- **Expediente N.º: EXP202212829**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Se han presentado diversas reclamaciones ante la Agencia Española de Protección de Datos (en adelante, los reclamantes) contra ***UNICAJA BANCO, S.A.U.*** con NIF ***A93139053*** (en adelante, la parte reclamada). Las fechas de presentación de las distintas reclamaciones son las siguientes:

21/10/2022: ***A.A.A.***

3/11//2022, ***B.B.B.***

03/01/2023 ***C.C.C.***

21/01/2023 ***D.D.D.***

23/01/2023 ***E.E.E.***

03/02/2023 ***F.F.F.***

03/02/2023 ***G.G.G.***

01/03/2023 ***H.H.H.***

21/06/2023 ***I.I.I***

Los mencionados reclamantes, todos ellos clientes de la parte reclamada, manifiestan haber sido víctimas de un fraude por ciberdelincuentes que simulaban ser empleados de la entidad. Dicho fraude consistió en la obtención por parte de los reclamantes, combinando técnicas de smishing, vishing e ingeniería social, de los códigos de seguridad que validaron las operaciones de transferencia de dinero desde su cuenta a la de los estafadores. Los reclamantes consideran que la parte reclamada no ha sido diligente en advertir a sus clientes de estos posibles fraudes, especialmente en el contexto de la fusión con otra entidad, dado que afirman que en el proceso de dicha fusión podría haberse producido una brecha de seguridad que permitió el acceso a sus datos personales por parte de los ciberdelincuentes.

Dentro de la documentación aportada por las distintas reclamaciones, destacan las siguientes:

- Informe pericial aportado por un reclamante que vincula la ocurrencia de los hechos descritos en las reclamaciones a la obtención de datos personales a través de internet, que se han subastado y usado posteriormente.
- Grabación de la llamada fraudulenta a uno de los reclamantes.

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

Los traslados, que se practicaron conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fueron recogidos y respondidos por la parte reclamada en los términos que en las actuaciones de investigación que seguidamente se exponen.

TERCERO: De conformidad con el artículo 65 de la LOPDGDD, se admitieron a trámite las reclamaciones presentadas.

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

De las diez reclamaciones admitidas a trámite, en nueve de ellas se pone de manifiesto que fueron los propios reclamantes quienes facilitaron los datos bancarios al ciberdelincuente que simulaba trabajar para la parte reclamada. Dichos datos fueron los que permitieron llevar a cabo las operaciones fraudulentas que les causaron un perjuicio económico. En la décima reclamación, la parte reclamante pone de manifiesto únicamente haber recibido una llamada telefónica y un SMS de carácter fraudulento suplantando a la parte reclamada, no habiendo facilitado ningún dato ni sufrido perjuicio económico alguno.

Relación entre las actuaciones fraudulentas y la brecha de datos de 20 de mayo de 2022 comunicada a la presente autoridad. Se trata de determinar, en primer lugar, si los hechos descritos en las reclamaciones se encuentran relacionados con la mencionada brecha sufrida por la parte reclamada que fue debidamente comunicada por esta el 3 de junio de ese mismo año. Para ello, se solicitó a dicha entidad información adicional relativa a la brecha notificada, solicitud de la cual se recibió respuesta por escrito, destacando del mismo los siguientes aspectos:

- En mayo de 2022 se llevó a cabo la puesta en producción de ******HERRAMIENTA.1*** como la herramienta de envío de comunicaciones a clientes en dicha entidad. Esta herramienta era ya utilizada por la entidad fusionada de forma previa a la integración tecnológica con la parte reclamada y proporcionada por el proveedor ******PROVEEDOR.1*** a través de un contrato de licencia y mantenimiento. Dicha herramienta tiene por finalidad agrupar la información sobre estados financieros para posteriormente ser ensobrada y remitida por correo ordinario a los clientes.

