Procedimiento Nº: E/07025/2019
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: Con fecha 28 de junio de 2019, la entidad ***VIDA-CAIXA S.A.U. DE SEGUROS Y REASEGUROS,*** con NIF ***A58333261*** (en adelante, Vida-Caixa) notificó a la Agencia Española de Protección de Datos (en adelante AEPD) una violación de seguridad de datos personales obrantes en el sistema de información como consecuencia de un acceso indebido por tercera persona ajena pudiendo haber afectado a 25.874 clientes.

SEGUNDO: Recibida la notificación, la Directora de la AEPD instó a la Subdirección General de Inspección de Datos a que procediera la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la notificación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Las actuaciones de inspección se inician por la recepción de un escrito de notificación de quiebra de seguridad remitido por VIDA-CAIXA en el que informan a la Agencia Española de Protección de Datos que, con fecha 25 de junio de 2019, la entidad VIDA-CAIXA S.A.U. DE SEGUROS Y REASEGUROS ha tenido conocimiento del acceso a datos de pólizas de seguros de clientes por parte de un tercero ajeno. La incidencia se ha ocasionado al haber asignado a un cliente un perfil de acceso erróneo que le daba permisos como si fuera un empleado interno de VIDA-CAIXA, pudiéndose descargar información de otras pólizas en su perfil de cliente. El propio usuario informa a la compañía del incidente.

ENTIDADES INVESTIGADAS

VIDA-CAIXA S.A.U. DE SEGUROS Y REASEGUROS con NIF A58333261 con domicilio en PASEO RECOLETOS 37, 3º - 28004 MADRID (MADRID).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 2 de agosto de 2019 se remite requerimiento de información VIDA-CAIXA y de la respuesta recibida se desprende:

Respecto de la empresa **CONTRATO CONFIDENCIAL**

- VIDA-CAIXA ha aportado copia del contrato marco suscrito con IT CORPORATE SOLUTIONS SPAIN SL (en adelante DXC TECHNOLOGY), de

fecha 21 de diciembre de 2018, para la prestación del servicio de soporte de proyecto informáticos incluyendo el mantenimiento de las aplicaciones de VIDA-CAIXA existentes así como el desarrollo de nuevas aplicaciones.

En virtud del contrato marco, por cada proyecto se firma un documento de encargo donde se incluyen una serie de medidas de seguridad respecto de la información a la que se va a tener acceso y un anexo sobre confidencialidad y tratamiento de datos de carácter personal.

VIDA-CAIXA manifiesta que DXC TECHNOLOGY tiene certificación en diferentes estándares, entre ellos, certificación ISO 27001.

Respecto de la cronología de los hechos. Las medidas realizadas para minimizar el impacto de la incidencia. Informe de la incidencia

- El día **25/06/2019** se detectó un incidente de seguridad en la Plataforma de Clientes por una llamada de un cliente (persona jurídica) que observó que la información descargada no correspondía a su póliza (opción Descarga de adhesiones de la Plataforma).
    - A las 9:40 horas, el cliente comunica la incidencia e indica que ha procedido a eliminar el fichero con la información descargada errónea.
    - A las 9:49 horas, VIDA-CAIXA contacta con la compañía LINECOM NETWORKS SL (en adelante LINECOM) encargada del mantenimiento de la Plataforma y con el equipo de Sistemas Informáticos de VIDA-CAIXA para comunicar la incidencia y solicitar el bloqueo de la Plataforma.
    - A las 10:19 horas, LINECOM confirma que ha procedido a ocultar la opción “Descarga de adhesiones” de la Plataforma para su revisión y para impedir que pudiera darse un nuevo incidente.
    - A las 12:35 horas se solicita un informe a LINECOM, el cual sospecha que el incidente ha podido producirse por un error en el procedimiento de alta de los usuarios y en la propia aplicación.
    - Con motivo de este informe se ejecuta el siguiente plan de acción:
        - Modificación del Protocolo de gestión de usuarios de tal forma que no se puede asignar un perfil interno de acceso a la Plataforma si no figura como empleado de VIDA-CAIXA.
        - Se verifican los usuarios internos
        - Se procede a la autenticación en llamadas a servicios web, servicios de acceso a datos en procesos de validación.
        - Implantar un sistema de alarma en caso de detectar accesos no autorizados.
        - Se procede a comprobar que se ha eliminado la opción de descarga de todas las adhesiones, y verificar si hay histórico

de peticiones similares que pudieran haber provocado brechas anteriores no detectadas.

- Se comprueba que no ha habido ningún otro incidente similar posterior al notificado.

- El día 27/06/2019 se descarta el error en asignación de usuario y se comprueba que ha sido un error de la aplicación cuando se solicitaba la descarga de información con los siguientes criterios: usuario tomador, póliza mediada y opción de descarga de adhesiones para todas las pólizas. En este caso el sistema entendía que la solicitud era interna y procedía a descargar todas las pólizas accesibles desde la plataforma en vez de las asociadas al cliente.

Este proceso de descarga masiva se realiza en diferido (batch) y el programa informático enviaba como parámetro el código de usuario para delimitar las pólizas asociadas al usuario. Se detectó que cuando el usuario era del tipo “tomador” no se enviaba bien el código de usuario por lo que el Sistema interpretó que el solicitante era un usuario interno. Además, al seleccionar la opción de “todas las pólizas” el Sistema descargó todas las pólizas accesibles desde la Plataforma (aquellas que se incluyen en el contrato de interacción).

