- **Procedimiento Nº: E/06711/2020**

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 la notificación a la Agencia Española de Protección de Datos (en adelante, AEPD) de una brecha de seguridad de datos personales por parte de la entidad AVALMADRID, S.G.R., (en adelante, AVALMADRID), con número de registro de entrada 027958/2020, relativa al acceso no autorizado a datos de clientes por parte de jáqueres, la Directora de la AEPD ordenó el 11/08/2020 a la Subdirección General de 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: 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 reclamación, teniendo conocimiento de los siguientes extremos:

Resumen de la notificación:
-Acceso no autorizado a sus repositorios de información en el que se extrajeron datos de personas relacionadas con su entidad de manera ilegítima por parte un tercero.

Documentación aportada con la notificación:
- Descripción sobre el acceso no autorizado, medidas adoptadas, medidas a adoptar, consideraciones sobre el ataque producido y valoración y participación del delegado de protección de datos en la notificación de la brecha y el Anexo que lo acompaña.
- Copia de su política general de seguridad de la información, versión 01 de fecha 22/10/2019.

Entidad investigada:
Durante las presentes actuaciones se ha investigado la siguiente entidad:
AVALMADRID, S.G.R. con NIF V28737526 y domicilio en C/ JORGE JUAN, Nº 30 - 28001 MADRID (MADRID).

Respecto de la cronología de los hechos:

Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final:
AVALMADRID manifiesta que el día 02/08/2020 comunica al Responsable de Sistemas de la Sociedad que se ha recibido un mensaje a través de la intranet indicando que se ha accedido de forma ilegítima al sitio web y a la intranet asociada al mismo.

Posteriormente a la recepción del mensaje, informa de haber detectado que en su sitio web https://www.avalmadrid.es/index.php se había producido una modificación en un texto de forma ilegítima;

La Entidad investigada afirma haber procedido a revisar los hechos descritos en la publicación y haber comprobado que terceras partes no autorizadas habían tenido acceso a su intranet. En la estructura de carpetas del servidor se encontraban las carpetas pertenecientes a un repositorio FTP (protocolo de transferencia de archivos) en el cual se almacenaba documentación relativa a procedimientos judiciales de reclamación de deuda iniciados por su parte contra socios partícipes. Los documentos presuntamente filtrados se encontraban en dicha FTP, por lo que considera que habrían tenido acceso a la misma y potencialmente podrían haber obtenido toda la información almacenada. Sin embargo, tras haber revisado los logs de dicha carpeta, no se ha podido constatar que se haya producido una descarga de información masiva.

AVALMADRID alega haber comunicado las incidencias detectadas a quien presenta como proveedor suyo de servicios ******EMPRESA.1*** con NIF ******NIF.1***, al que señala como encargado del tratamiento en la actividad del tratamiento puesta en cuestión en la presente brecha de seguridad

La entidad investigada afirma haber procedido a cambiar todas las contraseñas de acceso a la plataforma del proveedor, así como las contraseñas de acceso a su sitio web y las de todas las cuentas de su intranet. Según su versión, el 03/08/2020 procedió a desactivar el acceso a la web mediante usuario y contraseña, desactivando la intranet por completo para que ningún usuario pudiera tener acceso a dicha plataforma. El citado proveedor de servicios le comunica haber bloqueado el acceso a las “shells” (intérprete de órdenes/comandos) utilizadas por parte de los atacantes, así como haber corregido el código fuente que posibilitaba acceder al sitio web y a la intranet. La investigada añade que el proveedor le facilitó las direcciones IP (protocolo de internet) desde las que presuntamente se habrían realizado los accesos fraudulentos por parte de los atacantes, así como todos los logs del último mes, en las que no se constataban accesos fraudulentos.

Ante la posibilidad de comunicación con la red social tumblr para la posible retirada de contenidos publicado, la investigada responde que, dado el perfil de la organización que presuntamente ha producido el ataque, ha considerado contraproducente intentar ponerse en contacto para eliminar la publicación, atendiendo a casos previos en los que se ha producido un importante daño, sin que finalmente se haya logrado resultado alguno.

La entidad investigada expresa haber procedido a interponer la correspondiente denuncia ante la BIT (brigada de investigación tecnológica) de la Policía Nacional.

