- **Procedimiento Nº: E/07375/2020**

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 División de Innovación Tecnológica de la Agencia Española de Protección de Datos (en adelante, AEPD) de una brecha de seguridad de datos personales por parte del responsable del tratamiento CASA GRANDE ARIZÓN, S.A.U., con número de registro de entrada ******REGISTRO.1***, relativa al cifrado ilegítimo de un servidor, la Directora de la AEPD ordenó, el 08/09/2020, a la 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, teniendo conocimiento de los siguientes extremos:

Resumen de la notificación:
indisponibilidad del tratamiento legítimo de datos personales debida al acceso no autorizado por un tercero a los mismos, en el que se reclama un pago para la recuperación de dichos datos.

Documentación aportada:
- Copia de la denuncia de los hechos acontecidos en la brecha de seguridad ante la *Policía Nacional en fecha* ******FECHA.1,*** en la Dependencia de ******LOCALIDAD.1*** bajo el número de Atestado ******ATESTADO.1***.

ENTIDADES INVESTIGADAS
Durante las presentes actuaciones se ha investigado la siguiente entidad:
CASA GRANDE ARIZÓN, S.A.U. (en adelante, la investigada), con CIF A79330106 y domicilio en C/ ******DIRECCIÓN.1***.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN
Respecto de la cronología de los hechos:

- La investigada manifiesta no haber recibido novedades de la investigación por parte de la Policía Nacional a fecha 03/12/2020.

- La investigada expresa que el día 31/08/2020 a las 8:00 horas para comenzar la jornada laboral no funcionaban los programas informáticos ni se podían abrir los documentos existentes en uno de sus ordenadores.

- La investigada solicitó a su personal de informática la revisión de la situación pensando que se trataría de una cuestión de otro tipo, pero dicho personal esclareció que se había producido un ataque externo.

- La investigada informa que desde el primer instante el hacker les contactó para recibir bitcoin a cambio de recuperar los datos sustraídos. La investigada manifiesta que la Policía Nacional le aconsejó no contestar al hacker puesto que no era fiable que, una vez abonada la cantidad solicitada, la información les fuese devuelta.

- La investigada señala que se mantuvieron durante una semana sin poder trabajar con normalidad ante la falta de información, la carencia de sistema de gestión informático y resto de elementos informáticos con los que poder desempeñar el trabajo con el ordenador.

- La investigada se identifica como entidad gestora de un hotel y alega el perjuicio que le supuso mantener sus instalaciones abiertas, con la llegada de clientes y sin poder emitir facturas hasta restablecer el sistema, limpiar el servidor e instalar de nuevo las cuestiones necesarias, y reingresar los datos disponibles en el programa de reservas del hotel.

- La investigada expresa que también recuperó información de la que disponía en copias de seguridad del servidor, de tal modo que considera haber recuperado cierta normalidad el día 08/09/2020. Si bien es cierto, la investigada sostiene que ese día se considera como un inicio en sus sistemas, puesto que toda la información anterior a ese día de los registros de clientes fue perdida.

- La investigada expresa que la aparición de la entidad ESTUDIOS SANTA ANA, S.L. (con CIF B11707726) en la notificación de la brecha de seguridad a la AEPD responde a que el certificado digital de su entidad se encontraba caducado y no había sido posible renovarlo por motivo de las restricciones asociadas a la pandemia de COVID-19.

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

- La investigada expresa no conocer con exactitud cómo se logró el acceso a su sistema con las protecciones existentes.

- La investigada informa de que el ataque se realizó mediante ***el*** ataque de malware ***"***MALWARE.1"***.

<u>Respecto de los datos afectados:</u>

- La investigada señala que los datos implicados en la presenta brecha de seguridad se corresponden con:

    - Datos para el trabajo diario, entre otros:

- Plantillas de turnos.
- Horarios.
- Incidencias del día.
- Fotografías del hotel.

o Datos de los clientes y de sus reservas [el ataque también afectó al programa de gestión hotelera utilizado de ***XXXXXXXX XXXX (***con CIF ***XXXXXXXX***], tales que permitan elaborar una factura:

- Nombre completo o denominación social.
- DNI o NIF.
- Dirección completa o domicilio social.
- Otros datos que figuren en el DNI.
- Teléfono.
- Correo electrónico.