Al haber deshabilitado esta opción se ha evitado que la incidencia pueda de nuevo producirse.

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

- El día 27/06/2019 se implementa una corrección de código de la aplicación para evitar que todos los usuarios dispongan de la opción de descargar todas las pólizas permitiendo solo descargar las pólizas seleccionadas y visibles en el aplicativo desde su usuario.

Respecto de los datos afectados

- El número de clientes afectados es de 25.874
- Los datos accedidos corresponden a: nombre y apellidos, NIF, fecha de nacimiento e importes de referencia (salarios).
- La empresa ES FIELD DELIVERY SPAIN, S.L. (en adelante, “FDS”), cliente de VIDA-CAIXA fue la entidad que ha tenido acceso a la información y que avisó de la incidencia en el momento que detectó que la descarga no era correcta y que el fichero contenía información (adhesiones) de otros clientes.

A este respecto VIDA-CAIXA ha aportado certificado emitido por FDS donde se indica que el fichero descargado fue eliminado el 25 de junio de 2019 sin hacer uso indebido del mismo.

- VIDA-CAIXA manifiesta que no se ha comunicado la incidencia a los clientes ya que consideraron que no existía un riesgo para sus derechos y libertades puesto que se bloqueó inmediatamente la aplicación para evitar que el error se pudiera reproducir. Además el cliente que se había

descargado los datos aseguró la destrucción del fichero sin hacer ningún uso del mismo.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- VIDA-CAIXA ha aportado copia de la Norma de Seguridad y Privacidad, que desarrolla la Política de Privacidad y que recoge, a su vez, la adhesión de VidaCaixa al cuerpo normativo desarrollado por CaixaBank en materia de Seguridad de la Información que se transmite a todos los empleados. En dicho documento se designa como DPO el Delegado de Protección de Datos de CaixaBank y se especifica, entre otros aspectos, la adopción de la metodología de Evaluaciones de Impacto, de atención de ejercicio de los derechos y de las comunicaciones de violaciones de seguridad de CaixaBank.

Asimismo, se recoge un conjunto de procedimientos técnicos y normas de comportamiento para el correcto funcionamiento del Sistema de Seguridad: acceso a las bases de datos, obligaciones de los usuarios, confidencialidad de la información, utilización del correo electrónicos, etc …

- VIDA-CAIXA manifiesta que desde enero de 2006 se llevan a cabo campañas de concienciación en Seguridad y Protección de Datos.

Y desde el año 2016 se hacen seguimientos mensuales de las medidas técnicas y organizativas sobre Protección de datos y seguridad, se realizan análisis y tratamiento de riesgos y en el año 2017 se implantó un Gestor de Información y Eventos de Seguridad que notifica de cualquier incidente de seguridad.

En Mayo de 2018 se incluyó una revisión mensual de los registros de acceso a datos personales especiales y en enero de 2019 se realizaron auditorías periódicas de análisis de vulnerabilidades de todas las páginas webs abiertas al exterior.

En abril de 2019 se comenzó una auditoria anual de revisión del código de las aplicaciones y estaba previsto para julio de 2019 la revisión del Sistema de información origen del incidente de seguridad ocurrido. VIDA-CAIXA ha aportado diagrama de planificación de la Auditoria Anual.

- VIDA-CAIXA manifiesta que el motivo por el cual las medidas de seguridad implantadas no han impedido el incidente ha sido por un error en la programación del portal que no fue detectado.
- VIDA- CAIXA ha aportado Registro de Actividad de los tratamientos de asignación y control de permisos y de desarrollo y mantenimiento de software

Respecto de las medias implementadas con posterioridad a la incidencia

- VIDA-CAIXA dispone de un reporte diario de alarmas ante ciberataques y ha implementado un nuevo Firewall que bloquea los ataques webs.
- A raíz del incidente de privacidad ha iniciado un proyecto para incluir nuevos controles preventivos adicionales para verificar que la información

que se intercambia entre cliente y los sistemas sea la correcta. Este proyecto se implementará a lo largo de 2020. Actualmente, se encuentra en fase de análisis, selección de tecnología y oferta de los proveedores.

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 quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una posible brecha de confidencialidad como consecuencia del acceso indebido al sistema de información de VIDA-CAIXA por tercera entidad.

De las actuaciones de investigación se desprende que VIDA-CAIXA disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Asimismo, el VIDA-CAIXA disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente 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, 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 el Delegado de Protección de Datos. Consta también, certificado de la entidad que accedió al sistema de información de VIDA-CAIXA acreditando que los datos obtenidos tras el acceso indebido fueron destruidos y sin haber sido objeto de otro tratamiento.

No constan reclamaciones ante esta Agencia de los afectados.

En consecuencia, consta que el VIDA-CAIXA disponía de forma previa de medidas técnicas y organizativas razonables en función del nivel de riesgo para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente procediendo de forma rápida a eliminar del sitio web la pestaña de acceso masivo a descargas de pólizas. Además, el VIDA-CAIXA elaboró un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final que resultó ser mínimo para 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, se ha acreditado que la actuación de VIDA-CAIXA como entidad responsable del tratamiento ha sido acorde 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 ***VIDA-CAIXA S.A.U. DE SEGUROS Y REASEGUROS,*** con NIF ***A58333261*** y con domicilio en ***PASEO RECOLETOS 37, 3º - 28004 MADRID (MADRID).***

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