Respecto de las causas que hicieron posible la brecha:

La entidad investigada informa de que la técnica empleada por parte del grupo atacante fue la de inyección de código en el sitio web y la intranet, de tal modo que se permitió, a partir de dicha inyección de código, tener acceso al control del sitio web y la intranet, así como a la carpeta FTP a través de la que se intercambiaba la documentación con los diferentes despachos de abogados que le prestan servicios en relación con reclamación de cantidades económicas. AVALMADRID expresa que tanto los servidores como el sitio web y la intranet contaban con las medidas de seguridad relativas a la identificación de usuarios, control de accesos de conformidad con las recomendaciones realizadas por ENISA (Agencia de la Unión Europea para la Ciberseguridad) en su “Handbook on Security of Personal Data Processing”

Respecto de los datos afectados:

La entidad investigada reseña que se han publicado datos personales relativos, únicamente, a 9 personas físicas, siendo su tipología de carácter identificativo (nombres y apellidos) y de carácter económico patrimonial, todos ellos relacionados con la deuda contraída e impagada con su entidad. No se ha tenido acceso a datos personales especialmente protegidos en la presenta brecha de seguridad. En cuanto al archivo alojado en el servidor FTP, supuestamente se ha tenido acceso por parte de los atacantes a datos personales de 2.200 personas físicas de las tipologías carácter identificativo (nombres y apellidos) y de carácter económico patrimonial, todos ellos relacionados con la deuda contraída e impagada con su entidad. En este caso, la investigada manifiesta que no existen evidencias de la descarga de ninguna copia ni de la utilización de ningunos de estos datos por parte de los atacantes.

En relación con las consecuencias que pueden sufrir los posibles afectados, AVALMADRID defiende haber valorado los riesgos para determinar que el principal impacto que se podría producir es el hecho de que se conozca de forma pública que determinada persona jurídica, y por ende sus avalistas personas físicas, adeudan una cantidad determinada a su entidad, así como que dicha cantidad económica está siendo reclamada en vía judicial. La entidad investigada se presenta como entidad financiera con la obligación de comunicar periódicamente todos los riesgos financieros y operacionales existentes relacionados con sus socios partícipes, y avalistas de éstos, a la Central de Riesgos del Banco de España (CIRBE) y a los ficheros de solvencia patrimonial, por lo que el resto de las entidades financieras tienen conocimiento de la situación en la que se encuentran las operaciones que la investigada tiene con sus socios partícipes y los avalistas de éstos (situación normal, dudosa, morosa etc.) La entidad investigada expresa que sus clientes dan consentimiento expreso a esta comunicación a CIRBE y a los ficheros de solvencia patrimonial tanto en el momento en el que solicita la operación con la firma de la solicitud de aval, como en el momento en el que se firma el contrato con ella ante notario. La única evidencia de utilización de datos de terceros se encuentra en la publicación realizada por “La Nueve de Anonymous” en la web de tumblr, en la que únicamente existe evidencia mediante las capturas de pantalla publicadas (datos personales identificativos y financieros de 9 personas físicas).

Respecto de las medidas de seguridad implantadas previamente al acontecimiento de la brecha de seguridad:

AVALMADRID expone haber tomado como referencia para definir el sistema de seguridad de la información el cumplimiento de la normativa de protección de datos lo recomendado por ENISA en su “Handbook on Security of Personal Data Processing” y de que se encuentra en un proceso de alineamiento de sus sistemas de seguridad de la información interno con el estándar internacional ISO 27.701, teniendo previsto certificarse externamente. Asimismo manifiesta haber seleccionado a su proveedor encargado del tratamiento para el alojamiento web, tomando en consideración que la citada entidad cuenta con un sistema de seguridad de la información basado en ISO 27.001:2013 debidamente certificado por AENOR. La investigada expresa que la certificación de AENOR sigue la norma de referencia UNE-ISO/IEC 27001:2014 («Tecnología de la Información – Técnicas de seguridad – Sistemas de Gestión de la Seguridad de la Información (SGSI) – Requisitos») idéntica a la norma internacional

ISO/IEC 27001:2013 («Information Technology – Security Techniques – Information Security Management Systems – Requirements»), y es reconocida internacionalmente por la asociación IQNET. La entidad investigada alega que dicha certificación de su proveedor encargado del tratamiento abarca los procesos orientados a garantizar la seguridad en los sistemas de información que soportan los servicios prestados, así como el correcto y adecuado funcionamiento y mantenimiento de las infraestructuras de su centro de proceso de datos. Adicionalmente, expresa que los sistemas de información alojados en los servidores de su proveedor encargado del tratamiento cumplían con las medidas de seguridad de nivel básico y nivel medio recomendadas por ENISA.

