación;

que todo el sistema expuesto a Internet debería tener ejecutada Autenticación Multifactorial; que las investigaciones posteriores de las cuentas comprometidas por el atacante reveló ***36.-[……]***, cosa que habría hecho que al atacante le resultara más fácil comprometer esta cuenta; que es probable que el atacante usara ******ARCHIVO.1*** como servidor de pruebas desde el que exfiltrar información; que un análisis estadístico de los registros del cortafuegos reveló que el mayor número de conexiones a la dirección IP controlada por el atacante, tuvo lugar entre el 14 de mayo y el 4 de junio; que el atacante usó herramientas públicamente disponibles, ***37.-[……]*** con la dirección IP controlada por el atacante; que se observó una configuración de registros irregular en los sistemas analizados, de forma que únicamente algunos sistemas almacenaban archivos de registros archivados localmente.

La citada empresa realizaba una serie de recomendaciones: revisar la política de auditoría y retención y ***38.-[……]***; que aunque no ha sido posible determinar exactamente la fuente de la infección de los sistemas en alcance, una de las hipótesis más probables es ***39.-[……]*** observaron diversos sistemas con un funcionamiento más largo de un año, por lo que ***40.-[……]***.

Asimismo, el Informe de ******EMPRESA.3***, empresa contratada el 22/10/2018 por el reclamado y especializada en brechas de seguridad y análisis forense, de enero de 2019 señala: que había identificado pruebas concluyentes de la violación de seguridad; la identificación de 2,7 millones de tarjetas que habían sido extraídos de los sistemas de bases de datos consiguiendo el atacante utilizar herramientas de descifrado presentes en los sistemas; que el acceso ***41.-[……];*** un resumen de las posibles causas que habrían motivado el ataque ***(42.-[……];*** la existencia de pruebas de violación del entorno de datos de los titulares de las tarjetas; que el ataque comenzó al accederse ***43.-[……]***; que el atacante tenía una con un host externo y que ***44.-[……]***; la posible exposición de determinados tipos de datos (nombre del titular de tarjeta, dirección de titular de tarjeta, fecha de vencimiento).

Por tanto, se desprende de lo que antecede que las medidas de seguridad técnicas y organizativas implantadas por la entidad reclamada no eran apropiadas para garantizar un nivel de seguridad adecuado al riesgo e impedir un acceso no autorizado a los datos de los clientes.

Hay que señalar que dada la evolución tecnológica y digital que sufren las actividades de tratamiento de los datos personales, hay que afrontarlos desde el punto de vista de una gestión continuada del riesgo, definiendo desde el diseño las medidas de control y de seguridad necesarias para que el tratamiento se produzca respetando los requerimientos de privacidad asociados a los niveles de riesgo al que puedan estar expuestos y evaluando de manera periódica y continua la efectividad de las medidas de control implantadas.

Esto implica igualmente la protección de los datos personales desde el diseño y por defecto, es decir que el responsable debe aplicar, tanto en el momento de establecer los medios de tratamiento como en el momento del tratamiento mismo, todas aquellas medidas técnicas y organizativas adecuadas y concebidas para aplicar, de manera efectiva, los principios de protección de datos e integrar, en el tratamiento, las garantías necesarias para cumplir los requerimientos que nos señala el RGPD; además, el responsable debe aplicar las citadas medidas para garantizar que, por

defecto, sólo se tratan los datos personales necesarios para cada finalidad específica del tratamiento.

El reclamado ha manifestado que la interpretación de la AEPD por el hecho de sufrir una brecha de seguridad implicaría automáticamente el incumplimiento del artículo 32.1 del RGPD sin proporcionar motivación alguna respecto al motivo por el cual las medidas de seguridad son insuficientes.

Sin embargo, hay que señalar que tal manifestación no puede ser aceptada puesto que según el Informe elaborado por ******EMPRESA.2*** pone de manifiesto ***45.-[……]***, aunque puede que para el representante del reclamado no sea suficiente el acceso a unas 4000 tarjetas de crédito con la finalidad de cometer fraude; que el atacante hubiera recopilado como mínimo 488847 tarjetas de crédito únicas; que visualizara y archivara en ******ARCHIVO.1*** al menos 2651 números de tarjeta únicos, CVVs, fechas de vencimiento y nombres de titular de la tarjeta; que el número aproximado de registros afectados fueran 1.500.000, etc.

