- **Procedimiento Nº: E/05175/2020**

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: Como consecuencia de notificación a la Unidad de Evaluación y Estudios Tecnológicos de una brecha de seguridad de datos personales por parte de la entidad responsable del tratamiento WIZINK BANK, S.A.U, con número de registro de entrada ******REGISTRO.1***, la Directora ordenó el 12/06/2020 a la Inspección de Datos que valorase la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

SEGUNDO: A la vista de la citada notificación de quiebra de seguridad de los datos personales, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, teniendo conocimiento de los siguientes extremos:

INTERVINIENTES INVESTIGADOS
Durante las presentes actuaciones se han investigado a los siguientes intervinientes (entidad jurídica y persona física, respectivamente): WIZINK BANK, S.A.U. (en adelante, la investigada #1), con CIF A81831067.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Respecto de los intervinientes

- La investigada #1 se identifica como la responsable del tratamiento de los datos personales en que se ha producido la brecha de seguridad. Asimismo, la investigada #1 se presenta como la realizadora del mantenimiento de los sistemas informáticos involucrados en la brecha de seguridad.

- La investigada #1 cuenta, como encargada de dicho tratamiento, con IBERALBIÓN, A.I.E. (con CIF G84226224), que es una entidad filial suya, para la que trabajaba la empleada en el momento en que se produjo la presente brecha de seguridad de datos personales.

La investigada #1 aporta contrato, firmado en fecha 28/12/2019, con su encargada del tratamiento para la prestación de servicios auxiliares a la actividad económica de la responsable del tratamiento, el cual incluye en su Anexo I cuestiones relativas a la protección de datos, al encargo del tratamiento y a las medidas de seguridad.

- La investigada #1 identifica a la empleada como quien remitió datos personales de clientes de su entidad a terceros sin base legal provocando esta brecha de seguridad.

• La investigada #1 dispone de una delegada de protección de datos y así consta reflejado en la Agencia Española de Protección de Datos (en adelante, AEPD).

Respecto de la cronología de los hechos

Todo según manifestaciones de la investigadas #1 y la empleada:

• 02/06/2020: se produjo el envío de un documento que contenía datos de clientes de la investigada #1, a través del buzón genérico de la Sección Sindical de ***SECCIÓN.1** (***EMAIL.1)** a un tercero (***EMAIL.2**) que carecía de todo tipo de relación contractual con la investigada #1 ni con su encargada del tratamiento. Este archivo contenía 743 registros de clientes.

Este envío fue detectado ese mismo día por el sistema automático de alertas implementado en la investigada #1, por el cual su Oficina de Seguridad de la Información (en adelante, BISO) recibe una alerta sobre el envío de datos sin cifrar fuera del entorno de la investigada #1.

Al recibir la alerta, BISO revisó la mencionada alerta y al ver que se trataba de un envío realizado a través del buzón genérico de la Sección Sindical de ***SECCIÓN.1** de su encargada del tratamiento (en adelante, Sección Sindical), se puso en contacto con Recursos Humanos de la investigada #1 (en adelante, RR.HH.) para verificar si estaba justificado, por razón de sus propias funciones, que la mencionada Sección Sindical tuviese acceso a esa información y su envío externo.

Al mismo tiempo, un miembro de BISO pone en copia del correo electrónico informando de esta alerta identificada, al buzón genérico de la Sección Sindical, de modo que los miembros de la Sección Sindical quedan advertidos de la detección del email enviado indebidamente.

• 03/06/2020: RR.HH. contesta a CISO que la Sección Sindical, como consecuencia de la actividad que le es propia, no debía tener acceso al fichero con datos personales de clientes y, por consiguiente, tampoco estaba justificado su envío externo. RR.HH., con el objeto de aclarar los hechos, intentó ponerse en contacto con la Sección Sindical ese mismo día. Al no ser posible contactar,

RR.HH. envió un correo electrónico recordando que el envío de información con datos personales al exterior, sin autorización expresa de la investigada #1, es un incumplimiento de las Políticas de la Entidad y solicitando la identificación del remitente para poder esclarecer lo ocurrido. La investigada #1 aporta copia del correo electrónico enviado por RR.HH. a la Sección Sindical solicitando su colaboración.