AVALMADRID aclara que:

- Todas las medidas de seguridad asociadas a la infraestructura tecnológica en la que se encuentra alojada su web y su intranet se encuentran externalizada como hosting (servicio de alojamiento para sitios web) en el proveedor encargado del tratamiento. Entre las diferentes medidas de seguridad se encuentra la prestación de servicios de Firewall gestionado, así como la aplicación del resto de medidas de seguridad físicas y lógicas comprendidas en el citado estándar de seguridad.

- El sitio web y la intranet, así como el servicio de FTP a través del que se intercambiaba la documentación con los diferentes despachos de abogados proveedores de la entidad fue desarrollada por ******EMPRESA.2*** (con NIF ******NIF.2***), siendo realizado por ella el mantenimiento habitual de dicha plataforma y las actualizaciones de la misma.

La entidad investigada aporta copia parcial de su registro de actividades de tratamiento referida a las actividades del tratamiento “Contratación” y “Recursos Humanos”, que según informa son las afectadas por la presente brecha de seguridad. La actividad del tratamiento “Contratación” tiene por finalidad la gestión de las operaciones con titulares, avalistas y otros intervinientes no deudores e incluye los siguientes procesos: comercial, análisis de la operación, formalización y recuperación. El proceso afectado en la brecha de seguridad dentro de dicha actividad del tratamiento es el de recuperación de deudas como legítimos acreedores.

En cuanto a la actividad del tratamiento “Recursos Humanos”, aclara que su finalidad es la gestión del personal de la empresa, lo que implica la gestión de los contratos de trabajo, la gestión de nóminas y seguros sociales, la prevención de riesgos laborales y la vigilancia de la salud, por lo que se vio afectada al accederse a los correos electrónicos corporativos y al nombre de usuario corporativo.

AVALMADRID aporta copia de análisis de riesgos respecto a confidencialidad, integridad y disponibilidad referentes a las actividades del tratamiento “Contratación” y “Recursos Humanos”, presuntamente evaluadas en noviembre de 2018. En los resultados de ambos análisis de riesgos, concluye que el riesgo del tratamiento respecto a la confidencialidad, integridad y disponibilidad es bajo, de tal modo que no se requiere evaluación de impacto relativa a la protección de datos de los tratamientos afectados por la presente brecha de seguridad.

La entidad investigada informa de haber realizado los siguientes informes de auditoría y seguridad:

- Informe realizado por ******EMPRESA.3*** el 25 de abril de 2018. Su periodo de referencia el ejercicio 2017 y su alcance es recoger los resultados obtenidos tras la

realización de los análisis del tratamiento de datos de carácter personal por parte de la sociedad conforme a lo establecido en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Informe de consultoría realizado por ******EMPRESA.4*** de fecha 20 de noviembre de 2018 con el objeto de adaptar a la sociedad al nuevo RGPD.
- Informe realizado por ******EMPRESA.5*** en septiembre de 2019 cuyo alcance es la revisión de seguridad de Firewall, Office 365, Servidores y Puesto de Usuario.
- Tener previsto la realización un informe de auditoría sobre cumplimiento de normativa en protección de datos por una consultora independiente para el primer semestre de 2020, el cual fue pospuesto con motivo de la pandemia de COVID-19.

Respecto de las medidas de seguridad correctivas tomadas frente a la brecha de seguridad:

AVALMADRID señala que al detectar la incidencia en el entorno de las 20:00 horas del 02/08/2020 su responsable del Departamento de Sistemas puso en marcha el Procedimiento de Gestión de Incidentes de Seguridad, previsto para incidentes de esta naturaleza, notificándolo a través de la aplicación de gestión de incidentes a los departamentos competentes, y procediendo a su registro haciendo constar: fecha y hora de detección, descripción y calificación del incidente, estado actual, prioridad y medidas adoptadas. Aporta copias de imágenes como evidencias de medidas de carácter técnico: correo recibido por el personal, apertura de incidencia a su proveedor encargado del tratamiento, restauración de la página web de inicio, borrado de los accesos FTP y de los distintos repositorios, puesta en contacto con el INCIBE, puesta en contacto con los desarrolladores PXSP para conocer la fecha de la última actualización de su plataforma web y corrección por parte su proveedor encargado del tratamiento de los códigos utilizados para el jaqueo.

