- **Procedimiento Nº: E/12007/2019**

940-0419

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: Las actuaciones de inspección se inician por la recepción en la Agencia Española de Protección de Datos (en adelante AEPD) de un escrito de notificación de brecha de seguridad de los datos personales remitido por Caja Rural de Zamora Cooperativa de Crédito (en adelante Caja Zamora) en el que informan a la AEPD de que, con fecha 27 de noviembre de 2019, un cliente de la entidad les comunica que ha recibido un correo electrónico remitido desde la dirección <***EMAIL.1** > informando de que disponen de sus datos personales junto con datos de otros clientes de la entidad bancaria.

En la notificación adicional de fecha 10 de enero de 2020, Caja Zamora aporta Informe de la brecha de seguridad y copia del escrito de comunicación a los afectados remitido por correo electrónico.

En la notificación adicional de fecha 14 de enero de 2020, Caja Zamora aporta denuncia interpuesta ante la Dirección General de la Policía en esa misma fecha, en el que manifiesta que -según un cliente de la entidad- un hacker ("***HACKER.1**") ha robado datos a Caja Zamora y que dicha información ha sido publicada en el periódico ***PERIÓDICO.1**. Asimismo, informan de que el servidor afectado corresponde al cedido a la empresa encargada del tratamiento "Casado, Bueno y De Dios, S.L." habiéndose comprometido dos bases de datos de clientes y currículos.

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

ANTECEDENTES

Fecha de notificación de la brecha de seguridad de datos personales: Notificación inicial el 29 de noviembre de 2019 y dos notificaciones adicionales en fechas 10 y 14 de enero de 2020.

ENTIDADES INVESTIGADAS

CAJA RURAL DE ZAMORA COOPERATIVA DE CRÉDITO, con NIF F49002454 con domicilio en Avda. Alfonso IX número 7, 49013 Zamora.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 23 de diciembre de 2019 se solicitó información a Caja Zamora y de las respuestas recibidas entre los días 7 y 14 de enero de 2020 se desprende lo siguiente:

Respecto de las entidades intervinientes

- Caja Zamora, tuvo subcontratado el alojamiento y mantenimiento del sitio web de Caja Zamora denominado <***URL.1*> desde el 1 de septiembre de 2008 hasta mayo de 2016 con el proveedor de servicios en calidad de encargado del tratamiento "Casado, Bueno y De Dios, S.L.", entidad que gira con el nombre comercial JAUS.

En mayo de 2016, Caja Zamora decide integrar el citado sitio web dentro del entorno del Grupo Caja Rural, tarea encargada al mismo proveedor de servicios (JAUS), y en mayo de 2017 Caja Zamora decide internalizar el servicio de mantenimiento del sitio web <***URL.1* > ya alojado en el entorno del Grupo Caja Rural, dejando al proveedor de servicios JAUS el alojamiento y el mantenimiento del sitio web <***URL.2* > así como la gestión de las redes sociales. A tal efecto, en fecha 27/05/2016 se modifica el contenido del contrato inicial de encargado del tratamiento mediante la "*Adenda al contrato de prestación de servicios suscritos entre C.R. Zamora y Casado, Bueno y de Dios, S.L.".* A este respecto se ha aportado copia del contrato suscrito de fecha 1 de septiembre de 2008 y la Adenda mencionada.

A su vez, JAUS subcontrata el servicio con la empresa "Bluefactory Community, S.L.U." (en adelante, Bluefactory) que a su vez subcontrata a la entidad "Soluciones Web Online, S.L.U." (en adelante, Profesional Hosting).

- Tal y como consta en Axesor, la entidad "Casado, Bueno y De Dios, S.L." (JAUS) es una microempresa cuya actividad principal es: *actividades profesionales, científicas y técnicas*.

- La empresa "Bluefactory Community, S.L.U." es una entidad especializada en diseño de imagen corporativa, diseño gráfico y diseño de sitios webs.