Así, consta en los antecedentes de la presente propuesta y extractado del citado informe: "*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 del reclamado que realizaron reservas y modificaciones en AirEuropa.com. Los datos no incluían datos de viaje ni de pasaporte*" que *"El primer acceso confirmado a la red del reclamado 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"* y continua señalando que *"Tras este acceso inicial, el atacante comprometió una serie de sistemas del reclamado considerando que el atacante siguió accediendo a los sistemas y cuentas de GLOBALIA al menos hasta el 11 de agosto de 2018"*

Intrusión o acceso no autorizado ***46.-[……]*** y que la propia entidad no pudo detectar y que le tuvo que ser notificado por Banco Popular (VISA) al comprobar accesos a las tarjetas de clientes, como se pone de manifiesto en por el reclamado en la información remitida el 01/04/2019 aportando el análisis de riesgos efectuado respecto de la necesidad o no de notificación a esta Agencia y a los interesados en el que se señala: *"…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…".*

A mayor abundamiento el Informe forense de ******EMPRESA.3***, puesto en entredicho por la representación del reclamado igualmente señala la existencia de pruebas de violación de datos de titulares de tarjeta, que los datos expuestos eran los relativos a nombre del titular de tarjeta, dirección del mismo, fecha de vencimiento y que su número total era de 2722692, etc.

El propio reclamado en el análisis de riesgos efectuado tras el incidente sufrido señala *"En relación a los sistemas de AIR EUROPA, no existían medidas específicas,* ***47.-[……]****, que protegiese los datos a los que accedieron los atacantes…"*

La consecuencia de esta falta de medidas de seguridad adecuadas fue el acceso a datos personales no autorizados, a información de tarjetas bancarias, numeración, fecha de caducidad y CVV que se podrían estar utilizando para operaciones fraudulentas como comunicaba el Banco Popular al reclamado el ******FECHA.1***.

Esa mera posibilidad supone un riesgo que se ha de analizar y valorar a la hora de tratar los datos personales y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de los mismos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento y en función del mismo establecer las medidas que posiblemente hubieran impedido la pérdida de control de los datos y, por tanto, por parte de los titulares de los datos que le fueron proporcionados a éste como ha sido acreditado.

De acuerdo con lo señalado la actuación del reclamado supone la vulneración del artículo 32.1 del RGPD, infracción tipificada en su artículo 83.4.a).

V

El reclamado ha alegado la no aplicabilidad del RGPD puesto que al producirse el primer acceso el 12/05/2018, se cumplía en esa fecha los requisitos de seguridad exigidos por la legislación aplicable en el momento del incidente la LOPD y su Reglamento.

No obstante, tal alegato no puede ser aceptado; los hechos objeto de la presente reclamación quedan sometidos a las disposiciones del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos, cuya fecha de plena aplicación fue el 25/05/2018.

El acceso a los datos personales de los afectados por la quiebra se inició antes de la fecha de plena aplicación del Reglamento (UE) 2016/679 -lo que acontece el 25/05/2018- y cuando estaba aún vigente la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, LOPD. No obstante, la conducta del reclamado en la que se concreta la infracción, quiebra de seguridad motivada por la adopción de medidas técnicas y organizativas inadecuadas, se ha mantenido en el tiempo, al menos, hasta la adopción de medidas consecuencia de la comunicación de Banco Popular al reclamado y la contratación de las empresas forenses que provoco la implementación de medidas a fin de atajar el incidente de seguridad.

Es cierto que el primer acceso se produce, como señala el reclamado, el 12/05/2018 fecha en la que estaba en vigor la anterior LOPD y que el RGPD no es de plena aplicación hasta el 25/05/2018; sin embargo, no lo es menos que la infracción continuó produciéndose y extendiéndose en el tiempo hasta la adopción de aquellas medidas adecuadas para poner fin a la quiebra producida en los sistemas de la reclamada; no hay que olvidar que las medidas de seguridad técnicas y organizativas deben ser implementadas para impedir entre otros el acceso no autorizado a los datos de carácter personal y que estas medidas deben ser adecuadas.