- Tras su implantación en el entorno productivo, comenzó a ejecutarse los primeros procesos de generación y envío de comunicaciones a través de la herramienta, no detectándose en los primeros días ninguna anomalía en los datos, aunque sí retrasos en los tiempos de ejecución de las tareas.
- Al modificar el proveedor la programación del aplicativo con el fin de reducir dicho retraso, se genera una situación de condición de carrera que provoca errores en la dirección postal de algunos clientes quienes reciben la carta con los datos de otro cliente-
- Tras confirmarse con el proveedor la ocurrencia de la incidencia, se involucra a los diferentes interesados (incluyendo al DPD y a Ciberseguridad de la parte reclamada) y se consensuan las medidas a tomar para su subsanación.
- Con fecha 03 de junio de 2022 se procede a la comunicación de la brecha a la presente autoridad, cumpliendo lo exigido por la normativa. Asimismo, tras la comunicación de la incidencia se llevaron a cabo las siguientes acciones:
    - Se solicitó al proveedor de la herramienta un informe sobre la incidencia, sus causas y posibles medidas correctivas a adoptar.
    - Se bloqueó la generación e impresión de nuevos documentos.
    - Se llevó a cabo un proceso de vuelta atrás en la configuración que había provocado la incidencia, verificando que esta no se replicaba en las nuevas ejecuciones.
    - Se avisó a Correos para que paralizase envíos pendientes.
    - Se eliminó los comunicados pendientes que aún no habían sido lanzados.
    - Se llevó a cabo por parte del proveedor las tareas necesarias para solucionar cualquier alteración en los datos de los clientes que pudiera estar asociada a la incidencia.
- La afectación de la incidencia se limitaba a envíos en papel no existiendo impacto en clientes que reciben las comunicaciones de forma electrónica.

De todo lo expuesto, no resulta posible determinar que la brecha de seguridad notificada, fruto de un error humano en la configuración de una herramienta, motivase la producción de los hechos descritos en las reclamaciones objeto del presente expediente.

Relación con la absorción de Liberbank S.A. por la parte reclamada. Con fecha 26 de julio de 2021 se produjo la fusión por absorción de Liberbank S.A. por la parte reclamada. Como consecuencia de la fusión, Liberbank S.A. se extinguió y su patrimonio se transmitió en bloque a la parte reclamada, por lo que esta entidad se ha subrogado, por sucesión universal, en todos sus derechos y obligaciones.

La parte reclamada aporta el informe emitido por el Área de Ciberseguridad y Riesgo Tecnológico sobre las medidas adoptadas para garantizar la seguridad, integridad y confidencialidad de los datos personales en el proceso de migración de sistemas informáticos llevados a cabo tras la integración de Liberbank S.A.

En el informe se recogen las medidas adoptadas para advertir a los clientes de posibles intentos de fraude durante el proceso de migración de sistemas tras la absorción, publicándose, entre otras cuestiones, lo siguiente:

> *Revisa bien los mensajes que recibes por correo electrónico o por SMS. Los ciberdelincuentes pueden aprovechar el proceso de integración tecnológica para cometer sus fraudes. #NoPiques.*
>
> *Si tiene alguna duda, contáctanos por Messenger o llámanos al 952 076 263.*
>
> *¡Ojo!*
>
> *No abras archivos o pinches enlaces de remitentes desconocidos y/o sospechosos. Si dudas, contáctanos por redes sociales.*
>
> *No hagas clic en los enlaces de los SMS que te urgen a dar información personal o financiera.*

Del informe referido se concluye que no se han detectado fallos en la migración informática y/o los protocolos de seguridad existentes en la parte reclamada que hayan tenido relación con los supuestos de fraude reclamados a la entidad. Todo ello sin perjuicio de que, aprovechando la integración, los delincuentes hayan podido intensificar sus ataques sobre este colectivo.