La entidad investigada expone haber valorado la procedencia o no de comunicar la presente brecha de seguridad a los interesados al objeto de minimizar en lo posible las consecuencias negativas para los titulares de los datos, habiendo considerado los siguientes factores:

- Criterios establecidos en los apartados 1,2 y 3, del art. 34 RGPD.
- Categoría de los datos personales a los que se ha accedido de forma ilegítima.
- Riesgos para los interesados que se puedan derivar de la violación de seguridad.
- Perfil y objetivos reconocidos por parte de los presuntos autores del ataque.

Habiendo concluido que no se darían los requisitos necesarios para realizar la comunicación por ser menos de 100 registros, los datos involucrados son no sensibles y el impacto es público (accesible en internet).

Respecto de las medidas de seguridad preventivas tomadas frente a hechos como los acontecidos en esta brecha de seguridad:

AVALMADRID expone tener previsto llevar a cabo las siguientes medidas que define como de tipo técnico-organizativas:

- Cambio de la página web a la plataforma WordPress que implica una menor posibilidad de acceso por parte de jáqueres, eliminando la posibilidad de acceso por usuario y contraseña, no almacenando ningún tipo de dato personal y sometiendo la nueva web a una auditoría de seguridad por una empresa externa.
- Cambio de la intranet a su plataforma interna sin posibilidad de acceso desde el exterior.
- Nuevo protocolo de intercambio de información con los despachos externos mediante SFTP (sólo se permitiría el acceso mediante una IP fija) y borrado del contenido de los repositorios semanalmente.
- Revisión de las direcciones IP que han accedido a la web y a la intranet.
- Encargo de un análisis forense para conocer cómo se produjo la brecha de seguridad en su servidor contratado al proveedor encargado del tratamiento, valorando el alcance del jaqueo y estableciendo un plan de actuación para asegurar los servidores y evitar futuras intrusiones, con los siguientes objetivos:
    - o Determinar cómo se produjo la brecha de seguridad y saber si los atacantes dejaron activos que permitiesen tomar el control nuevamente del servidor.
    - o Determinar el alcance del ataque, concretando si el único activo afectado es el servidor contratado al proveedor encargado del tratamiento o se han visto afectados sus servidores internos, o en su caso los servidores de correo electrónico (Microsoft Office 365) utilizados por la organización.
    - o Establecimiento de un plan de actuación para asegurar los servidores y evitar futuras intrusiones.

La entidad investigada presenta copia de un informe de evaluación de la brecha de seguridad sufrida, elaborado en fecha 06/11/2020 por ******EMPRESA.6*** (con NIF ******NIF.3***).

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo:
AVALMADRID expresa que no existe recurrencia ni han acontecido eventos análogos en el tiempo respecto a la presente brecha de seguridad de datos personales, alegando que es la primera y única vez que se ha visto inmersa en un ataque informático.

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 artículo 4 apartado 12 del 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."*

Hay que señalar, que la notificación de una quiebra de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado.
AVALMADRID no ha considerado necesario ni procedente comunicar la presente brecha a los afectados, por los motivos ya expuestos anteriormente.

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, como consecuencia del acceso indebido por terceros ajenos a la base de datos de AVALMADRID.
De la documentación aportada por la entidad investigada en el curso de estas actuaciones de investigación, se desprende que, con anterioridad a producirse la brecha, AVALMADRID disponía de medidas de seguridad y organizativas preventivas razonables a fin de evitar este tipo de incidencias, y acordes con el nivel de riesgo.

En el presente caso, la actuación de AVALMADRID, como entidad responsable del tratamiento, ha sido rápida, razonable y proporcional con la normativa sobre protección de datos personales, y ha implantado nuevas medidas de seguridad proporcionales al riesgo evaluado para evitar la repetición de incidentes similares en el futuro.

No constan reclamaciones ante esta AEPD por parte de posibles clientes afectados

III

Por lo tanto, se ha acreditado que la actuación del reclamado 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 AVALMADRID S.G.R. con NIF V28737526

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