Y aunque los accesos continuaron hasta agosto de 2018, cesando a partir de esta fecha las medidas implantadas continuaron siendo inadecuadas hasta que no se implementaron otras con motivo de la comunicación del incidente y la adopción de aquellas otras nuevas con motivo de la intervención de las empresas contratadas.

La infracción de la que se responsabiliza al reclamado participa de la naturaleza de las denominadas infracciones permanentes, en las que la consumación se proyecta en el tiempo más allá del hecho inicial y se extiende, vulnerando la normativa de protección de datos, durante todo el periodo de tiempo en el que los datos son objeto de tratamiento. En el presente caso, pese a que en la fecha en la que se inició la conducta infractora la norma aplicable era la LOPD, la normativa que resulta de aplicación es la que estaba vigente cuando la infracción deja de consumarse con la aplicación de aquellas medidas adecuadas y pertinentes a fin de que los accesos a los datos de carácter personal no se pudieran producir.

El Tribunal Supremo se ha pronunciado sobre la norma que ha de aplicarse en aquellos supuestos en los que las infracciones se prolongan en el tiempo y ha habido un cambio normativo mientras se cometía la infracción. La STS de 17/04/2002 (Rec. 466/2000) aplicó una disposición que no estaba vigente en el momento inicial de comisión de la infracción, pero sí en los posteriores, en los que continuaba la conducta infractora. La Sentencia examinó un supuesto que versaba sobre la sanción impuesta a una Jueza por incumplimiento de su deber de abstención en unas Diligencias Previas. La sancionada alegaba la no vigencia del artículo 417.8 de la LOPJ cuando ocurrieron los hechos. La STS consideró que la infracción se había venido cometiendo desde la fecha de la incoación de las Diligencias Previas hasta el momento en que la Jueza fue suspendida en el ejercicio de sus funciones por lo que esa norma sí era de aplicación. En idéntico sentido se pronuncia la SAN de 16/09/2008 (Rec.488/2006)

VI

El reclamado ha alegado que le produce indefensión la ausencia de respuesta a las pruebas presentadas a requerimiento de la AEPD de fecha 23/11/2020 y no haberse valorado las mismas, señalando, además, que le resulta muy perjudicial que la AEPD no haya tomado en consideración ni una sola de las alegaciones formuladas ni haya tenido en cuenta ni uno solo de los documentos aportados en la contestación al requerimiento cursado por la AEPD durante esa fase probatoria.

Sorprende la causa de indefensión alegada; hay que señalar que si no se hizo referencia a las mismas fue debido a que la respuesta ofrecida no hacía sino consolidar y reforzar los informes aportados por IBM y Foregenix acerca de que las medias implantadas al tiempo y momento de la quiebra producida no eran las más adecuadas para la seguridad de los datos.

Medidas que deben ser establecidas por el responsable del tratamiento teniendo en cuenta el análisis del riesgo llevado a cabo y en función del mismo aplicar aquellas medidas técnicas y organizativas más adecuadas.

Así, se aportaba en primer lugar una serie de diagramas de red del entorno de pagos, pero no se acreditaba el lugar donde se guardaban cada tipo de datos, donde se almacenaba cada tipo de dato concreto.

En sus manifestaciones el reclamado señalaba que los datos de carácter personal de los afectados (direcciones postales, teléfono, pasaporte, DNI, fecha nacimiento, etc.), eran guardadas de manera independiente de la información relativa a las tarjetas bancarias y que, por tanto, los citados datos no se vieron comprometidos.

No obstante, tampoco se acredita que los datos relativos al titular de los datos y por ende los relativos a las tarjetas fueran archivados por separado; el propio informe de auditoría de ***EMPRESA.2** se señala que *"El atacante visualizó y archivó en ***ARCHIVO.1** (…) al menos 2651 números de tarjeta únicos, CVVs, fechas de vencimiento y nombres de titular de la tarjeta"*. Y en el mismo informe también se establece que *"Los datos robados incluían datos personales y financieros de los clientes de GLOBALIA que realizaron reservas y modificaciones en ***URL.1**. Los datos no incluían datos de viaje ni de pasaporte"* (el subrayado corresponde a la AEPD).

