- **Procedimiento Nº: E/11934/2019**

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 de un escrito de notificación de brecha de seguridad de datos personales remitido por el Ayuntamiento de Madrid en el que informan a la Agencia Española de Protección de Datos (AEPD) de que, con fecha 8 y 9 de diciembre de 2019, se detectaron en las pantallas interactivas de los puntos de información de BiciMAD (Tótem) la presencia del texto ******TEXTO.1***

Una vez revisados los Tótem se constata la fuga de información. Aparentemente el hacker ha conseguido el acceso físico a la unidad central de procesamiento del Tótem (CPU) en local consiguiendo una vía remota de acceso a datos personales de DNI e identificativo de la tarjeta de usuario, lo que permite a su vez acceder posteriormente en remoto a datos de los usuarios de nombre y apellidos y saldo de su tarjeta BiciMAD.

En la notificación, el Ayuntamiento de Madrid indica que se va a comunicar a los afectados y remite escrito de la Dirección General de Sostenibilidad y Control Ambiental, de fecha 11 de diciembre de 2019, donde se informa que la "*Empresa Municipal de Transportes de Madrid (EMT) que, como concesionario del contrato integral de movilidad del Ayuntamiento de Madrid, presta el servicio público de bicicleta (BiciMAD), ha denunciado ante la Policía Nacional el posible ataque informático a seis estaciones de BiciMAD* (…) y *como consecuencia de dicho ataque, permanecieron temporalmente bloqueados sin servicio seis tótems de BiciMAD y quedaron expuestos sus números de DNI/Pasaporte e ID de usuario de BiciMAD, a través de los cuales se podría haber accedido también a los siguientes datos sobre su persona: nombre, apellidos y saldo.*

Con fecha 15 de diciembre de 2019 se recibe en esta AEPD escrito de reclamación interpuesto por uno de los afectados respecto de la brecha de seguridad mencionada manifiestando que no ha recibido comunicación de la incidencia.

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 lo siguiente:

ANTECEDENTES

Fecha de notificación de la brecha de seguridad de datos personales: 12 de diciembre de 2019

ENTIDADES INVESTIGADAS

- AYUNTAMIENTO DE MADRID, con NIF P2807900B y con domicilio en C/ Alcalá 45, 28014 Madrid.
- EMPRESA MUNICIPAL DE TRANSPORTES DE MADRID, S.A., con NIF A28046316 y con domicilio en C/ Cerro de la Plata 4, 28007 Madrid.
- BOOSTER BIKES, S.L., con NIF B86862166 y con domicilio en C/ Mauricio Legendre 40, 28046 Madrid.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 23 de diciembre de 2019 se remitió escrito de solicitud de información al Ayuntamiento de Madrid y de la respuesta recibida el 13 de enero de 2020 se desprende:

Respecto de la empresa. Contratos empresas encargadas del tratamiento

- BiciMAD es un medio de transporte público de la ciudad de Madrid, un servicio prestado al cien por cien con bicicletas eléctricas.
- Bonopark, S.L. cedió a la Empresa Municipal de Transportes de Madrid S.A. (en adelante EMT), con autorización del Ayuntamiento de Madrid, el contrato de prestación del servicio de BiciMAD (concesión administrativa).
- Para la prestación de este servicio, la EMT contrató los servicios de mantenimiento de la mercantil Booster Bikes, S.L. como adjudicataria del procedimiento "*Mantenimiento de la infraestructura de tecnología del sistema de bicicletas de la EMT de Madrid S.A*." (actualmente adquirida por AVANZA BIKE, S.L,).
- Funcionamiento de BiciMAD
- Cada estación de BiciMAD está compuesta de *tótem* y *bases*. El *tótem* es el punto de información que facilita la interacción del usuario mediante una pantalla táctil. Las *bases* de anclaje son los elementos donde se amarran las bicicletas y donde se produce la carga (eléctrica) de las mismas.
- La operativa entre un usuario y una estación viene descrita a continuación:

  o En función de cada usuario y del saldo disponible, se permite desanclar las bicicletas mediante la presentación de una tarjeta identificativa en el lector que se encuentra en la base de anclaje de la bicicleta.

  Se permite el anclaje de las bicicletas directamente en la base de la estación sin necesidad de realizar ninguna operación adicional por parte del usuario.

  o La interacción de las estaciones con los usuarios también se produce a través de la pantalla táctil en la cual los usuarios se identifican con la tarjeta de abonado de BiciMAD y pueden realizar las siguientes operaciones:

  ✓ Visualizar el mapa de estaciones y observar el nivel de ocupación. Visualizar el último trayecto realizado.