- La entidad "Soluciones Web Online, S.L.U." es una empresa especializada en actividades de alojamiento (hosting).

- La entidad "Rural Servicios Informáticos, S.L." (en adelante, RSI), es proveedora de servicios informáticos de Caja Zamora y adscrita al Grupo Caja Rural, tal y como consta en su web que gestiona más de 79 sucursales del Grupo Caja Rural al que pertenece Caja Zamora.

Respecto de la cronología de los hechos

Caja Zamora ha aportado informe sobre la brecha notificada en el que expone lo siguiente:

- El 27 de noviembre de 2019, un cliente de Caja Zamora recibe un correo electrónico de un supuesto *hacker* que le indica que tiene información personal suya y parece que tiene su origen en una brecha de seguridad en la Banca Electrónica del Grupo Caja Rural (Ruralvía). Por este motivo el cliente, en fecha 28 de noviembre, contacta con la directora de su oficina de Caja Zamora que a su vez contacta, vía telefónica, con el Departamento de Informática exponiendo los hechos. Ante la falta inicial de información fehaciente se considera que es un intento de fraude sobre el cliente del tipo *Phishing*. No obstante, el Delegado de Protección de Datos de Caja Zamora contacta con el cliente para que remita el correo recibido.

Una vez analizado el correo remitido por el cliente, inicialmente se descarta una posible una brecha de seguridad de Banca Electrónica dado que se detectan dentro del correo información sobre no clientes, información sobre clientes inactivos, e información sobre clientes que no disponen de Banca Electrónica.

Caja Zamora ha aportado correo del cliente en el que figura como remitente <***EMAIL.1** > y remitido a varios destinatarios entre los que se encuentra el cliente <***EMAIL.2** > (anonimizados por la AEPD). En el cuerpo del correo figuran datos personales de, al menos, dieciocho personas con datos de nombre y apellidos, sexo, fecha de nacimiento, domicilio, dirección de correo electrónico y un campo codificado.

- El 29 de noviembre de 2019, se recibe una llamada de la Delegada de Protección de Datos de RSI, informando del anuncio por parte de un *hacker* de la brecha en la Banca Electrónica del Grupo Caja Rural (Ruralvia). Asimismo, indican que parece que la brecha está relacionada sólo con Caja Zamora.

RSI también informa que otra sociedad del Grupo (Banco Cooperativo Español) ha recibido una llamada del periódico ***PERIÓDICO.1** indicando que dispone de una base de datos de clientes donde figura, entre otros datos, la clave de acceso a la Banca Electrónica.

RSI se pone en contacto con la empresa especializada en seguridad informática Grupo S21sec Gestión, S.A. (en adelante S21sec) para que comprueben si efectivamente se trata de un ataque sobre la Banca Electrónica (Ruralvía). Una vez analizada la información parece que la brecha está relacionada solamente con Caja Zamora no así con la Banca Electrónica dado que el *hash* de las contraseñas publicadas no se corresponde con los procesos de generación de los *hash* de Banca Electrónica.

Dentro del análisis se estudia la auditoría realizada por Caja Zamora en agosto de 2019 sobre los dominios:

***URL.1**

***URL.2** y

***URL.3**

El primer análisis ya descarta el acceso indebido al dominio www.cajaruraldigital.com

Se analiza también la notificación de la brecha a la AEPD con la información inicial que se dispone hasta este momento.

- El 30 de noviembre de 2019 se continua con el análisis de las otras webs:
- ***URL.2**

***URL.3**

Se realizan pruebas de intrusión sobre los dos dominios.

Caja Zamora se pone en contacto telefónico con el proveedor del servicio JAUS, el cual proporciona las credenciales de acceso al Panel de Control donde se aloja ***URL.2**. Se detecta la existencia de una carpeta en este servidor denominada <***URL.3** > (dominio oculto) que contiene lo que parece una copia de la antigua página web de Caja Zamora. En la carpeta se observa la existencia de dos bases de datos, y una de ellas parece ser la fuente de los datos notificados por el *hacker* dado

que coincide exactamente con la información filtrada. Esta base de datos contiene 643 registros.