Y la propia reclamada en su respuesta de fecha 16/12/2020 manifestaba que *"Tal y como se puede observar, ni las bases de datos del entorno objeto de la presente investigación, ni el potencial compromiso de datos, incluían información que no fuera la ya indicada; esto es, números de tarjeta únicos, CVVs, fechas de vencimiento y nombres del titular de la tarjeta"*. Es decir, implícitamente se estaba reconociendo que el nombre del titular estaba incluido en los datos dentro del potencial compromiso de datos, lo que debería haber sido relevante a la hora de establecer la necesidad de dar a conocer con diligencia la notificación de la incidencia de seguridad a la AEPD, dada la importancia de los datos a los que potencialmente o no se podía o se pudo acceder.

En cuanto a los análisis de riesgos, el último documento presentado por el reclamado es de fecha 04/06/2020 con motivo del EIPD, más completo que el presentado el 01/04/2019. El aportado en primer lugar no determina qué nivel de riesgo resulta o no aceptable para el tratamiento llevado a cabo, ni determinan su cálculo, ni desglosa las medidas mitigadoras, etc., en comparación con el último presentado (donde si se tienen en cuenta medidas como la doble autenticación y las contraseñas robustas que se implementan en el Análisis de Riesgo).

El reclamado alega que cuando se inició el incidente de seguridad no se aplicaba el RGPD y que las medidas propuestas en el Análisis de Riesgo en ese momento eran conformes con las recomendaciones existentes en el momento.

Sin embargo, habría que señalar que en relación con dos tipos de medidas, ***48.-[……]*** a la que el reclamado alude recomienda ***"49.-[……]"***, es decir, lo mismo que ya establecían los informes de las empresas actuantes y que figura reflejado en el informe de actuaciones previas y, en cuento a la longitud y complejidad de la contraseña, en el mismo informe anterior (el de la CNN) se señala y recomienda ***50.-[……]***.

En cuanto a ***51.-[……]***, manifiesta que estaba completamente actualizado a fecha del incidente y presentan un documento justificativo. Sin embargo, ***52.-[……].***

En cuanto ***53.-[……]*** como medida implantada en el momento del incidente obedece según el reclamado a que en el informe del CCN a que se hace referencia anteriormente establece que la longitud de las contraseñas deben ser de al menos 8 con diferentes tipos de caracteres y que estas recomendaciones ya se cumplían a 17/01/2018 siguiendo sus recomendaciones y aportan captura de pantalla con la política de contraseñas donde figura que *"las contraseñas deben cumplir los requisitos de complejidad", "habilitado", "longitud mínima de la contraseña"* y *"8 caracteres".*

Sin embargo, no se aprecia, acredita o justifica a que tipo de complejidad habilitada se está refiriendo y en cualquier caso, en el informe de ***EMPRESA.2** se señala que *"las investigaciones posteriores de las cuentas comprometidas por el atacante, como la cuenta de servicio ***SERVICIO.1**, 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."

En relación con la ***54.-[……]*** señalan que estaban ***XXXXXXXX*** presentando el diagrama de red.

Sin embargo, el informe de ******EMPRESA.3*** de enero de 2019 hacía referencia a que el servidor ***55.-[……]***, *"El ataque comenzó al acceder el atacante al* ***56.-[……]***" y *"Aunque había* ***XXXXX*** *y* ***XXXXX****, el atacante pudo "pivotar" la entrada* ***57.-[……]"***

Por último, en relación con el bloqueo de IPs externas que no tienen relación con ningún sistema de pago señalaba que *"No era posible técnicamente acotar las IP's de los diversos centros autorizadores. Por tanto, las conexiones salientes (no así las entrantes) no estaban, ni podían estar restringidas."*

Sin embargo, tampoco se acredita ni se da información alguna del porque no era técnicamente posible o por qué no era posible acotar las IPs.