Campañas informativas y de concienciación En relación con las técnicas de fraude phishing, vishing o smishing, la parte reclamada indica que viene realizando en redes sociales, en medios de comunicación, en la propia web, en cajeros automáticos y en el servicio de banca a distancia, múltiples campañas informativas y de concienciación en aras a prevenir de este tipo de fraudes, incluyendo mensajes claros de actuaciones de prevención a su clientela. A fin de acreditar este extremo se aportan los siguientes documentos:

- Informe del Departamento de Redes Sociales. Este informe recoge todas las publicaciones informativas-preventivas de ciberseguridad difundidas a través de las redes sociales de la parte reclamada desde su creación, en junio de 2018, hasta junio de 2023.
- Informe del Departamento de Redes Sociales en el que constan los artículos publicados en Uniblog. Este informe recoge todos los artículos sobre Ciberseguridad publicados en UniBlog desde su creación, en octubre de 2018, hasta junio de 2023. Uniblog es el blog corporativo de la parte reclamada y cuenta con una categoría específica de ciberseguridad donde se agrupan todos los artículos con información de servicio en los que se abordan, en profundidad, cuestiones de interés para ayudar a los usuarios a conocer cómo funciona el ciberfraude y como prevenirlo. En la actualidad hay un total de 38 artículos en la sección de ciberseguridad, los cuales además de quedar publicados permanentemente en el propio blog, son difundidos a través de los perfiles en redes sociales para amplificar su alcance al mayor público posible.
- Contenido de los carteles expuestos en la red de oficinas de la parte reclamada con consejos para evitar el fraude digital.
- Contenido de emails enviados a clientes con banca digital activa en los últimos tres meses, o que realizaran compras en comercio electrónico en

los últimos seis meses. Se enviaron cuatro emails con consejos para prevenir el phishing, el vishing y el smishing así como para crear una contraseña segura.

- Anuncios destinados a evitar el fraude digital publicados en toda la red de cajeros automáticos de la parte reclamada.
- *Informe del Área de Ciberseguridad y Riesgo Tecnológico* en el que se detallan las medidas, tanto puntuales como permanentes adoptadas relativas a campañas informativas y de concienciación, externas e internas con impacto externo, llevadas a cabo por la Entidad para la prevención de fraudes del tipo phishing, vishing o smishing durante el año 2022, en el que tuvo lugar la integración tecnológica de las plataformas de la parte reclamada y Liberbank S.A.
- Asimismo, se Incluye las actuaciones llevadas a cabo sobre origen Liberbank S.A. en las semanas previas a producirse la integración tecnológica.

Servicios de monitorización y cierre de amenazas en internet ***(…)***

Evaluación de la efectividad de las medidas. Asimismo, en relación con el aumento notable del número de reclamaciones interpuestas por clientes que se han visto afectados por fraudes de terceros mediante la utilización de las técnicas de phishing, smishing, vishing y spoofing, se solicita a la parte reclamada aclaración de si ha encontrado alguna justificación al respecto, si ha evaluado la efectividad de las medidas implantadas y si ha llevado a cabo alguna actuación adicional.

A tal respecto, en relación con la justificación del incremento del número de reclamaciones, traslada que entiende que *se trata de un aumento que se ha producido a nivel global de la utilización de estas técnicas para llevar a cabo actuaciones fraudulentas y que han afectado no sólo a clientes de entidades de bancarias, sino también a usuarios de otros servicios como correos o servicios de paquetería, incluso a usuarios de servicios públicos, habiendo llegado a ser suplantadas entidades públicas como la Agencia Tributaria o la Tesorería de la Seguridad Social.*

Señala que ello ha motivado campañas de difusión reiteradas por parte de asociaciones, organismos públicos, las propias entidades bancarias y, en particular, la parte reclamada, que las ha acreditado en el marco de las presentes actuaciones de investigación.

Cita, por su relevancia en relación con las entidades bancarias, la *Memoria de Reclamaciones de 2022* publicada en el mes de octubre de 2023 por el Banco de España, en la que constata este incremento dentro del sector bancario.

Destaca que estos datos confirman la previsión de aumento de la ciberdelincuencia que recoge la Secretaría de Estado de Seguridad del Ministerio del Interior en su *Informe sobre la cibercriminalidad en España 2022.*

Campaña de subasta y venta de datos de clientes En el marco de las actuaciones de investigación se pregunta a la parte reclamada si tiene constancia de la existencia, en agosto de 2022, de una campaña de subasta y venta de datos de cliente de su Entidad a través de canales de Telegram, donde también se venderían procedimientos de phishing y de robo de contraseñas.