Al confirmarse por parte de RR.HH. que dicho acceso a datos personales de clientes de la investigada #1 no estaba enmarcado dentro de la actividad sindical de la Sección Sindical, a las 22:31 horas de ese día se informa del incidente a su delegada de protección de datos.

• 04/06/2020: Se mantiene una reunión con todas las áreas implicadas para analizar el incidente en profundidad y determinar las acciones a tomar. Acuden, a la reunión,

entre otras áreas: CISO, RR.HH., Tecnología y delegada de protección de datos de la investigada #1. En la reunión se identifican a las siete personas que tienen acceso al buzón genérico de la Sección Sindical. La investigada #1 aporta los datos identificativos de estas siete personas, entre las que se encuentra la empleada.

En la reunión se decide:

o Averiguar la persona que ha enviado el email;

o Averiguar quién de los miembros sindicales pudo tener acceso a la información enviada o si se la pudo enviar otro trabajador de la investigada #1;

o Reunión entre RR.HH. y la Sección Sindical para pedir la colaboración de la Sección Sindical para el esclarecimiento de los hechos;

o Involucrar al Departamento Legal por si es necesario adoptar medidas legales.

RR.HH. mantiene conversaciones con el Secretario General de la Sección Sindical dirigidas a esclarecer los hechos e intentar averiguar qué persona y por qué motivo se envió esta información, así como con el abogado de la Sección Sindical. Como consecuencia de dichas reuniones, RR.HH. pone de manifiesto a la delegada de protección de datos de la investigada #1 la negativa del Secretario General de la Sección Sindical a colaborar con la investigada #1. El Secretario General de la Sección Sindical no proporciona el nombre de la persona que realizó el envío, en un primer momento indicó que se trataba de un email que se quería enviar al asesor laboral de la Sección Sindical, y en un segundo momento, indicó que se había enviado el documento con datos de clientes por error; y en un tercer momento indicó que el envío se hacía a un colaborador para labores de impresión de documentación.

El Secretario General de la Sección Sindical envía a RR.HH. un correo electrónico del destinatario del correo electrónico generador del incidente, en el que trata de negar su relación con la persona remitente del correo, aduciendo que ha procedido a la eliminación de los correos electrónicos recibidos. La investigada #1 aporta copia de dicho correo electrónico.

Se confirma que el fichero enviado a ******EMAIL.2*** está guardado en una carpeta a la que solo pudo tener acceso la empleada para el ejercicio de las funciones laborales que tenía asignadas.

Tras investigaciones internas, se detectó que se habían realizado seis envíos a la dirección de correo electrónico ******EMAIL.2***. Entre esos envíos, destacó que dos minutos antes del envío del archivo del incidente, la empleada intentó enviar el mismo email a la dirección ******EMAIL.2*** desde su cuenta corporativa ***(***EMAIL.3***). No obstante, debido a las medidas de seguridad implementadas por la investigada #1 y todas las compañías de su grupo, por la cual los agentes no pueden enviar correos electrónicos al exterior, este envío no se pudo completar. Ante estas evidencias y la no colaboración de la Sección Sindical, la encargada del tratamiento de la investigada #1 solicitó a ***XXXXXXXX*** (proveedor del software utilizado para la gestión del correo electrónico) que identificara, de las siete personas que tienen acceso al buzón genérico de la Sección Sindical, cuál de ellas había procedido al envío del fichero,

determinando que había sido la empleada. Tal que, presuntamente, ante la imposibilidad de enviarlo a través de su correo electrónico corporativo, procedió a realizar el envío desde el buzón genérico de la Sección Sindical que sí tiene habilitados los envíos al exterior para permitir el ejercicio de las labores sindicales de la Sección Sindical de la que es miembro. La investigada #1 aporta copia de los registros de los envíos detectados al destinatario ******EMAIL.2***.

- 05/06/2020: RR.HH. se reúne con la empleada, en presencia del Presidente y Secretario General de la Sección Sindical, para esclarecer lo sucedido. En dicha reunión la empleada entrega una declaración firmada por su parte en la que indica lo sucedido y deja constancia, del borrado del correo electrónico de la bandeja de salida y de elementos eliminados.