VII

Alega el reclamado en relación con el informe aportado por ******EMPRESA.3*** que el mismo no es un informe pericial, ni un informe técnico objetivo, ***58.-[……]***, con el fin de calcular el importe de la indemnización que ese entorno regulatorio exige a las entidades asociadas en determinadas situaciones y que existe un incompatibilidad absoluta entre las finalidades de ese informe y las que se deben perseguir en un expediente administrativo sancionador.

Sin embargo, tal alegato tampoco puede ser aceptado: en primer lugar, porque el reclamado no ha aportado prueba alguna de su parcialidad, lo que tal vez habría provocado su impugnación, sin que se haya acreditado en el procedimiento prueba alguno de ello.

Y en segundo lugar, porque el Informe emitido por la citada empresa señala:

1.La presente investigación se realiza en estricto cumplimiento de todos los requisitos aplicables previstos en el Apartado 2.3 de los Requisitos relativos a la cualificación de los investigadores forenses de PCI, lo cual incluye, sin limitación, los requisitos previstos en dicho apartado relativos a independencia, opinión profesional, integridad, objetividad, imparcialidad y escepticismo profesional.

2. Este Informe Preliminar del PFI de Respuesta a un Incidente identifica, describe, representa y caracteriza todas las pruebas objetivas que la Empresa de PFI y sus Empleados recogieron, generaron, descubrieron, analizaron y/o consideraron a su sola discreción relevantes para esta investigación en el curso de la realización de la misma.

3.Las opiniones, conclusiones y hallazgos que contiene el presente Informe Preliminar del PFI de Respuesta a un Incidente (a) reflejan exactamente y se basan exclusivamente en las pruebas objetivas descritas más arriba, (b) reflejan solamente las opiniones, conclusiones y hallazgos de la Empresa de PFI y sus Empleados, actuando a su sola discreción, y (c) no han sido influenciadas, dirigidas, controladas,

modificadas, proporcionadas o sometidas a la aprobación previa de la Entidad objeto de Investigación o de ningún contratista, representante, asesor profesional, agente o afiliado de la misma o cualquier otra persona o entidad distinta a la Empresa de PFI y sus Empleados (el subrayado corresponde a la AEPD).

VIII

En segundo lugar, se imputa al reclamado la vulneración del artículo 33 del RGPD, *Notificación de una violación de la seguridad de los datos personales a la autoridad de control,* que establece:

"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".

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (en lo sucesivo RGPD) define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o

ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

En este sentido el considerando 87 estable que:

"Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento".

Independientemente de las actuaciones de índole interno que se llevaron a cabo por el reclamado para gestionar la brecha o incidente de seguridad una vez que se tuvo conocimiento de la misma, el RGPD establece que en caso de brecha de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente 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 brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

El RGPD también establece los casos en los que una brecha de seguridad se debe comunicar al afectado, en concreto cuando sea probable que la brecha de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas.

Tanto la notificación a la autoridad de control competente como la comunicación al afectado son obligaciones del responsable del tratamiento, aunque puede delegar la ejecución de las mismas en otras figuras.

Por tanto, lo que subyace a dicha obligación es un deber más amplio y que insta al responsable a implantar un procedimiento de gestión de incidentes de seguridad que afecten a datos de carácter personal adaptado a las características del tratamiento.

Por consiguiente, un elemento clave de cualquier política en materia de seguridad de los datos es poder, en la medida de lo posible, prevenir una violación y, cuando a pesar de todo se produzca, reaccionar de forma rápida.

Señala el RGPD que son brechas aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

En el caso examinado, de la documentación aportada en el expediente se ofrecen indicios evidentes de la existencia de un incidente de seguridad provocado y sufrido en los sistemas de la entidad, catalogado como brecha comportando el acceso no autorizado a datos de los usuarios, en concreto información relativa a datos personales, tarjetas bancarias, numeración, fecha de caducidad y CVV que se podría

haber utilizado para la comisión de operaciones fraudulentas y que de conformidad con lo señalado en el fundamento anterior infringiría el artículo 32.1 del RGPD, *Seguridad del tratamiento*, de la que tuvo conocimiento el reclamado por la comunicación recibida de entidades financieras provocando la activación del plan de respuestas ante incidentes (PRI) el día siguiente.