La parte reclamada afirma no tener constancia de la subasta y venta de datos de clientes a través de canales de Telegram, si bien, ha tenido conocimiento de la venta de datos de clientes a través de distintos mercados, de la información obtenida a partir de la infección de los equipos de los clientes con diferentes tipologías de software malicioso (malware).

No ha resultado posible comprobar el contenido del anuncio de la presunta venta en el citado canal de Telegram, ni que dicho contenido consista, precisamente, en datos personales pertenecientes a clientes de la parte reclamada.

Sentencias y Acuerdos Extrajudiciales En los datos informados por LA PARTE RECLAMADA para el período solicitado, desde enero de 2021 hasta febrero de 2023, se incluye, en relación con la devolución de las cantidades reclamadas, el número de sentencias dictadas, el número de los procedimientos judiciales en los que está pendiente dictarse la correspondiente sentencia y el número de acuerdos extrajudiciales a los que se ha llegado.

(...)

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

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

II
Seguridad y confidencialidad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

"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."

Resulta necesario señalar que el citado precepto no establece un listado de las medidas de seguridad concretas de acuerdo con los datos objeto de tratamiento, sino que establece la obligación de que el responsable y el encargado del tratamiento apliquen medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este sentido, el considerando 83 del RGPD 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".

Por su parte, por lo que se refiere a la integridad y confidencialidad de los datos, la letra f) del artículo 5.1 del RGPD propugna:

"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»)."

III
Conclusión

Teniendo en cuenta el principio de la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario previsto en el artículo 53 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, de las actuaciones investigadoras realizadas y se deducen las conclusiones que seguidamente se exponen.

Durante el desarrollo de la investigación, no se ha podido constatar la existencia de una relación causal directa entre la actividad fraudulenta de los ciberdelincuentes y la brecha de datos personales producida con anterioridad. La información disponible muestra que la brecha de datos de mayo de 2022 tuvo lugar como consecuencia de un error humano derivado de la integración de las entidades bancarias .Dicha brecha no se trataba de una filtración masiva de datos en soporte informático, sino que tuvo lugar como consecuencia de la remisión de envíos postales a otros clientes distintos de los destinatarios, brecha que, asimismo, fue comunicada debidamente a la presente autoridad. La actividad fraudulenta, por el contrario, parece haberse producido mediante el envío masivo e indiscriminado de mensajes a diversos usuarios por parte de los ciberdelincuentes aprovechando la fusión entre las mencionadas entidades.

Asimismo, resulta oportuno destacar que la entidad reclamada ha proporcionado documentación respecto a las medidas implementadas con el fin de prevenir actividades fraudulentas y proteger la seguridad de los datos, incluyendo diversas campañas informativas y de divulgación de este tipo de ciberdelincuencia.

De la misma forma, tal y como se desprende de las actuaciones investigadoras, no se han detectado fallos en la migración informática y/o los protocolos de seguridad por lo

que no resulta posible determinar que dicha migración tenga relación directa con los hechos objeto de las reclamaciones. Dicha ausencia de relación de causalidad no obsta a que, como se indica en las actuaciones previas, los ciberdelincuentes hayan podido intensificar sus ataques aprovechando la integración de las entidades.

Por último, en relación a la posible venta de datos a través de redes sociales, no se ha logrado obtener evidencia sólida que respalde la existencia de ventas o divulgaciones indebidas de datos personales de la entidad reclamada en un canal de Telegram u otros medios. De forma concreta, no se ha podido comprobar que el contenido del citado anuncio en la red social contenga datos personales de clientes de la entidad reclamada.

Como puede observarse, la falta de pruebas concluyentes impide la atribución de responsabilidad a la entidad respecto a las actividades fraudulentas denunciadas.

Por tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos**,** todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, al no haber sido posible atribuir una responsabilidad a la entidad reclamada respecto de las actividades fraudulentas a los reclamantes, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a ***UNICAJA BANCO, S.A.U.*** y a la parte reclamante.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-301023

Mar España Martí

Directora de la Agencia Española de Protección de Datos