  ✓ Realizar recargas de saldo. Para ello, el usuario proporciona datos sobre el medio de pago que se remite al Sistema de Información Central. El sistema le devuelve el saldo.

- ✓ Darse de alta como usuario ocasional (turista). El usuario proporciona los datos de; nombre y apellidos, mail, teléfono, tipo de documento identificativo y número. Si se hace recarga también debe proporcionar los datos de medio de pago. Estos datos se remiten al Sistema de Información Central.
- ✓ Reportar Incidencias de la estación y/o bicicletas.
- ✓ Reservar estación.
- ✓ Recoger abono de usuario. El usuario se identifica con el DNI o documento acreditativo y una clave secreta.
- ✓ Conocer el saldo de un usuario. El sistema devuelve el saldo y el nombre y apellidos.
- ✓ Conocer el último trayecto de un usuario.

- Los Tótems se comunican con el Centro de Proceso de Datos a través de VPN identificándose mediante credenciales (certificados digitales).

Respecto de la cronología de los hechos. Medidas de minimización de la incidencia

El Ayuntamiento de Madrid ha aportado informe con fotografías sobre hechos ocurridos en los que se indica:

- A las 11:23 del día 09 de diciembre de 2019 se informa a través del grupo de incidencias de BiciMAD de Telegram de una supuesta incidencia de hackeo en tres estaciones, comprobándose que se había producido alteraciones desde el 7 de diciembre de 2019 a las 17:10 hasta el día 9.

En todas ellas aparecía la imagen fija o en formato *gif*: ******TEXTO.1***

Aparentemente, un hacker había entrado en los tótems en local y localizado en la máquina una vía de conexión remota a través de la cual se puede operar.

- A las 12:30 se realiza un seguimiento en las Redes Sociales y se comprueba que en los tótems hackeados no solo se ha introducido la modificación del salvapantallas de la estación, sino que además han podido interactuar con la estación expidiendo tarjetas, así como liberando bicicletas de las *bases* directamente a través del programa de la estación.
- A las 20:43 se detecta que el usuario <******USUARIO.1***> sube un video en Instagram en el que muestra como se ha conectado de forma remota a una de las estaciones e indica que ha descargado parte de la información de la misma, conteniendo el listado de DNIs de los usuarios BiciMAD, así como sus IDs de tarjetas asociados. En dicho video se indica "*Pues tenemos todos los usuarios de Bicimad"*
- A las 23:15 en el perfil de Instagram del usuario <******USUARIO.1***> se ha publicado un nuevo video *con* el siguiente mensaje ******MENSAJE.1***

Se pone en conocimiento de estos hechos a BOOSTER BIKES y concluyen que con la apertura física de las consolas de los *tótems* y ejecutando determinados comandos se permite el accesos remoto a los tótems hackeados..

- A las 23:36 empleados de BiciMAD se personan en las 3 estaciones que han sufrido ataque y a las 00:10, se observa a dos personas, coincidiendo una de

ellas con las imágenes vistas en redes sociales referentes al usuario <***USUARIO.1***>. Se comprueba que hay problemas en otra estación.

- El Ayuntamiento manifiesta que existen evidencias de la creación de un nuevo usuario BiciMAD, con un saldo de 1.337€, con fecha 10 de diciembre de 2019. (A las 22h del martes 10 de diciembre, <***USUARIO.1***> publica en Instagram que ha creado un nuevo usuario, con un saldo de 1.337€).
- El 11 de diciembre de 2019, BOOSTER BIKES sobre las 11:30h, corta el servidor imposibilitando cualquier acceso a los servicios centrales desde las estaciones incluido el equipo informático del hacker que simula ser una estación.

A partir de ese momento existe un impacto en el servicio BiciMAD que provoca que el servicio de uso de bicicletas siga operativo, pero en modo degradado con las siguientes restricciones:

- o No se pueden crear nuevas altas de usuarios,
- o No se pueden realizar recargas de saldo por parte de los usuarios
- o No se puede actualizar los saldos de los usuarios que hagan uso del servicio BiciMAD.

Al cortar el acceso a los servidores se anula cualquier potencial riesgo de acceso indebido y cesan todos los ciberataques.

- El mismo día se contacta con el Grupo de Ciberataques de Policía Nacional.
- El 12 de diciembre se notifica a la AEPD la brecha de seguridad sufrida y una fuga de datos personales (DNI y el ID de la tarjeta de usuario) a través de la cual se pueden recuperar datos de nombre, apellidos y saldo de los usuarios.
- El 13 de diciembre de 2019 el Ayuntamiento de Madrid y la EMT hacen público el ciberataque informático.
- El 20 de diciembre de 2019 se comienza a distribuir una versión software *resistente* en las estaciones que finaliza el día 27.
- El Ayuntamiento de Madrid contrata los servicios de ciberseguridad de la empresa OESÍA NETWORKS SL (en adelante OESÍA) para realizar un análisis forense de uno de los ordenadores hackeados. No obstante, detectan que continua el acceso indebido por lo que se realizan trabajos para mitigar las vulnerabilidades que han dado lugar a estos accesos.