El reclamado adoptó la decisión de notificar a esta autoridad de control la quiebra de seguridad detectada el 27/11/2018, a través del formulario habilitado en sede electrónica pero el procedimiento online imposibilitó su presentación por lo que se tuvo que ser realizada al día siguiente, el 28/11/2018 de manera presencial.

Es cierto, como manifiesta la representación del reclamado que hubo notificación de la quiebra, si bien esta se realizó de manera extemporánea 41 días después de que fuera conocida infringiendo claramente lo dispuesto en el artículo 33 del RGPD que establece la obligación de notificar a la autoridad de control sin dilación indebida y, a más tardar, 72 horas después de que haya tenido constancia de ella.

El reclamado justifica la notificación tardía realizada porque no se tenía conocimiento suficiente de la naturaleza o alcance sufrido y que hubiera afectado a datos personales.

Sin embargo tal alegato no puede ser admitido puesto que el responsable del tratamiento tenía pruebas claras de que se había producido tal violación y no cabían dudas de que tenía constancia de ello como consecuencia de la notificación del Banco Popular el ***FECHA.1 que provoco como anteriormente se ha señalado la activación del plan de respuestas ante incidentes el día siguiente. Así figura en el informe de IBM *“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”.*

Además, si fuera cierto lo que el propio reclamado señala en su escrito de fecha 22/01/2019 donde manifiesta que la quiebra estaba solucionada el 17/11/2018, ¿Porque no lo notificó antes?

A más, en el análisis de riesgos efectuado respecto de la necesidad o no de notificación a la Agencia, en conclusiones, se señala que *“Aplicando la metodología de análisis de la AEPD al incidente actual (Anexo 1), tanto el resultado cuantitativo como el cualitativo superan el umbral de notificación a la AEPD…”*

Por otra parte, de las investigaciones y análisis realizados por la entidad no se catalogó el incidente como de alto riesgo para los derechos y libertades de los interesados, por lo que la quiebra, que afectó a 1.500.000 de registros de datos aproximado y a 489.000 usuarios aproximadamente, no fue notificada a los afectados ya que únicamente se tuvo constancia de 20 peticiones de información por parte de clientes dando respuesta a todos ellos. En las conclusiones de análisis de riesgo anterior se señala que *“En relación a la notificación a interesados y según la metodología de análisis de la AEPD (Anexo 1), el resultado cuantitativo no superaría el umbral establecido para dicha notificación (30 vs. 40), mientras que el umbral cualitativo sí se vería superado”.*

De conformidad con lo párrafos precedentes, la actuación del reclamado supone la vulneración del 33.1 del RGPD, infracción tipificada en su artículo 83.4.a) del mismo texto legal.

IX

La vulneración de los artículos 32.1 y 33 del RGPD se encuentran tipificadas en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. 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.

(…)

Por su parte, la LOPDGDD en su artículo 71, *Infracciones,* señala 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".*

Y en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves":*

"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:

(…)

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679".

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.

Los hechos acreditados evidencian la existencia de una brecha de seguridad en los sistemas del reclamado permitiendo su vulnerabilidad provocando el acceso no autorizado e ilícito a información relativa a clientes en relación con sus tarjetas bancarias, numeración, fecha de caducidad y CVV que se podría haber utilizado para la comisión de operaciones fraudulentas, lo que unido a la notificación extemporánea de la citada brecha o incidente de seguridad supone la infracción de los artículos 32.1 y 33 del RGPD.

X

A fin de establecer la multa administrativa que procede imponer han de observarse las previsiones contenidas en los artículos 83.1 y 83.2 del RGPD, que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

En relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76, *"Sanciones y medidas correctivas",* establece que:

"2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado."

