Procedimiento Nº: E/07027/2019
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: *SICOMORO SERVICIOS INTEGRALES, S.L.*, con NIF B99020547 (en adelante, SICOMORO) ha notificado a esta Agencia que tras revisar diversos códigos fuente de la plataforma de ventas de entradas denominada IACPOS, han detectado en la URL un subdominio con posibilidad de acceso público desde buscadores externos. SICOMORO actúa en calidad de encargado del tratamiento de la entidad Aragón Desarrollo y Expansión, S.L. para la gestión de venta de entradas para un evento puntual.

SICOMORO añade que tuvo conocimiento del incidente a través de una noticia publicada en el diario El Confidencial en fecha 22/05/2019.

SEGUNDO: Con fecha de 24/05/2019 la Directora de la Agencia Española de Protección de Datos acuerda iniciar actuaciones de investigación respecto de la supuesta brecha de seguridad notificada por SICOMORO, por lo que la Subdirección General de Inspección de Datos procedió a realizar actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de quiebra: 24/05/2019

ENTIDADES INVESTIGADAS

SICOMORO SERVICIOS INTEGRALES, S.L. con NIF B99020547 con domicilio en Paseo Isabel La Católica 6 - 50009 ZARAGOZA (ZARAGOZA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 24/06/2019 se requiere información a SICOMORO y de la respuesta recibida con fecha 8/07/2019 se desprende:

   Respecto de la Plataforma de gestión de entradas

   - SICOMORO manifiesta que la plataforma de gestión de entradas el evento para el que fue contratada fue un proyecto puntual y fue implantada para la

empresa Aragón Desarrollo y Expansión, S.L. en fecha 3/02/2017, para la gestión de venta de entradas de un evento concreto.

- SICOMORO actúa como encargado del tratamiento para la gestión de venta de entradas.

Respecto de la cronología de los hechos

- El 22/05/2019 SICOMORO tuvo conocimiento de un incidente de seguridad por la publicación de una noticia en el diario El Confidencial, accesible en ***URL.1.

- A este respecto, desde la Inspección de Datos, con fecha 24/05/2019, se ha accedido a la citada dirección verificando que figura información sobre una brecha de seguridad en un determinado evento y en el que constan datos personales parcialmente anonimizados de nombre y apellidos de los visitantes junto con datos de la visita y su importe económico.

- Nada más tener conocimiento de la noticia publicada, SICOMORO se reúne con HIBERUS TECNOLOGIA DE LA INFORMACION, S.L., entidad con la que han creado una Unión Temporal de Empresas (UTE) para la gestión integral de venta de entradas a distintos eventos.

- El propio día 22/05/2019, se inhabilita el acceso a la URL por la que se gestionaba la venta de entradas, se elimina el acceso a la base de datos y se procede al borrado de la base de datos del servidor tras la realización de una copia de seguridad. Asimismo, se revisan otras direcciones del sitio web y subdominios en busca de posibles vulnerabilidades, que no se detectan. También se comprueba que la URL ya no es accesible. Y se encarga la realización de un análisis pericial de los accesos en el sitio web.

- El 23/05/2019 se registra internamente como brecha de seguridad y se presenta denuncia ante la Guardia Civil.

- SICOMORO ha aportado copia del Registro de Incidencias de Seguridad donde se indica que en la aplicación relativa al evento era de uso interno de SICOMORO y del cliente y, por error, quedo accesible al público en general.

- El 24/05/2019 se procede a la notificación de brecha de seguridad a la Agencia Española de Protección de Datos.

- 29/05/2019 se efectúa un peritaje para analizar los registros de accesos (logs) a la web y se detectan distintas direcciones IP asignadas a distintos operadores nacionales que han accedido entre los días

27/03/2019 y 22/05/2019, de las cuales una de ellas se encuentra asociada al nodo de salida de la red "*TOR"*, que no permite identificación.

- El 31/05/2019 se amplía la denuncia ante la Guardia Civil, aportando la documentación resultante del peritaje.

- El 28/06/2019 se recibe ampliación de informe inicial pericial en el que se indica que la causa del incidente fue una mala configuración del servidor que permitió al atacante acceder a la base de datos.

- Según el informe pericial, el sistema permitía a quien conociera la correspondiente ruta interna, acceder a un formulario web con datos de adquirentes de entradas al evento: nombre y apellidos, dirección de correo electrónico, número de teléfono, bienes y servicios recibidos (entradas compradas o anuladas). Todo ello debido a una incorrecta configuración del servidor.

