Procedimiento Nº: E/05726/2019
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 quiebra de seguridad remitido por ISTA METRING SERVICES ESPAÑA S.A (en adelante ISTA) en el que informan a la Agencia Española de Protección de Datos que han tenido conocimiento, a través de un correo electrónico de un cliente de fecha 12 de Marzo de 2019, de una incidencia en la seguridad de la aplicación web GesCon, propiedad de ISTA, en relación a la visualización y acceso a datos de recibos de abonados.

Se procede por parte de ISTA a abrir una incidencia en la aplicación de Gestión de Incidencias Mantis, y se comunica la misma a las áreas de sistemas de información y otras áreas/departamentos de ISTA para su análisis y verificación.

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:

ANTECEDENTES

Fecha de notificación de quiebra: 15 de marzo de 2019

ENTIDADES INVESTIGADAS

ISTA METERING SERVICES ESPAÑA S.A., con C.I.F. núm. A50090133 y con domicilio en Madrid, en la Avenida de la Albufera num.319, 4ª Planta (28031 Madrid)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 30 de julio de 2019 se requiere información a ISTA y de la respuesta recibida con fecha 9 de agosto de 2019 se desprende:
    - GesCon es una aplicación para realizar el servicio a los clientes (Comunidades de Propietarios) de mantenimiento, lectura y recibos de los contadores de medición de consumos de agua y calefacción.

      Con el fin de poder prestar los servicios anteriormente descritos, es necesario mantener una base de datos con la información de dichos clientes (Comunidades de Propietarios y de los propietarios de las viviendas que las componen), así como su historial de lecturas y recibos.

- Una de las partes del aplicativo es facilitar el acceso a sus datos por los clientes.
- Para el acceso a la plataforma GesCon, el cliente /abonado debe encontrarse registrado, y acceder a GesCon a través de la introducción de sus identificadores personales.
- La aplicación GesCon dispone de un servicio de identificación y autenticación, y solo podrán acceder a la plataforma después de que los accesos sean autorizados con un token de autenticación de destino.

Respecto de la cronología de los hechos

- El 12 de Marzo de 2019 a las 20:45 horas se recibe por parte de los servicios informáticos de ISTA una incidencia en la seguridad de la aplicación web GesCon, propiedad de ISTA, en relación a la visualización y acceso a datos de recibos de abonados.
- Se procede por parte de ISTA a abrir una incidencia en la aplicación de Gestión de Incidencias Mantis, y se comunica la misma a las áreas de sistemas de información y otras áreas/departamentos de ISTA para su análisis y verificación.
- Recibida la incidencia, por parte de los servicios informáticos de ISTA se realiza una simulación del proceso, verificándose que tal y como traslada el usuario que detectó la incidencia, se puede acceder por parte de un abonado registrado al acceso a los datos de recibos de otros usuarios de la aplicación con la modificación del enlace de descarga de recibos.
- Se verifica que en los accesos a la aplicación GesCon, una vez logado el usuario y autentificada su identidad a través de la comprobación de nombre de usuario y contraseña de acceso, el “id” que se está enviando por la URL (ya sea el idRecibo, idFinca, idAbonado), para ser utilizado por el backend se hace a través de un “método GET” donde en la URL se exponen todos los valores que necesita (originando la brecha de seguridad).

  Así, el método GET lo que hace es pasar las variables y sus valores por la URL, es decir, no solo queda a la vista de cualquier usuario, sino que además la información puede quedar guardada en el historial del navegador, provocando ese fallo de seguridad.

Respecto de la categoría de los datos afectados

- La base de datos de clientes cuenta con unos 33894 registros de abonados.
- De la documentación aportada se desprende que el usuario que notifico la incidencia a ISTA METERING SERVICES realizó 74 accesos a la plataforma; dicho usuario no ha podido modificar información de los otros usuarios, pero procedió a la descarga e impresión de 6 recibos de distintos clientes.
- Los datos a los que se ha tenido acceso son: Identificativos, económicos, financieros y de consumo.

Respecto de las acciones tomadas para minimizar la incidencia

- La medida inicial adoptada el 13 de marzo de 2019 por los Departamentos de sistemas de ISTA METERING SERVICES ESPAÑA, a las 10:00 fue el cierre temporal de la plataforma GesCon y desactivación del sistema de identificación y autenticación, evitando así cualquier nuevo acceso por parte de usuarios a la aplicación GesCon vía web.
- Posteriormente, conforme a los procedimientos internos de gestión de incidencias, se procedió a la búsqueda de soluciones técnicas, así como priorizar el desarrollo de la solución técnica necesaria dentro del equipo de desarrolladores de GesCon del Departamento de IT de ISTA METERING SERVICES ESPAÑA.

Respecto a la utilización por terceros de los datos personales obtenidos a través de la brecha

- En relación a esta cuestión, desde ISTA METERING SERVICES ESPAÑA no se ha tenido conocimiento de la utilización de los datos por parte de la persona que puso en conocimiento la brecha de seguridad, ni que los datos personales a los que pudo acceder el usuario que puso en conocimiento dicha brecha hayan sido utilizados o indexados por motores de búsqueda en Internet.