De conformidad con los preceptos transcritos a efectos de fijar el importe de la sanción a imponer en el presente caso por las infracciones tipificadas en el artículo 83.4.a) del RGPD de la que se responsabiliza a AIR EUROPA, se estiman concurrentes los siguientes factores:

- En relación con la infracción del artículo 32.1 del RGPD tipificada en el artículo 83.4 del citado Reglamento:

La naturaleza y gravedad de la infracción dado su alcance no meramente local de la brecha de seguridad declarada, sino todo lo contrario puesto que se han podido ver comprometidos datos de carácter personal no solo de nacionales sino extranjeros, sin olvidar el elevado número de personas, clientes, al que potencialmente afecto la misma (489.000) y el número de registros afectados (1.500.000); en el informe de IBM de 20/12/2018 se señalaba que *"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" ,"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*" y en el informe de ******EMPRESA.3*** aportado por el reclamado el 14/11/2019 se señalaba que *"La investigación de* ******EMPRESA.3*** *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";* la categoría de datos afectados por la infracción, sin olvidar los daños y perjuicios sufridos por algunos de los clientes.

El grado de responsabilidad del responsable del tratamiento, habida cuenta de las medidas técnicas u organizativas aplicadas y que fueron vulneradas. Así**,** ******EMPRESA.2*** señala que *"…, el atacante se aprovechó de* ***59.-[……]*** *conseguir acceder a la red por vez primera",* que *"Todo sistema expuesto a Internet,* ***60.-****[……] "…, las investigaciones posteriores de las cuentas comprometidas por el atacante,* ******SERVICIO.1****, 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."*

******EMPRESA.3*** en su informe señala que *"La intrusión probablemente tuvo su origen en sistemas inseguros disponibles a través de internet.* ******EMPRESA.3*** *identificó varios dispositivos que no se habían parcheado con regularidad…",*

Pero la propia entidad reclamada ha señalado que *"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."

Las categorías de los datos de carácter personal que se han visto afectados como consecuencia de la infracción pues a los datos identificativos hay que unir los bancarios y financieros, consecuencia del acceso a las tarjetas, con una finalidad claramente fraudulenta. En el informe de auditoría realizado por ******EMPRESA.2*** de 20/12/2018 se manifiesta que *"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* ******URL.1***" (el subrayado corresponde a la AEPD).

La forma en que se ha tenido conocimiento de infracción pues ello se debió a una comunicación de BANCO POPULAR, y como se señala en el párrafo anterior por compañías de tarjetas de crédito, sin que la reclamada hubiera tenido constancia de la intrusión y accesos cometidos que comenzaron el 12/05/2018.

El carácter continuado de la infracción en el sentido interpretado por la Audiencia Nacional como infracción permanente, pues desde que se produjo el incidente de seguridad hasta que la brecha fue detectada transcurrió un periodo de tiempo de varios meses.

La actividad de la entidad presuntamente infractora está vinculada con el tratamiento de datos tanto de clientes como de terceros; es conocida la citada vinculación ya que la entidad por su actividad está en permanente contacto con clientes y terceros tratando un gran volumen de datos, lo que le impone un mayor deber de diligencia.

El volumen de negocio de la reclamada pues se trata de una de la compañía líder dentro del mercado español, en su objeto de negocio transporte aéreo; el reclamado forma parte del holding empresarial Globalia Corporación Empresarial S.A. y del que forman parte un gran número de empresas, habiendo tenido unos ingresos anuales de 2.367.061.000 € (2018) y 2.130.517.000 € (2019) y un resultado de explotación de 82.921.000 € (2018 y 93.984.000 (2019) según consta en la página web del grupo corporativo y según la última publicación del BORME el 30/12/2020 un capital social de 17.923.050 €.

Por todo ello, se establece una cuantía de la sanción por vulneración del artículo 32.1 del RGPD de 500.000 euros.

En relación con las circunstancias de la responsabilidad el reclamado ha alegado que no se han tenido en cuenta en la ponderación de la sanción la aplicación de circunstancias atenuantes, considerando que de entenderse cometida la infracción del artículo 32.1 habrían de aplicarse las siguientes circunstancias atenuantes: la escasa gravedad del incidente y el bajo nivel de perjuicios causados; las medidas tomadas por el responsable para paliar los daños y perjuicios sufridos; la cooperación con la autoridad de control y la falta de beneficios obtenidos.

Sin embargo tal pretensión no puede ser aceptada; las circunstancias agravantes que han sido tenidas en cuenta son las que concurren en el presente caso.