La investigada #1 aportó en la notificación de brecha de seguridad a la AEPD una copia de la citada declaración de la empleada en que ésta reconoce que tuvo acceso a los datos personales de los clientes por sus funciones laborales dentro del Departamento de Cobros de la encargada del tratamiento de la investigada #1 y que los remitió externamente a ******EMAIL.2*** a través de la cuenta de correo electrónico sindical, a la que tiene acceso en sus labores sindicales, ya que esa no impide la salida de documentación alguna al exterior de la entidad (a diferencia de su cuenta de correo laboral). En esa declaración, la empleada afirma haber eliminado el fichero que contenía datos personales de clientes de la investigada #1, que no ha sido guardado dicho archivo y que no ha utilizado la información en él contenida.

La empleada se ratifica en la declaración que, según su versión, la encargada del tratamiento le puso a la firma y aporta copia de una aclaración posterior firmada en fecha 03/07/2020 en la que muestra su disconformidad en lo referente a la intencionalidad por su parte. La empleada expresa que desconocía el contenido del correo electrónico enviado al exterior por su parte y que no tenía la intención de enviar a un tercero información sensible alguna. La empleada aporta copia de acta de reunión mantenida el 11/07/2020 con la encargada del tratamiento, entre otras partes, en que insiste en no estar conforme con lo firmado refiriéndose a que no hubo por su parte intencionalidad y conciencia en el envío de datos personales de clientes realizado a un tercero.

Según la investigada #1, la empleada entrega el ordenador corporativo puesto a su disposición para el ejercicio de las funciones que tiene asignadas, el cual fue precintado y posteriormente depositado ante Notario, en su presencia. Ese mismo día también, se le comunica la suspensión cautelar de empleo, que no de sueldo y se le informa que dada la gravedad de los hechos y la necesidad de tomar acciones legales encaminadas a los derechos y libertades de los clientes de la investigada #1 afectados por la violación de seguridad, se va a interponer una denuncia penal, para que se pueda iniciar una investigación oficial de los hechos. La investigada #1 aporta copia del acta firmada ante notario por la que se procede a depositar el ordenador de la empleada ante Notario y copia completa de la denuncia penal presentada ante el Juzgado de Guardia de Madrid para su reparto al Juzgado de Instrucción que por turno corresponda relativa a los hechos acontecidos en la brecha de seguridad

- 06/06/2020: La investigada #1 notifica la brecha de seguridad a la AEPD.

- 17/06/2020: La investigada #1 firma un contrato con una empresa especializada en análisis forense**,** DUFF & PHELPS, S.L. ***(***con CIF B85173136***),*** para realizar una análisis informático forense del suceso y de las fuentes de información relacionadas con este disponibles, a los efectos de acreditar técnicamente lo sucedido, contemplándose el análisis del ordenador corporativo puesto a disposición de la empleada para el ejercicio de las funciones que tiene asignadas y otras fuentes de información digital almacenadas en los sistemas de la investigada #1 o de terceros (por ejemplo, ***XXXXXXXX***). La investigada #1 aporta copia de la propuesta de servicios profesionales de la empresa especializada en análisis forense de fecha 17/06/2020 y copia de situación de investigaciones referentes a la brecha de seguridad emitida en fecha 16/07/2020. Ambos documentos son calificados como PRIVADO y CONFIDENCIAL, por lo que se catalogan por esta AEPD como RESTRINGIDOS.

- 10/07/2020: En la Notaría señalada anteriormente, en presencia de la empleada, del Secretario General de la Sección Sindical y representante de RR.HH., se realiza una copia del disco duro del ordenador de la empleada, el cual estaba depositado en la mencionada Notaría.

La empleada manifiesta incorporar diversos argumentos que, según su versión, extrae del pliego de descargos al expediente contradictorio instruido por la empresa. Dicha información por su presunto carácter RESTRINGIDO procede a ser así catalogada por esta AEPD.

La empleada expone no disponer de copia de los correos electrónicos y sus archivos adjuntos que contenían datos personales de clientes de la investigada #1 remitidos a un tercero de forma ilegítima el 02/06/2020 por su parte.