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

- El Ayuntamiento ha aportado copia del informe emitido por OESIA en el que se concluye:
  - o Manipulando físicamente el *tótem* se logró acceso completo al sistema y al terminal del tótem.
  - o Tras acceder al sistema del *tótem* se pudo extraer archivos con datos y exteriorizar el terminal de la red local.
  - o Una vez fuera de la red local se produjo sobre ella accesos en remoto.

- Además, el atacante accedió a la clave privada del protocolo de acceso de comunicación entre el *tótem* y el Sistema Central.

- Una vez comprometido el sistema, el atacante accedió al portal que funciona en la red local de los *tótems* y se descargó varios ficheros.

- El Ayuntamiento manifiesta que una vez obtenidas y extraídas de una estación las credenciales (certificado digital) de comunicación del *tótem*, el hacker desde un equipo informático ajeno a la estación, se conecta con los métodos y servicios accesibles por las estaciones BiciMAD y puede solicitar datos personales que figuran en el Sistema Central (nombre y apellidos, saldo).

Otras medidas de minimización de la incidencia y acciones tomadas para la resolución final. Medias implementadas con posterioridad a la incidencia

- Desde el 27 de diciembre de 2019, la versión software resistente está distribuida en todas las estaciones y se han cambiado las credenciales de acceso a la VPN.

- Se ha realizado una planificación para proteger físicamente las estaciones y el cambio de tecnología de comunicaciones de las estaciones.

- Se ha modificado la tecnología de acceso a la VPN que impide el acceso a los servidores a direcciones IP no autorizadas.

- EMT quita físicamente el cable entre el router y el ordenador de las estaciones. De este modo resulta imposible acceder a los datos de las estaciones.

- Se ha deshabilitado la WiFi

- Se realiza un análisis de vulnerabilidades en el ordenador de la estación para construir una nueva imagen para las estaciones que se distribuirá a todas ellas con nuevas credenciales,

- Se hace un escaneo de vulnerabilidades de la nueva versión software del ordenador de la estación para ratificar que todos los riesgos informáticos han sido corregidos.

Respecto de los datos afectados. Notificación e indexación

- Finalmente se produjo un ciberataque a 13 estaciones,

- Aproximadamente los datos de unos 63.000 usuarios activos fueron susceptibles de ser accedidos.

- Los datos de carácter personal son DNI, nombre y apellidos viéndose comprometidos tanto los datos existentes en los *tótems* como los datos que el sistema central devuelve a los *tótems* ante una petición.

- El Ayuntamiento de Madrid manifiesta que no les consta tratamiento posterior por terceros de los datos personales obtenidos a través de la brecha de seguridad de datos personales.

- El Ayuntamiento de Madrid manifiesta que no les consta indexación por los buscadores de los datos personales obtenidos a causa de la brecha.

- El ataque informático a estaciones de BiciMAD ha estado publicado en la web de EMT en la dirección : ******URL.1*** entre el 13 y el 26 de diciembre, ambos

inclusive y en la web de BiciMAD se ha publicado un banner que enlazaba al comunicado alojado en la web de la EMT.

En el comunicado se informa de la denuncia interpuesta ante la Policía Nacional sobre un ataque informático a 13 estaciones de BiciMAD y de las consecuencias, al resultar comprometidos los datos del identificador de la tarjeta de los usuarios de BiciMAD. Con estos datos, podrían haber tenido acceso también a nombre, apellido e información del saldo disponible en la tarjeta de usuario. En ningún caso, se ha producido acceso a las transacciones bancarias realizadas por los usuarios.

Asimismo, informan de que se han puesto en marcha nuevas medidas de seguridad que afectarán a la interacción de los usuarios con BiciMAD hasta que finalice este proceso, que durará aproximadamente una semana. Durante este periodo los usuarios podrán seguir utilizando el sistema de BiciMAD pero no se realizarán actualizaciones de saldo.

Una vez terminado el proceso de securización del sistema, el saldo de los usuarios se regularizará. Durante este periodo, no se podrán realizar recargas ni nuevas altas; del mismo modo, los usuarios no podrán realizar gestiones en el sistema a través de los *tótems.*

EMT informa también de que mientras dure esta situación, la información de disponibilidad de bicicletas y anclajes mostrada en la App y en la Web no es exacta.