Se procede al cierre de los servicios de este servidor para evitar la exposición de la información, cierre realizado a las 13:00 horas por S21sec por orden de Caja Zamora.

El INCIBE contacta mediante correo electrónico con RSI para solicitar información sobre la brecha, notificación respondida por RSI.

- 1 de diciembre de 2019 se intenta obtener más información sobre el servidor con objeto de planificar un clonado y analizar las actividades llevadas a cabo por el *hacker*.

Se notifica la brecha al proveedor JAUS quien manifiesta, según figura en el informe aportado y elaborado al efecto, que Caja Zamora tiene contratados desde el año 2017 los alojamientos de dos webs, entre ellas <******URL.3*** >, estando a su vez subcontrato por JAUS con la empresa Bluefactory, que a su vez subcontrata a la entidad Profesional Hosting. Manifiestan que ni JAUS ni ninguna de las empresas subcontratadas realizan tareas de mantenimiento o gestión de ese dominio.

Asimismo, JAUS manifiesta que la antigua web (******URL.1***) junto con los contenidos se ubicaron ocultos bajo el alojamiento de:

<******URL.3*** >

con la aceptación de Caja Zamora y en ningún momento se les solicitó el borrado de la información allí disponible.

A este respecto, el dominio <******URL.3***> consta creado con fecha 4 de abril de 2017, como registrante Bluefactory y registrado con privacidad *"redacted for privacy"*.

Una vez notificada la brecha a JAUS, el responsable de la empresa Bluefactory, indica que ha vuelto a poner en servicio la página web. Inmediatamente se les requiere detener los servicios y se informa de la necesidad de que el servidor esté inaccesible para evitar la exposición de la información.

- El 2 de diciembre de 2019, el Delegado de Protección de Datos de Caja de Zamora se desplaza a RSI para realizar el clonado del servidor que aloja la web pero finalmente no es posible acceder al servidor. Bluefactory les informa que este servidor está alojado bajo el control de la empresa Profesional Hosting.

Se analizan las dos bases de datos encontradas observando que la segunda base de datos parece contener antiguos currículos enviados desde un formulario web en la que aparecen contraseñas sin cifrar.

Se solicita información de todos los logs del servidor a JAUS.

Se realizan búsquedas de las bases de datos comprometidas en todos los Sistemas de Caja Zamora con el fin de explorar todos los escenarios probables.

Se analizan los resultados del último análisis de vulnerabilidades realizado sobre los sistemas internos de Caja Zamora sin obtener ninguna evidencia sobre los hechos producidos.

- El 3 de diciembre de 2019 se procede a la búsqueda del origen de los datos y se descubre que en la antigua página web <******URL.1*** > había dos opciones que coinciden con la información expuesta: "*Actualiza tus datos*", (desde agosto de 2012 hasta el cierre de la página en 2016) que se corresponde con la

información de la primera base de datos, y "*Trabaja con nosotros*", (desde diciembre de 2008 hasta el cierre de la página en 2016) que se corresponde con la segunda base de datos.

A última hora de la mañana JAUS remite una opción para extraer información por medio del panel de control del servidor, pero la información proporcionada no aclara la filtración de los datos, por lo que se solicita de nuevo la información de los *logs* del sistema operativo.

- El 4 de diciembre de 2019, se reclama la información del *log* del sistema.
- El 5 de diciembre de 2019 se reclama de nuevo los *logs* del servidor, concretando la información necesaria.

Se planifica el envío de comunicación a los afectados para el día 11 de diciembre.

- El 6 de diciembre de 2019 el *hacker* publica en su blog (******BLOG.1***, anonimizado por la AEPD) que dispone de la base de datos de currículos, y continúa apuntando a una brecha en el Grupo Caja Rural. En dicho Blog se publica una muestra de registros, que coincide con la base de datos de currículos.

