Procedimiento Nº: E/09388/2019

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: Con fecha de 20/12/2018, la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación en relación con la notificación de una brecha de seguridad relativa al robo de un ordenador desde el que se almacenaba en servicios *cloud* datos de menores de un centro de educación.

El 14/12/2018 fue notificada la brecha de seguridad por RAPINFORMES ON LINE, S.L. (en lo sucesivo RAPINFORMES), que contiene, entre otra, la siguiente información:

- Fecha de detección de la brecha: 12/12/2018
- Fecha de inicio de la brecha: 12/12/2018
- Brecha resuelta a 13/12/2018.
- Responsable del tratamiento: Incluido en el apartado de Entidades Investigadas.
- Resumen de la brecha: Consistió en el robo de un ordenador portátil en el domicilio de una docente del centro educativo CAUDE (El CATON, SCM). A través del portátil se podía acceder a Dropbox, correo electrónico y Google drive del centro. Una vez se dio cuenta del robo, procedió a la actualización de las contraseñas para evitar cualquier acceso no autorizado.
- Que antes de la brecha se aplicaron las siguientes medidas preventivas:

Usuario y contraseña para acceder a Google drive, Dropbox y correo electrónico, así como para acceder al propio ordenador.

- Que las categorías de datos afectados son:

Datos básicos.
DNI, NIE y/o pasaporte.
Datos de contacto.
Datos de salud.

- Que el perfil de los sujetos afectados son estudiantes y menores afectando a un número aproximado de 50 personas.
- Que cataloga la severidad de las consecuencias como “Baja”.
- Que las medidas tomadas para solucionar la brecha y minimizar el impacto fue denunciar los hechos ante la policía y actualizar usuario y contraseña.
- Que está pendiente de decidir si comunicar la brecha a los interesados.

En fecha 11/03/2019, D. ***A.A.A.*** (en lo sucesivo JRPC), de la entidad remite a esta Agencia la siguiente información:

1. Indica las medidas tomadas para asegurar la confidencialidad e integridad de los datos manejados y de la documentación facilitada.

Aporta documento con una enumeración de las medidas adoptadas, entre otras:

a. Nombramiento de RAPINFORMES como Delegado de Protección de Datos del centro.
b. Análisis de riesgos y, en su caso, evaluación de impacto.
c. Generación de documento de seguridad.
d. Recomendaciones informáticas personalizadas para una mejor adaptación tecnológica al RGPD y LOPDGDD como cambio de contraseñas, antivirus, necesidad de procedimientos de anonimización, etc.
e. Manifiesta que los empleados están formados e informados de todos sus derechos y obligaciones en materia de protección de datos.

2. Aporta copia de la denuncia policial de fecha 14 de diciembre de 2018, donde se manifiesta:

a. Que el robo del ordenador portátil tuvo lugar el día 12 de diciembre de 2018 en el domicilio de la docente del colegio CAUDE de la localidad de Majadahonda (Madrid).
b. Que dicho ordenador portátil poseía datos sensibles sobre los estudiantes de dicho centro educativo.

3. Manifiesta que:
a. Que el número estimado de afectados menores de edad es de 90.
b. Que entre los datos se encontraban nombres y apellidos de los menores y sus tutores legales, datos de salud (alergias, intolerancias, enfermedades sufridas por el menor), notas de clase, ausencias.
c. Que para la resolución de la incidencia tomaron la medida del cambio de usuario y contraseña para acceder a Google drive, Dropbox y correo electrónico del centro.
d. Que no tienen constancia de la utilización por terceros de los datos obtenidos por el robo.
e. Que no se notificó la incidencia a los afectados porque tomaron medidas ulteriores que garantizan que ya no existiera probabilidad de que se concretase alto riesgo para los derechos y libertades del interesado, basándose en el art 34.3 apartado b del RGPD.

Con fecha 15/04/2019, RAPINFORMES remite a esta Agencia la siguiente información:

1. Que el procedimiento para facilitar a los empleados las normas de seguridad a aplicar a los tratamientos de datos consistió en una formación presencial. Los empleados firmaron unas hojas comprometiéndose a cumplir con la normativa.

Aporta programa de la formación que consiste exclusivamente en una enumeración de epígrafes que incluyen entre otros:

• Política de Seguridad:
Acuerdo de confidencialidad y secreto profesional.
Política de seguridad del personal.
Medidas adicionales de seguridad.
Violaciones de seguridad:
Gestión de una violación de seguridad.
Casuística de violaciones de seguridad.