A medida que se produzcan novedades sobre este proceso, EMT actualizará puntualmente la información relativa a la resolución de la incidencia a través de sus diferentes canales de comunicación."

Este comunicado se ha publicado también en la web del Ayuntamiento de Madrid:

******URL.2***

El mismo día de publicación de la noticia en la web (13 de diciembre) se publicó en redes sociales, en el perfil de BiciMAD Facebook:

******URL.3*** y de Twitter ******URL.4***, y se compartió en la cuenta de EMT.

Cuando volvió a estar operativa la opción de recarga de saldo se publicó otro mensaje informativo en las cuentas de BiciMAD:

******URL.5***. Este mensaje se retuiteó en el perfil de la EMT.

- En relación con las publicaciones mencionadas, desde la Inspección de Datos, con fecha 19 de maro de 2020, se ha accedido a las citadas direcciones verificando que figuran los comunicados en las redes sociales y en la web del Ayuntamiento de Madrid.

- El Ayuntamiento de Madrid manifiesta que respecto a los comentarios que han recibido en redes sociales han publicado la siguiente respuesta : "*Hemos puesto en marcha la securización del sistema y la funcionabilidad de los tótems se encuentra limitada hasta su finalización. Las estaciones están operativas para anclar y desanclar bicis, siempre que se tenga saldo positivo. Sentimos las molestias*."

- En relación con la obligación de notificación a los afectados, el Ayuntamiento de Madrid manifiesta que se ha seguido el procedimiento que se

recoge en la "*Guía para la gestión y notificación de brechas de seguridad*" publicada por la AEPD, habiéndose concluido que no sería aplicable dicha obligación al presente caso valorando el volumen de afectados, la tipología de los datos y el impacto, entre otros.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- EMT inició en enero de 2019 un análisis de la situación actual de la organización con el fin de diseñar un plan de adecuación tanto al Esquema Nacional de Seguridad como a la legislación vigente en materia de protección de datos. De dicho análisis se desprendió un Plan de Acción para corregir las carencias identificadas, el cual está actualmente en implantación.
- Actualmente EMT tiene aprobada una Política de Seguridad de la Información y cuenta con un cuerpo Normativo aún en desarrollo e implantación. EMT asumió la gestión del servicio de BICIMAD en octubre de 2016, en aquel momento EMT no contaba con política de seguridad ni normativa asociada en la que se definieran las medidas de seguridad a implantar en los sistemas de información.
- La EMT no tiene constancia de la existencia de un Análisis de Riesgos ni de una Evaluación de Impacto realizada previamente a la fecha en la que asumió la gestión del servicio de BICIMAD. No obstante EMT realizó una auditoría de Seguridad de la aplicación móvil de usuarios, así como de los servicios Web sobre los que se soporta el servicio. En ambos análisis se encontraron vulnerabilidades que implicaban riesgos de seguridad de nivel bajo y medio, que se corrigieron
- El Ayuntamiento de Madrid ha aportado los siguientes documentos:

o Normas de Gestión de Incidentes de Seguridad.

o Política de Seguridad de la Información

o Registro de Actividad de los tratamientos de usuarios de BiciMAD y de reclamaciones e incidencias de BiciMAD.

o Manual de Usuarios (Interfaz usuarios Tótem).

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 brecha 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 brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad y disponibilidad, a través del acceso indebido al sistema de información BiciMAD.

No obstante, también consta que el Ayuntamiento de Madrid y EMT, en colaboración con Booster Bikes, S.L., disponían de medidas técnicas y organizativas razonables y proporcionadas para afrontar un incidente como el ahora analizado, 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 y minimizar el impacto e implementar las medias oportunas para evitar que se repita en el futuro a través de la puesta en marcha de un plan de actuación definido por las figuras implicadas del responsable del tratamiento.

Asimismo, consta que la EMT comunicó a los interesados a través de comunicaciones públicas conforme dispone el art 34.3.c) del RGPD que señala *"3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes: (…)*
c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados."

También debe valorarse la adopción de medidas técnicas y de gestión, como es la contratación de una auditoria de seguridad y forense a todos los sistemas de información del servicio BiciMAD, al objeto de comprobar y en su caso mejorar la calidad de las aplicaciones de gestión de datos personales.

El informe final tras el seguimiento y cierre sobre la brecha y su impacto es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos futuros. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

III

Por lo tanto, se ha acreditado que la actuación del Ayuntamiento de Madrid como entidad responsable del tratamiento de los datos personales del servicio BiciMAD, ha sido proporcional y 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 AYUNTAMIENTO DE MADRID con NIF P2807900B, y con domicilio en calle Alcalá 45, 28014 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