A este respecto, desde la Inspección de Datos, con fecha 14 de abril de 2020, se ha accedido al blog mencionado obteniendo como respuesta que el canal no se ha encontrado.

- El día 10 de diciembre de 2019, el periódico ******PERIÓDICO.1*** publica dos artículos haciéndose eco de la existencia de una nueva filtración, aunque realmente es la misma, bajo el título "******TÍTULO.1***" y una segunda publicación bajo el título ¿"******TÍTULO 2*** "*? Compruébalo aquí*". Esta segunda publicación permite introducir el número de teléfono móvil indicando si el número estaba afectado por la brecha.

Se comprueba que estas publicaciones hacen referencia a la base de datos de currículos y se observa que el acceso al servidor que contiene la web <******URL.3*** > está activo, por lo que se solicita el cierre al proveedor JAUS.

Se notifica la brecha de seguridad al Banco de España.

Desde la Inspección de Datos de la AEPD se comprueba que con fecha 13 de abril de 2020 en la dirección ******URL.4*** (anonimizado por la AEPD) figura la publicación de la noticia "*¿*******TÍTULO.2****? Compruébalo aquí"* de fecha 30 de noviembre de 2019, donde se pone de manifiesto que se ha difundido una base de datos de al menos 637 clientes con información personal y privada, entre la que se incluye el *hash* de su contraseña y se adjunta un listado parcialmente anonimizado.

Asimismo, en esta misma fecha se comprueba que en la dirección ******URL.4*** (anonimizado por la AEPD) figura la publicación de la noticia "***NOTICIA.1****"* de fecha 10 de diciembre de 2019, en la que se informa que el 30 de noviembre hubo una filtración con datos de 637 clientes que fueron expuestos en internet y de otra filtración de currículos con datos personales, y acompaña un listado parcialmente anonimizado. (ambas publicaciones se han incorporado al expediente mediante diligencia de fecha 13 de abril de 2020)

- El 11 de diciembre de 2019, personal de Caja Zamora y de RSI se reúnen con la Unidad de Ciberdelitos de la Policía Nacional con la intención de denunciar el hecho ante las autoridades.

Se confirma el cierre del acceso al servidor

Se realiza la notificación a los afectados mediante correo electrónico, realizándose 1443 notificaciones. Se reciben 28 solicitudes individuales de petición de ampliación sobre la información expuesta respondiéndose a todas ellas.

- El 16 de diciembre de 2019 se procede al traslado de los dominios desde Bluefactory a JAUS con objeto de obtener los *logs* del sistema.
- El 17 de diciembre de 2019 se cierra el blog de ******BLOG.1***, tras lo que el hacker envía nuevas comunicaciones a afectados haciendo referencia a un nuevo blog (******BLOG.2***, anonimizado por la AEPD).

En relación con este nuevo blog, desde la Inspección de Datos y con fecha 14 de abril de 2020, se verifica que existe una noticia relacionada con una brecha en Ruralvia.

- El 18 de diciembre de 2019 se solicita informe a JAUS explicando los motivos de la brecha, que se recibe el 2 de enero de 2020.
- El 3 de enero de 2020 se envían por correo postal certificado las comunicaciones a los afectados rechazadas, quedando 15 pendientes de las que no existe información.
- El día 9 de enero de 2020 se comunica a los cinco afectados que solicitaron la cancelación de los datos la imposibilidad conforme a lo dispuesto en el art. 17.3. del RGPD.