- La investigada señala no poder especificar las nacionalidades de las personas afectadas puesto que dicha información no ha sido recuperada y no disponen de dichos registros.
- La investigada expresa no tener constancia de afectado alguno por la presente brecha de seguridad.
- La investigada señala no tener indicios que indiquen la publicación de datos personales a causa de la brecha de seguridad en Internet.

<u>Acciones tomadas con objeto de minimizar los efectos adversos y medidas correctivas adoptadas para su resolución final:</u>

- La investigada manifiesta que en el momento en que conoció el incidente procedió a ***XXXXXXXXXX*** y comenzó a trabajar en intentar desencriptar los archivos. La investigada expresa que pudo recuperar ciertos datos de ***XXXXXXXXX***, pero otros, como los del programa de gestión hotelera, que guardaba en ***XXXXXXXXXX***, no fue posible de recuperar. La investigada aporta copia de factura con fecha 07/09/2020 emitida por parte de la entidad anteriormente citada ***XXXXXXXX XXXXX*** para reinstalación en el servidor del programa de gestión hotelera utilizado.
- La investigada informa de haber mantenido conversaciones telefónicas y presenciales con personal informático para subsanar el incidente.

- La investigada expresa no haber procedido a la comunicación a los afectados por el incidente puesto que con la brecha de seguridad se perdieron sus datos y la forma de subsanación de la brecha de seguridad consistió en una nueva instalación del sistema al completo sin datos de partida.

Respecto de las medidas de seguridad implantadas con anterioridad a la brecha de seguridad:

- La investigada manifiesta disponer de ***XXXXXXXXXXXXXXXXXXXXXXX.***
- La investigada expresa que para los clientes ***XXXXXXXXXXXXXXXXXXXX.***
- La investigada identifica a la entidad ***XXXXXXX (con CIF XXXXXXX***) como aquella que le realiza las copias de seguridad y a ***XXXXXXX (***a efectos legales mercantiles, ***Doña A.A.A. con DNI ***NIF.1)*** como su responsable de informática.
- No consta ***XXXXXXXXXXXXXXXXXXXXXXXXXX*** por parte de la investigada.

Respecto de las medidas de seguridad de tipo preventivo frente a la posible repetición en el futuro de la brecha de seguridad:

- La investigada expresa haber reforzado los sistemas de seguridad de la entidad ***XXXXXXXXXXXXXXXXXXXXXXX***. La investigada aporta copia de factura con fecha 25/09/2020 emitida por parte de la anteriormente citada ***XXXXXX*** referidas a medidas informáticas tomadas posteriormente a la brecha de seguridad.
- La investigada aporta un informe técnico emitido por ***XXXXXX*** a fecha 31/08/2020 en que se presentan las soluciones tomadas para resolver el incidente y las medidas establecidas para evitar su recurrencia en el futuro.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo:

- La investigada manifiesta que no había recibido un ataque igual anteriormente, por lo que lo reseña como el único hasta su ocurrencia.

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.

Artículo 32

"Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a)la seudonimización y el cifrado de datos personales;

b)la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c)la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d)un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

Artículo 33

"Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a)describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b)comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c)describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d)describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo".

Artículo 34:

"Comunicación de una violación de la seguridad de los datos personales al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida. L 119/52 ES Diario Oficial de la Unión Europea 4.5.2016

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes: a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1; 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.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad, al haber tenido acceso a datos personales personas no autorizadas, y de disponibilidad, puesto que los datos fueron encriptados o borrados, de manera que la investigada no pudo acceder a los mismos, habiendo perdido toda la información. Es por ese mismo

motivo por el que no pudo cumplir con lo establecido en el artículo 34 del RGPD en lo que a la comunicación a los interesados se refiere.

Si bien las medidas de seguridad y organizativas preventivas adoptadas con anterioridad al incidente podrían haber sido más completas y eficaces, cabe destacar la rápida actuación de la investigada, desde el mismo momento en que tuvo conocimiento de los hechos, interviniendo de forma activa en su resolución, ***XXXXXXXXXXXXX-XX.***

Tras el requerimiento de información llevado a cabo por la Inspección de esta AEPD, la investigada ha informado de todas las actuaciones llevadas a cabo para paliar el incidente, y de las nuevas medidas implementadas para prevenir posibles ataques futuros.

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

III

Por lo tanto, se ha acreditado que la actuación de la investigada 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 CASA GRANDE ARIZÓN, S.A.U. con CIF A79330106 y domicilio en C/ ******DIRECCIÓN.1***.

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