Respecto de la resolución final de la incidencia

- Para evitar este problema se ha realizado una “codificación” de la URL (ya sea el idRecibo, idFinca, idAbonado), para luego decodificarlo en el método que recupera dicho id, el pasado 13 de Marzo de 2019. De esta forma en la URL no mostrará un identificador como tal.
- La solución inicial adoptada ha procedido a implementar una nueva funcionalidad de seguridad que elimina la manera en cómo la aplicación llama al “backend”.
- Los valores del idRecibo son codificados bajo la “codificación Base 64 modificado” no permitiendo que en la URL de la web se muestre el valor del id de los recibos.
- Estos mismos cambios fueron aplicados para otros “ids” expuestos en la web de abonados, como lo pueden ser el idAbonado y el idFinca. Ambos “ids” fueron codificados para que su información no pueda ser alterada por el usuario. Esta implementación fue pasada al entorno de producción el día 13 de marzo de 2019 a las 14:38 horas.

  Todo esto con el objetivo de que cualquier id que se muestre en la URL de la web de abonados esté debidamente codificada.
- Estos cambios fueron pasados al entorno de producción el día 21 de marzo de 2019 a las 10:30 horas.

Respecto de la notificación realizada a los clientes afectados:

- Se procedió por parte de ISTA METERING SERVICES ESPAÑA S.A. ha realizar un análisis de la información y datos que podían ser visualizados por el usuario que detectó y notificó la vulnerabilidad de seguridad de la aplicación web GESCON, y atendiendo a los criterios descritos por el artículo 34 del Reglamento UE 679/2016 General de Protección de Datos y al Considerando

75 de dicho Reglamento, así como a lo especificado dentro del Documento WP250 Rev01 del Grupo de Trabajo sobre Protección de Datos del Artículo 29 relativo a las “Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento”, se verificó que el acceso por el usuario que detectó la vulnerabilidad de la aplicación no afectaba a los derechos y libertades de las personas físicas, ni entrañaba riesgos de gravedad y probabilidad variables, que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, y en particular, problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación.

- Se procedió por parte de ISTA METERING SERVICES ESPAÑA S.A., el pasado 13 de marzo de 2019, a contestar al Usuario que comunicó la brecha de seguridad indicándole las medidas iniciales que se habían adoptado las medidas iniciales de encriptación de la URL, así como la posibilidad de contar con su colaboración para la mejora de la aplicación.

Respecto de la seguridad:

- Se ha llevado a cabo un proyecto de adecuación al Reglamento Europeo de Protección de Datos de forma integral por parte de ISTA Deutschland GmbH consistente en la realización de un Análisis Gap, para evaluar el nivel de cumplimiento de las nuevas obligaciones que establece la nueva norma.

  Como consecuencia de este proyecto, se han elaborado nuevos protocolos internos para la atención al ejercicio de derechos, la comunicación de brechas de seguridad, se han actualizado los contratos de encargado de tratamiento con prestadores de servicio que pueden tener acceso a los datos, se han adaptado textos y formularios a las nuevas exigencias de información

- Aportan copia del Registro de Actividad de los tratamientos donde se ha producido la incidencia.

- Aportan documentos de evaluación de Impacto y análisis de riesgos realizados sobre los tratamientos de datos que fueron objeto del incidente de seguridad realizados y aprobados por el Delegado de Protección de Datos de ISTA Deutschland GmbH, empresa matriz a la que pertenece ISTA METERING SERVICES ESPAÑA S.A.

- Aportan documento de evaluación de Impacto de la Privacidad elaborado con posterioridad a la corrección de la incidencia por parte del auditor externo que da soporte jurídico a ISTA METERING SERVICES ESPAÑA S.A. en materia de protección de datos de carácter personal.

- Aportan copia del Procedimiento de Gestión de Brechas de Seguridad adoptado por ISTA METERING SERVICES ESPAÑA S.A.

- Se procede a incorporar en el cuerpo normativo de políticas de seguridad establecidas por ISTA METERING SERVICES ESPAÑA S.A. basadas en la norma ISO 27001:2013 de Sistemas de Seguridad de la Información.

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, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha confidencialidad por el acceso, a través de la aplicación de gestión de clientes propiedad de ISTA, a datos de terceros ajenos.

No obstante, también consta que ISTA, a través del servicio de Informática, disponía de medidas técnicas y organizativas para afrontar un incidente como el ahora analizado, lo que ha permitido tras una reclamación de un ciudadano la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante el mismo al objeto de notificar y minimizar el impacto e implementar las medias razonables oportunas para evitar que se repita en el futuro a través de la puesta en marcha de un plan de actuación previamente definido por las figuras implicadas del responsable del tratamiento.

También debe valorase la adopción de medidas técnicas y de gestión, como es la contratación de una auditoria a todos los sistemas de información similares, al objeto de comprobar y en su caso mejorar la calidad de las aplicaciones de gestión de datos personales, así como la elaboración de un nuevo análisis de riesgos y evaluación de impacto tras la subsanación de la incidencia.

La elaboración del 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 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 ***ISTA METERING SERVICES ESPAÑA S.A.,*** con ***C.I.F. núm. A50090133*** y con domicilio ***en Madrid, en la Avenida de la Albufera num.319, 4ª Planta (28031 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