2. Aporta informe con las medidas de seguridad implantadas en la fecha en que tuvo lugar la brecha. Entre otras medidas, se relacionan:

a. El responsable y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos.
b. El trabajador está obligado a mantener el deber de confidencialidad durante y una vez finalizada la relación con la empresa y en prueba de ello firmará un documento.
c. Actividades permitidas y/o prohibidas en relación a:
La utilización de sistemas informáticos.
La protección de contraseñas personales.
El acceso a redes.
Queda expresamente prohibido almacenar datos de carácter personal en el disco duro del ordenador
Utilización del correo electrónico.
Uso de internet.
Dispositivos móviles y tablets.

3. Aporta documento de análisis de riesgos.

4. Manifiesta que no se ha determinado la necesidad de realizar evaluación de impacto al no existir alto riesgo para los derechos y libertades de las personas físicas según lo establecido en el art. 35 RGPD.

El 26/07/2019 se comprueba en el Registro Mercantil Central que JRPD es administrador único de RAPINFORMES.

El 05/08/2019, JRPC remite a esta Agencia información y manifiesta:

1. Que el Manual del Trabajador adjunto acredita la entrega de información a los trabajadores haciendo explícitas las normas que aplican a los ordenadores que se les proporciona.

Aporta documento con el Manual del Trabajador.

2. Que los datos no estaban almacenados en el disco duro de la afectada, sino en la plataforma informática ******PLATAFORMA.1*** a la que solo se tiene acceso por usuario y contraseña y que se procedió a cambiar después del robo.

3. Que en dicha plataforma ******PLATAFORMA.1*** se encontraban los datos relativos a la salud de los menores y datos personales no sensibles de menores y de sus padres/tutores legales.

4. Que el Delegado de Protección de Datos es RAPINFORMES.

Aporta copia de autorización dada a RAPINFORMES por parte del colegio CAUDE (El CATON, SCM), para la realización de los trámites necesarios ante esta Agencia que permitan su inscripción como Delegado de Protección de Datos.

Aporta justificante de comunicación de Delegado de Protección de Datos a esta Agencia en fecha 30/01/2019.

FUNDAMENTOS DE DERECHO

I

En virtud de 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 las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales en el sentido señalado en el artículo 32 del RGPD debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación

de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

También 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.

En concreto el artículo 32 del RGPD *"Seguridad del tratamiento",* establece que:

"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".

En el artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control, determinando lo siguiente:

"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."

Y el artículo 34 del Reglamento mencionado indica cuando es necesario informar de una violación de la seguridad de los datos personales al interesado, señalando lo siguiente:

"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.

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 este mismo sentido se señala en los Considerandos 85 y 86 del RGPD:

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72

horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

III

En el caso examinado, el 12/12/2018 se detectó una brecha de seguridad, siendo solucionada al día siguiente y comunicando el 14/12/2018 a la AEPD la incidencia producida, así como las medidas adoptadas.

De la documentación aportada y de la recabada por los servicios de inspección de este centro directivo se desprenden indicios evidentes que la brecha de seguridad vulneró el artículo 32 del RGPD, *Seguridad del tratamiento*, relacionada con el posible acceso a los datos como consecuencia del robo de un ordenador portátil en el domicilio de una docente del centro educativo y desde donde se tenía acceso a Dropbox, es decir, la herramienta que permite tener copia de archivos en «la nube», así como al correo electrónico y Google drive del centro educativo; si bien se comprobó que los datos no se encontraban almacenados en el ordenador sino en la plataforma a la que se accedía desde el dispositivo mediante usuario y contraseña.

No obstante, una vez que se tuvo conocimiento del robo del ordenador se procedió con inmediatez a adoptar medidas para minimizar su impacto y asegurar la integridad de la información y documentación existente en los sistemas, su alcance, medidas, etc. Inmediatamente se actualizaron las contraseñas y usuarios para evitar cualquier acceso no autorizado, no teniéndose constancia de la utilización de los datos por terceros. Se aporta igualmente copia de la denuncia policial efectuada.

Por otra parte, si bien es cierto que con anterioridad a la brecha el centro tenía implantadas medidas suficientes para evitar accesos no autorizados ni deseados, tras la incidencia provocada de adoptaron medidas para garantizar que no pudiera existir la mínima probabilidad de que se llevaran a cabo acceso a los datos personales, aun teniendo la constancia de que en la presente quiebra no se ha producido la utilización de los mismos por terceros.

De igual forma, se aporta información sobre la batería de medidas puestas en marcha como la formación de los empleados en materia de protección de datos y los procedimientos a aplicar en los tratamientos detallando aquellas actividades permitidas

y prohibidas, manual con las normas que han de aplicar en los ordenadores; informe sobre las medidas de seguridad implantadas; análisis de riesgos; etc.

IV

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:

1. **PROCEDER al ARCHIVO** de las presentes actuaciones.

2. NOTIFICAR la presente resolución a **RAPINFORMES ON LINE, S.L.,** con NIF ***B83566398.***

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