- SICOMORO ha aportado la ampliación del informe pericial donde figura que, con la información publicada, no es posible conocer el número de registros accedidos de un total de 1929 que constan en la base de datos.

Respecto de la categoría de los datos afectados

- SICOMORO manifiesta que el número de afectados sería de 1006, tras la correspondiente depuración de datos nulos o duplicados.

- SICOMORO manifiesta que los datos estarían desactualizados por tratarse de información relativa al año 2017.

- Los datos personales corresponden a: nombre y apellidos, dirección de correo electrónico y número de teléfono.

- SICOMORO manifiesta teniendo en cuenta el tipo de datos comprometidos, los interesados (clientes mayores de edad), el volumen de afectados y la antigüedad de los datos, no supone un alto riesgo para los derechos y libertades de las personas afectadas por lo que no se consideró necesaria la comunicación a las mismas.

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

- SICOMORO manifiesta que inmediatamente inhabilitaron la URL.

- Eliminación de la base de datos del servidor, previa realización de copia de seguridad.

- Suspensión de credenciales con acceso a la web

- Revisión de otras páginas o subespacios dentro de la misma web en búsqueda de posibles vulnerabilidades. Finalmente se cerró la web.

- Comprobaciones para detectar la posible indexación o difusión de los datos personales comprometidos.

  SICOMORO ha aportado búsquedas realizadas en Google con datos de posibles afectados concluyendo que el buscador no devuelve resultados con los datos asociados al evento.

- Comunicación de la incidencia a la empresa cliente.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- SICOMORO ha aportado copia del informe final elaborado por el Comité de Delegados de Protección de Datos de SICOMORO y HIBERUS TECONOLOGIAS DE LA INFORMACIÓN, S.L. sobre el incidente de seguridad del evento donde figuran las medidas de seguridad implantadas.

  En dicho informe figura que la Plataforma IACPOS tiene implantadas las medidas de seguridad previstas en la norma ISO 27001 y las estipuladas por el ANEXO II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

  SICOMORO ha aportado certificación ISO/IEC 27001 vigente hasta el 27/11/2020.

  SICOMORO ha aportado además, los siguientes documentos:

  - ISO 27001 Activos y Análisis de Riesgos 2018

  - ISO 27001 Descripción de Riesgos. Entre ellos se encuentra la descripción de la fuga de información por un ataque intencionado.

  - Análisis de Riesgos Reglamento de Protección de Datos (RGPD). Entre los riesgos evaluados se encuentra el de Acceso no autorizado a datos personales, valorado a 2018.

  SICOMORO manifiesta que con los análisis de riesgos tanto de la norma ISO como del RGPD no se consideró necesario realizar una Evaluación de Impacto a la vista de los riesgos.

- SICOMORO dispone de un procedimiento de notificación de brechas incluido en el procedimiento de Gestión de Incidencias.

- SICOMORO dispone de diversos documentos que se integran su la Política de Seguridad.

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

En el presente caso, de las actuaciones de investigación llevadas a cabo por esta Agencia, se desprende que si bien los datos de los clientes que asistieron a un determinado evento y que gestionaron su entrada a través de SICOMORO quedaron expuestos al público en general, no se ha acreditado que hayan sido objeto de tratamiento por terceros. Además, una vez conocida la incidencia de seguridad la entidad actuó de forma diligente e implantó los medios adecuados para minimizar el impacto y corregir la incidencia para evitar la repetición en el futuro, no sólo en el subdominio afectado sino en el resto de subdominios de la plataforma de gestión de entradas, tal y como arriba se indica.

Por último, señalar que, dado que los datos afectados correspondían al año 2017, se procedió a cerrar definitivamente el subdominio correspondiente, sin que consten en esta Agencia reclamaciones de los afectados.

III

Por lo tanto, se ha acreditado que la actuación del reclamado como entidad encargada del tratamiento de la gestión de entradas a un evento cuyo responsable es la entidad Aragón Desarrollo y Expansión, S.L., 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:

- ***SICOMORO SERVICIOS INTEGRALES, S.L. con NIF B99020547 con domicilio en Paseo Isabel La Católica 6, CP: 50009, ZARAGOZA.***

- ***ARAGÓN DESARROLLO Y EXPANSIÓN, S.L.*** con NIF ***B99231573,*** y con domicilio en ***C/ CÁDIZ 12, CP: 50004, ZARAGOZA.***

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