La empleada, en fecha 11/11/2020, alega no tener conocimiento de la existencia de procedimiento judicial en el orden jurisdiccional penal relativo a la presente brecha de seguridad.

La empleada insiste en que no hubo intencionalidad de difundir ni utilizar un fichero con datos personales de clientes de la investigada #1 y añade que el archivo que los contenía lo adjuntó por error a uno de los varios correos que, según su versión, remitió a su pareja con el concepto [sic]: “para imprimir” con información y documentos relativos a su actividad sindical.

Respecto de las causas que hicieron posible la brecha de seguridad

La investigada #1 expresa que el incidente se ha producido, no como consecuencia de un fallo en las medidas de seguridad técnicas y organizativas implementadas en su encargada del tratamiento o en su grupo empresarial, sino por la conducta inadecuada y no autorizada de la empleada, quien presuntamente pudo aprovechar su condición de miembro de la Sección Sindical para utilizar los medios puestos a disposición de la misma para el ejercicio de sus funciones, y enviar el fichero con datos personales de clientes de la investigada #1 a terceros de forma no legítima.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo.

• La investigada #1 informa de no haber sufrido ningún incidente similar, si bien como consecuencia de la Sentencia del Tribunal Supremo (Sala de lo Civil) 600/2020, de 4 de marzo, Recurso 4813/2019 ha aumentado su riesgo de sufrirlos y, consecuentemente, las medidas implementadas para prevenir este tipo de situaciones.

La investigada #1 detalla que, a raíz de la citada Sentencia, en la que se desestima su recurso de casación, está recibiendo numerosas reclamaciones ante los Tribunales de Justicia relacionadas con sus líneas de crédito, especialmente con los intereses de la tarjeta revolving que ofrecía a sus clientes.

• La investigada #1 añade que ha aumentado el interés que tienen diversos despachos de abogados y gestorías en obtener información identificativa de sus clientes, con el objeto de captarles como reclamantes en vía judicial e impulsarles a presentar denuncia, con la finalidad de conseguir, en caso de un resultado positivo, beneficios económicos para estos despachos y gestorías. Por ello, la investigada #1 defiende haber remitido a la AEPD, en fecha 06/03/2020, otro presunto intento telefónico a extraer datos de sus clientes potenciales reclamantes el 05/03/2020 a cambio de otorgar una cantidad económica a su agente telefónico a cambio de hacerle llegar esos datos [Número de registro de entrada en la AEPD 011859/2020, incorporado en el procedimiento E/04309/2020 para acabar siendo inadmitido a trámite como reclamación y remitida esta decisión a la investigada #1 el 02/06/2020 y número de registro de salida AEPD 043418/2020]. La investigada #1 puso también en conocimiento de la Policía Nacional este otro suceso, mediante denuncia (de la que aporta copia) en la Comisaría de Policía Nacional de Madrid-Chamartín el día 06/03/2020.

• La investigada #1 aclara que el documento interno puesto a disposición de un tercero ilegítimamente por parte de la empleada contenga datos de 743 clientes de la investigada #1 que son susceptibles de presentar demanda judicial contra ella por la jurisprudencia anteriormente identificada.

Respecto de los datos afectados

• La investigada #1 manifiesta que el archivo Excel implicado en la presente brecha de seguridad por haber sido enviado indebidamente a un tercero poseía las siguientes características respecto a datos personales e información de clientes suyos:

o Tipología de datos implicados: el fichero incluía datos identificativos (nombre, apellidos y DNI) y datos de comportamiento (si acepta, o no, los acuerdos de pago, y la razón). No se incluían datos de contacto.

o Número real de afectados: 743 clientes.

o Posibles consecuencias para sus clientes afectados: Uso ilegítimo de los datos por parte de terceros, pudiendo ser dichos terceros despachos de abogados y gestorías.

• La investigada #1 expone no tener constancia alguna de la utilización indebida de los datos personales afectados por la presente brecha de seguridad. La investigada #1 aporta copia de la declaración firmada del borrado del correo electrónico por la

empleada y copia del correo electrónico desde la dirección del tercero receptor del correo ***(***EMAIL.2***) en que afirma haber eliminado la información recibida.