<u>Respecto de las causas que hicieron posible la brecha</u>

- La brecha se ha producido por la existencia de una copia de la antigua página web, que Caja Zamora tenía contratado con JAUS el alojamiento y mantenimiento desde diciembre de 2008 hasta mayo de 2016. Esta copia de la antigua página web tenía dos bases de datos con información personal (correspondiente al periodo mencionado), con un total de 1443 registros de distinta índole.
- Caja Zamora manifiesta que la copia se encuentra almacenada en un dominio abandonado, en un servidor con vulnerabilidades, gestionado por un tercero, y desconocía su existencia por lo que consideran que los encargados del tratamiento contratados han incumplido el contrato en los siguientes términos:
  - Cláusula decimosegunda aparatado III, almacenando información sin las debidas medidas de seguridad. "*El proveedor aplicará a los ficheros de CR de Zamora las medidas de seguridad a que se refiere el artículo 9 LOPD y demás normativa de desarrollo*"
  - Cláusula decimosegunda apartado V, guardando información perteneciente a Caja Zamora, una vez cumplida la prestación del servicio. "*Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al cliente como responsable del tratamiento al igual que cualquier soporte o documentos en que consta algún dato de carácter personal objeto de tratamiento*".

Medidas de minimización del impacto de la brecha de seguridad

- En el momento en el que se detecta el origen de la información expuesta, se procede a la parada de los servicios del servidor, evitando así la exposición de la información. El servidor queda inactivo el día 30 a la 13:00 horas. El proveedor de servicios Bluefactory lo vuelve a poner en servicio y se vuelve a cerrar el servidor.

- Como medida preventiva, se corta el acceso a todas las páginas web alojadas por proveedores externos, cerrando los sitios web <***URL.2***> y <***URL.3***>.

- Se realiza un profundo análisis de la información obtenida en el análisis de vulnerabilidades a lo largo septiembre de 2019 descartando una brecha dentro de la estructura de Caja Zamora.

Se complementa la acción anterior con una revisión manual de todos los sistemas de Caja Zamora, realizando revisiones de ordenadores personales, servidores y unidades de red.

- Se realiza la notificación de la brecha a la AEPD y al Banco de España. Se ha mantenido contacto con INCIBE para notificar la brecha,

Respecto de los datos afectados.

- El incidente afecta a dos bases de datos de la antigua web de Caja Zamora, estas son: "*Actualiza tus datos*", aplicación activa desde agosto de 2012 hasta el cierre de la página en 2016. Esta aplicación se corresponde con la primera base de datos con 643 registros. Y "*Trabaja con nosotros*", activa desde diciembre de 2008 hasta el cierre de la página en 2016. Se corresponde con la segunda base de datos, con 800 registros.

- El número total de registros afectados es de 1.443.

- La aplicación "*Actualiza tus datos*" contiene información básica relativa a datos identificativos y de contacto, en concreto: apellidos, nombre, NIF, sexo, fecha de nacimiento, dirección postal, mail, teléfono, nacionalidad y contraseña cifrada.

- La aplicación "*Trabaja con nosotros*" contiene información relativa a datos identificativos, de contacto, y datos curriculares como datos de formación, idiomas, experiencia profesional y contraseña sin cifrar.

- Caja Zamora manifiesta que no era posible el acceso a Banca Electrónica, ni la realización de movimientos económicos debido a las medidas de seguridad de doble factor de autenticación implantado.

- Se comunicó la brecha de seguridad a los 1443 afectados a través de correo electrónico el 11 de diciembre de 2019 y por carta postal certificada a los correos electrónicos rechazados. Hay 15 afectados con los que no se ha podido contactar.

Caja Zamora ha aportado escrito remitido a los afectados donde se les informa sobre el incidente que ha provocado que los datos personales quedaran expuestos a terceros y uno de los datos hace referencia a una contraseña por lo que les recomiendan la modificación de la misma si la utilizaban en otras aplicaciones.

También informan de que no se han producido accesos a información financiera, transacciones, ni movimientos de ningún tipo. Y proporcionan la dirección de correo electrónico del Delegado de Protección de Datos.

- Caja Zamora manifiesta que no hay constancia de que los motores de búsqueda hayan indexado los datos de los afectados.

Respecto de las acciones tomadas para la resolución final de la brecha

- Caja Zamora manifiesta que se continúa solicitando los registros del sistema operativo (*logs*) para intentar determinar la actividad del *hacker*.