En cuanto a la gravedad de la infracción ya concurre como agravante en la gradación de la sanción por infracción del artículo 32.1: *"La naturaleza y gravedad de la infracción dado su alcance no meramente local de la brecha de seguridad declarada, sino todo lo contrario puesto que se han podido ver comprometidos datos de carácter personal no solo de nacionales sino extranjeros, sin olvidar el elevado número de personas, clientes, al que potencialmente afecto la misma (489.000) y el número de registros afectados (1.500.000); en el informe de* ******EMPRESA.2*** *de 20/12/2018 se señalaba que…"*

Además, resulta llamativo que se califique de escasa gravedad a la infracción cometida cuando la propia LOPDGDD en su artículo 73 la considera a efectos de prescripción como infracción grave y cuando resulta evidente y palpable la falta de diligencia en la aplicación de las medidas adecuadas de carácter técnicas y organizativas, prolongándose desde el 12/05/2018 fecha del primer acceso hasta que se implantaron medidas apropiadas a instancias de las empresas contratadas.

En cuanto al bajo nivel de los perjuicios causados como consecuencia de la infracción, no es predicable al presente caso donde además existen perjudicados, pero aunque no los hubiera nos encontramos ante la infracción de un derecho fundamental y se ha de tener en cuenta el alto grado de intromisión en la privacidad de los clientes siendo esto suficiente perjuicio para los mismos.

Aun es más llamativo es la petición de que se considere como atenuantes la adopción de medidas tomadas por el responsable para paliar los daños y perjuicios y la cooperación con la autoridad de control, cuando no son sino obligaciones legales que se les ha de exigir a cualquier responsable y encargado del tratamiento y, más cuando como se señalaba anteriormente se ha evidenciado la falta de diligencia en la aplicación de las mismas para evitar accesos no autorizados, aunque es cierto que sus incumplimientos podrían suponer su aplicación como agravantes.

Y en cuanto a la ausencia de beneficios resulta improcedente; el RGPD se refiere a los beneficios obtenidos como consecuencia de la comisión de la infracción, no que la ausencia de beneficios deba ser considerada como atenuante.

Por tanto, valorando las circunstancias concurrentes y tomando en consideración especialmente las que operan como agravantes y que se han analizado anteriormente, se considera ponderada y proporcionada la sanción impuesta por infracción del artículo 32.1 del RGPD, dada la gravedad de los hechos producidos

- En relación con la infracción del artículo 33 del RGPD tipificada en el artículo 83.4 del citado Reglamento:

La grave falta de diligencia en el cumplimiento de las obligaciones impuestas por la normativa de protección de datos, realizando una notificación extemporánea de la quiebra de seguridad a que estaba obligado.

La forma en que se ha tenido conocimiento de infracción pues ello se debió a una notificación de BANCO POPULAR y por compañías de tarjetas de crédito, sin que la reclamada hubiera tenido constancia de la intrusión y accesos cometidos que comenzaron el 12/05/2018.

La actividad de la entidad presuntamente infractora está vinculada con el tratamiento de datos tanto de clientes como de terceros; es conocido la citada

vinculación ya que la entidad por su actividad está en permanente contacto y trata un gran volumen de datos, lo que le impone un mayor deber de diligencia.

El volumen de negocio de la reclamada pues se trata de una de la compañía líder dentro del mercado español, en su objeto de negocio.

Por todo ello, se establece una cuantía de la sanción por vulneración del artículo 33 del RGPD de 100.000 euros.

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 AIR EUROPA LINEAS AÉREAS S.A., con CIF ***CIF.1**, por una infracción del artículo 32.1 del RGPD, tipificada en el Artículo 83.4.a) del RGPD, una multa de 500.000 € (quinientos mil euros).

SEGUNDO: IMPONER a AIR EUROPA LINEAS AÉREAS S.A., con CIF ***CIF.1,** por una infracción del artículo 33 del RGPD, tipificada en el artículo 83.4.a) del RGPD, una multa de 100.000 € (cien mil euros).

TERCERO: NOTIFICAR la presente resolución a AIR EUROPA LINEAS AÉREAS S.A.

CUARTO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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.

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