• La investigada #1 informa de haber procedido, como acción adicional, a implementar una medida consistente en realizar un seguimiento y monitorización de los casos afectados por la presente brecha de seguridad de datos personales para identificar un posible uso indebido de los mismos. A fecha 20/07/2020, la investigada #1 indica no haber detectado comportamiento alguno que haga sospechar de un uso indebido de los datos personales.

• La investigada #1 expresa no tener evidencia de que el fichero objeto del incidente haya sido compartido con otros terceros, aunque el alcance del mismo se encuentra en investigación por parte de los Juzgados correspondientes y del análisis pericial.

• La investigada #1 manifiesta no tener constancia de que la información haya sido publicada en Internet o en algún buscador en la red.

Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

• La investigada #1 reseña que tras el análisis de los hechos y a la vista de que por las primeras indagaciones efectuadas se evidenciaba que no había existido una conducta negligente o un fallo de los protocolos por parte de su entidad, sino una conducta ilícita de la empleada, la investigada #1 presentó denuncia penal ante el Juzgado de Guardia de Madrid ante un posible delito de descubrimiento y revelación de secretos de empresa -arts. 278 y 219 del Código Penal- (así como, alternativamente, por si pudieran constituir delito contra la intimidad -art. 197 del Código Penal-), el 05/06/2020:

o En virtud de la misma, a la investigada #1 le consta la Incoación de Diligencias Previas por parte del Juzgado de Instrucción ******JUZGADO.1*** de Madrid por delito de revelación de secretos. Por razones de competencia territorial dicho Juzgado se inhibe a favor de los Juzgados de ******LOCALIDAD.1***, no sin antes ordenar a la Policía Judicial proceder a la investigación de los hechos. La investigada #1 aporta copia del auto donde se oficia de inmediato a la oportuna unidad de la Policía Judicial para que investigue con urgencia los hechos denunciados.

o Una vez remitido el asunto al Decanato de los Juzgados de ******LOCALIDAD.1***, el asunto es turnado al Juzgado de Instrucción nº 12 de dicha capital (Diligencias Previas 1341/2020). Como suele ser práctica habitual en supuestos de inhibición, antes de aceptarla, el Juez ha acordado dar traslado al Ministerio Fiscal.

o La investigada #1 presentó escrito personándose en las Diligencias Previas incoadas por el Juzgado de Instrucción nº 12 de ******LOCALIDAD.1***. La admisión de dicha personación se efectuará una vez aceptada la competencia. La investigada #1 aporta copia del escrito de personación que incluye además la escritura de poderes otorgados y el justificante de haberlo presentado.

o A fecha 20/07/2020, el asunto estaba en proceso de investigación ante la jurisdicción penal, pendiente de la determinación de la competencia territorial para proceder a la investigación de los hechos.

- La investigada #1 detalla y aporta evidencias sobre las siguientes medidas de seguridad técnicas y organizativas:

o ***XXXXXXXX.***

o ***XXXXXXXX.***

o ***XXXXXXXX.***

o ***XXXXXXXX.***

o ***XXXXXXXX.***

o ***XXXXXXXX.***

o ***XXXXXXXX.***

Respecto de las medidas de seguridad implantadas

- En la cláusula 3.g del Anexo I del contrato presentado por la investigada #1 con su encargada del tratamiento consta la obligación de la encargada del tratamiento de garantizar que todas las personas autorizadas para tratar datos personales responsabilidad de la investigada #1 deben comprometerse de forma expresa y por escrito a respetar la confidencialidad y cumplir las medidas de seguridad correspondientes. La empleada como empleada de la encargada del tratamiento firmó el 08/09/2017 un compromiso de confidencialidad con la encargada del tratamiento como filial de la investigada #1. La investigada #1 aporta copia de esta declaración y compromiso de la empleada sobre la confidencialidad.

Además, la investigada #1 afirma tener un Código de Conducta de obligado cumplimiento a todas las empresas de su grupo empresarial, incluyendo su filial la encargada del tratamiento, en el que se definen todas las reglas de comportamiento, valores y estándares por los que han de regir la actuación de todos los empleados del Grupo. La investigada #1 aporta copia del documento con la firma de la aceptación y recibí del Código de Conducta del grupo empresarial por parte de la investigada #1 en fecha 08/09/2017.