Respecto de las medidas de seguridad implantadas con anterioridad la brecha

- Caja Zamora ha aportado la siguiente documentación:

  o Registro de actividad del tratamiento *Gestión de clientes* y Evaluación de Impacto realizada en 2018 sobre dicho tratamiento. Entre los riesgos altos que se detectan consta textualmente "*1.30 Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron"*. Asimismo, figura que una vez implantados los controles necesarios el riesgo residual es de nivel *Medio.*

  o Copia del registro de actividad del tratamiento *Gestión de selección de personal* en el que figura que no es necesario la realización de una Evaluación de Impacto.

  o Plan de Adecuación e Implantación de las medidas derivadas del Esquema Nacional de Seguridad de fecha 23 de octubre de 2019.

Respecto de las medias implementadas con posterioridad la brecha

- Se están revisando todos los contratos de todos los proveedores que tengan algún tipo de relación contractual con Caja Zamora, especialmente aquellos proveedores que tengan acceso a datos personales, analizando la posibilidad de realizar una auditoría de seguridad sobre aquellos proveedores que manejen datos personales de la Caja Zamora.

- Se ha comenzado la elaboración de un procedimiento de control para la solicitud de borrado de datos personales a aquellos proveedores que dispongan de datos personales en los que actúe Caja Zamora como responsable del tratamiento.

- Se ha ordenado a todos los proveedores de servicios web el cierre de sus páginas y la entrega de la documentación a Caja Zamora, con el fin de internalizar el servicio utilizando únicamente la estructura del Grupo Caja Rural.

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, se produjo una brecha de seguridad de los datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, como consecuencia del acceso indebido por terceros ajenos al sistema de información de Caja Rural Zamora.

El artículo 32 del RGPD señala 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.".

El citado artículo contempla que "*el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".* En consecuencia, no adopta una relación cerrada de medidas técnicas y organizativas, sino que éstas deberán ser las apropiadas en función del nivel de riesgo previamente analizado.

Añade el artículo 33.1 y 2 del RGPD que: "*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.".* Y el apartado 2 : *"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".*

El artículo 34.1 y 2, establece la obligación de comunicar la brecha de seguridad en los siguientes términos:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

1. *La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d)".*

En consecuencia, se trata de determinar si las medidas técnicas y organizativas eran las adecuadas al nivel de riesgo predeterminado, así como la diligencia en la reacción ante una brecha de seguridad y, en su caso, las medidas adoptadas para evitar que en el futuro pueda repetirse una incidencia de similares características que pueda comprometer los derechos y libertades de los interesados.

De las actuaciones de investigación se desprende que Caja Zamora, en calidad de responsable del tratamiento, disponía de medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias pero, sin embargo, de forma excepcional se produjo la incidencia ahora analizada con la intervención de un ataque exterior mediante una actuación presuntamente delictiva.

Consta que Caja Zamora realizó una auditoria y análisis de riesgos (en 2018) en el que se advirtió, tras la realización del registro de tratamientos, un riesgo de nivel alto como consecuencia de "*Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron*.", Ante este tipo de riesgo detectado, Caja Zamora procedió a implantar los controles necesarios para minimizar el riesgo a nivel medio (riego residual). Tras esta

disminución de la gradación del riesgo no consideró preciso realizar una evaluación de impacto.

Con posterioridad, agosto de 2019, Caja Zamora procedió a auditar los tres dominios indicados sin que se detectara el origen de la brecha ahora analizada, que consistió en la salvaguarda del dominio web antiguo de Caja Zamora en una carpeta oculta embebida en una de las nuevas webs corporativas y ajena al contrato de mantenimiento, lo que propició que un atacante malicioso aprovechara esta vulnerabilidad sobrevenida para acceder a los datos. Este cúmulo de errores sobrevenidos de índole administrativa, temporal y técnica, no fue detectado en el análisis de riesgos como probable o de riesgo alto. Hay que señalar de forma especial la causa administrativa indicada ya que el origen de la brecha pudo haberse evitado mediante un escrupuloso seguimiento del contrato de mantenimiento/alojamiento suscrito entre Caja Zamora y las entidades encargadas del mantenimiento y/o alojamiento de los diferentes dominios web en construcción y mantenimiento.