La investigada #1 reseña que en apartado 3.2 de su Código de Conducta se incluye el deber de confidencialidad, así como que se informa a los trabajadores de las consecuencias que se pudiesen derivar del incumplimiento del mismo. La investigada #1 aporta copia de su Código de Conducta que incorpora los anteriores preceptos.

Adicionalmente, la investigada #1 manifiesta que todos los empleados de su grupo empresarial reciben, entre otras formaciones obligatorias, una relativa a su Código de Conducta, otra relativa a protección de datos y otra a seguridad de la información. La investigada #1 aporta un listado en que expone recoger estas formaciones impartidas

a la empleada desde la empresa, y pretendiendo acreditar que la empleada estaba debidamente informada de sus obligaciones y recibió formación laboral sobre ellas.

La empleada reconoce haber procedido, junto a la firma de su contrato de trabajo y como anexos, a la firma de los dos documentos aportados por la investigada #1 relativos a su deber de confidencialidad.

- La investigada #1 detalla y aporta evidencias sobre las siguientes medidas de seguridad técnicas y organizativas existentes en su entidad antes de la ocurrencia de la presente brecha de seguridad:

  - ***XXXXXXXX:***

  - ***XXXXXXXX:***

  - ***XXXXXXXX:***

  - ***XXXXXXXX.***

  - ***XXXXXXXX:***

  - ***XXXXXXXX*.**

- La investigada #1 aporta copia parcial de su registro de actividades del tratamiento en que recoge lo relativo a la actividad de tratamiento denominada por su parte "Gestión de Reclamaciones WZB SP", en la cual, según su versión, se encuentra incluido el fichero afectado por el incidente.

- La investigada #1 aporta copia del análisis de riesgos realizado sobre la actividad de tratamiento "Gestión de Reclamaciones WZB SP" en la que se reseña un nivel de riesgo bajo.

- La investigada #1 alega que, al haber sido categorizado como nivel de riesgo bajo la actividad del tratamiento "Gestión de Reclamaciones WZB SP", no se ha llevado a cabo una evaluación de impacto relativa a la protección de datos al respecto puesto que no existía un riesgo alto para los derechos y libertades de los afectados.

- La investigada #1 aporta copia de política de seguridad y de los estándares de seguridad que se aplican en su entidad.

- La investigada #1 aporta copia de su política interna de protección de datos que incluye un protocolo de actuación ante brechas de seguridad, en que se explicita el procedimiento de interacción con las autoridades de control de protección de datos. Añade la investigada #1 la aportación de copia de su proceso operativo de brechas de seguridad.

- La investigada #1 declara que las auditorías internas de seguridad son su tercera línea de defensa (tras las unidades de negocio y áreas de apoyo y las áreas de control de riesgo y de cumplimiento). La investigada #1 aporta copia de su documento

informativo sobre gobierno corporativo y copia del informe de auditoría externa de ciberseguridad emitido en fecha 20/12/2019.

- La investigada #1 aporta certificado de su pertenencia a la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), en el que se la identifica como participante activa en la Comisión de Tratamiento y Protección de Datos de dicha asociación.

- La investigada #1 establece no haber comunicado la brecha de seguridad a los afectados por haber identificado previamente que no existía un riesgo alto para sus derechos y libertades tras la ocurrencia de la misma. En este sentido, la investigada #1 alega:

o Ponerse siempre en contacto con los interesados en caso de detectar un posible o eventual uso fraudulento de los productos que tenga contratados con la entidad. En este caso, la investigada #1 no considera que, con los datos afectados por el incidente, se pueda realizar un uso fraudulento.

o Que el riesgo consistiría en el potencial uso de los datos por parte de despachos de abogados o gestorías para incitarlos a la interposición de demandas contra la entidad. Por ello, la investigada #1 entiende que es ella la que tiene el riesgo principal ya que podría recibir un alto volumen de demandas judiciales, con las consecuencias económicas que esto podría acarrearle.

o Que no se incluyen datos que faciliten la suplantación de identidad de los afectados por el presente incidente.

o Que los afectados no pueden tomar acciones para evitar los efectos adversos de la brecha de seguridad en cuestión.