Con carácter previo a la brecha de seguridad (en octubre de 2019), Caja Zamora inició un plan de adecuación e implantación de las medidas de seguridad derivadas del Esquema Nacional de Seguridad (ENS).

Asimismo, Caja Zamora disponía de protocolos de actuación para afrontar el incidente, lo que ha permitido la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, comunicar, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas, como son el responsable del tratamiento y las agencias colaboradoras en calidad de encargadas, así como con los distintos Delegados de Protección de Datos del Grupo Caja Rural. Consta también que Caja Zamora interpuso denuncia ante la unidad de delitos informáticos de la Policía Nacional al considerar la conducta del *hacker* como presunto hecho delictivo.

Cabe señalar que los datos personales de los afectados no están afectos a datos especialmente protegidos y que no permiten acceder a las cuentas financieras ni hacer uso indebido de ellas, precisamente, a los protocolos previamente implantados de doble factor de autenticación. Por otro lado, en cuanto a la base de datos denominada *“actualiza tus datos”,* los datos comprometidos son datos básicos: apellidos, nombre, NIF, sexo, fecha de nacimiento, dirección postal, mail, teléfono, nacionalidad y contraseña cifrada. Y respecto de la base de datos denominada *“Trabaja con nosotros”* los datos afectados hacen referencia a identificativos, de contacto, y datos curriculares (datos de formación, idiomas, experiencia profesional) y contraseña sin cifrar, motivo por el que se procedió a comunicar a los afectados la incidencia para que procedieran a modificar las claves iguales de aquellas otras aplicaciones de las que eran usuarios, al objeto de evitar accesos indebidos. No obstante, se significa que con solo la clave expuesta no es posible el acceso a la banca electrónica al estar el acceso configurado con doble factos de autenticación.

Consta que Caja Zamora durante el proceso de respuesta, en una primera fase intenta contener el incidente, tras lo cual se erradica la situación generada por el mismo y termina con las acciones de recuperación oportunas. También contrató la investigación

con una entidad especializada en ciberataques al objeto de analizar los hechos y recopilación de evidencias forenses precisas para posteriormente interponer denuncia ante la policía.

Solucionada la brecha de seguridad y verificada la eficacia de las medidas adoptadas, Caja Zamora abordó la fase de recuperación, que tiene como objetivo el restablecimiento de la seguridad del servicio en su totalidad, confirmando finalmente su correcto funcionamiento y evitando en la medida de lo posible que sucedan nuevos incidentes basados en la misma causa.

No constan reclamaciones ante esta Agencia de los afectados aun habiendo sido informados de la brecha de seguridad, y aquellos que solicitaron ampliación de información les fue facilitada.

En consecuencia, se debe concluir que Caja Zamora disponía de medidas técnicas y organizativas razonables y proporcionales al nivel de riesgo para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente mediante formación y concienciación en materia de seguridad a los empleados y personal externo, revisión de pruebas de cumplimiento de prácticas de seguridad, revisión de los contratos con agentes externos que se refieran a tratamientos de datos personales, internalización de aplicaciones web e implantación de auditorías de seguridad. Además, Caja Zamora dispone de un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto sobre los afectados. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada causada previsiblemente por un error puntual.

III

Por lo tanto, la actuación de Caja Zamora como entidad responsable del tratamiento ha sido razonable y proporcional con las obligaciones que impone 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 CAJA RURAL DE ZAMORA COOPERATIVA DE CREDITO, con NIF F49002454 y con domicilio en Avda. Alfonso IX número 7, 49013 Zamora.

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

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

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