En todo caso, la investigada #1 defiende que todos los clientes afectados por la brecha de seguridad han sido marcados en el sistema con el objeto de realizarles un seguimiento en caso de que se pongan en contacto con ella indicando un posible uso no autorizado de sus datos personales.

- La investigada #1 detalla y aporta evidencias sobre las siguientes medidas de seguridad técnicas y organizativas tomadas en su entidad tras de la ocurrencia de la presente brecha de seguridad para evitar su repetición:

*o **XXXXXXXX**.*

*o **XXXXXXXX**.*

*o **XXXXXXXX**.*

*o **XXXXXXXX**.*

*o **XXXXXXXX.***

FUNDAMENTOS DE DERECHO

I

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

II

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra de seguridad) como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos." En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad.

De la documentación aportada por la empresa en el curso de estas actuaciones de investigación, entre otra, copia parcial del RAT en que recoge la actividad denominada "Gestión de Reclamaciones WZB SP", en la cual, según su versión, se encuentra incluido el fichero afectado por el incidente, copia del Análisis de Riesgos, en el que es calificada de actividad de riesgo bajo, motivo por el cual no es necesario realizar una evaluación de impacto, copia del informe de auditoría externa de ciberseguridad emitido en fecha 20/12/2019 y copia de su política interna de protección de datos incluyendo un protocolo de actuación ante brechas de seguridad. Asimismo afirma contar entre otros procedimientos con Proceso de Content Monitoring (sistema de alertas cuando se envía un documento con datos personales no cifrados fuera de la entidad), obligar al encargado del tratamiento a que sus empleados firmen un compromiso de confidencialidad, además todas las empresas del grupo cuentan con un código de conducta de obligado cumplimiento, y realizar formaciones obligatorias sobre el código de conducta, protección de datos y seguridad de la información. Se desprende que, con anterioridad a producirse la brecha, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados

La brecha se produjo por el envío, detectado inmediatamente por la empresa, de un correo no autorizado al exterior por parte de una empleada, hecho que ha motivado la formulación de denuncia por la vía penal ante el juzgado.

.

En cuanto al impacto, los datos que se han visto vulnerados contienen información identificativa, (nombre, apellidos y DNI) y datos de comportamiento (si acepta, o no, los acuerdos de pago, y la razón).

El volumen de Datos se encuentra en el rango de 743, realizándose por parte del encargado seguimiento y monitorización de los casos, para identificar un posible uso indebido de los mismos y a fecha 20/07/2020, no se ha detectado comportamiento alguno que haga sospechar de un uso indebido de los datos personales, tampoco se

tiene constancia de que hayan sido compartidos con otros terceros, ni de que se haya producido la publicación en Internet o en algún buscador en la red. Obteniéndose también la declaración de borrado del correo, firmada por la empleada, así como correo electrónico de la dirección receptora del fichero, en el que se afirma, haber eliminado la información recibida.

Para evitar que estos hechos se repitan, aparte de proceder a la suspensión de empleo de la empleada y al bloqueo de su perfil. Se ha recordado a los empleados la importancia que tiene cumplir con los procedimientos de seguridad de la información y protección de
datos al tratar datos personales. Se ha procedido a modificar la configuración actual para que no solo advierta a BISO del posible envío de un correo electrónico con datos personales al exterior, tanto si el archivo está o no cifrado, sino que bloquee su salida en tanto no disponga de las correspondientes autorizaciones. Así como se va a implementar un protocolo automático por el cual, en caso de que un archivo de cualquier índole no sea modificado en los últimos 3 años, se almacene en un repositorio específico, con accesos muy limitados.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia, no obstante y una vez detectada ésta, se produce una diligente reacción al objeto de notificar a la AEPD, e implementar medias para eliminarla.

III

En el presente caso, la actuación de la investigada como entidad responsable del tratamiento, ha sido diligente y proporcional con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

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

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a WIZINK BANK, S.A.U. con NIF A81831067).

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.

940-0419

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