- **Expediente N.º: EXP202100390**

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: La Agencia Española de Protección de Datos ha tenido conocimiento a través de las noticias aparecidas en diversos medios de comunicación sobre una brecha de seguridad de datos personales sufrida por el Ministerio de Trabajo y Economía Social relativa a un ataque ransomware que ha podido provocar una brecha de disponibilidad, vulnerándose la legislación en materia de protección de datos.

Con fecha 15 de julio de 2021, la Directora de la AEPD instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) para investigar a Ministerio de Trabajo y Economía Social con NIF ******NIF.1*** (en adelante, MITES) en relación con los siguientes hechos:

Las noticias aparecidas en diversos medios de comunicación sobre una brecha de seguridad de datos personales sufrida por el MITES relativa a un ataque ransomware que ha podido provocar una brecha de disponibilidad, vulnerándose la normativa de protección de datos.

- El 9 de junio de 2021, el Ministerio de Trabajo y Economía Social publicaba en su cuenta de Twitter el siguiente tweet:
  "El Ministerio de Trabajo y Economía Social se ha visto afectado por un ataque informático. Los responsables técnicos del Ministerio y del Centro Criptológico Nacional están trabajando de manera conjunta para determinar el origen y restablecer la normalidad lo antes posibles".
- Varias publicaciones en Internet de fecha 9 de junio de 2021 informaban sobre el ciberataque:
  ******URL.1***. En esta publicación se indica que parece que la mayoría de los servicios siguen funcionando con normalidad.
  ******URL.2***. Se informa de que se trata de un ciberataque RyuK que fue el causante de la brecha en el SEPE.
  ******URL.3***.
- El ******FECHA.1*** el periódico digital de EL MUNDO
  ******URL.4*** informa también del ataque y el ******FECHA.2***
  ******URL.5*** indican que fuentes del Ministerio reportan que no ha habido robo de datos y que están restaurados casi todos los equipos.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en

cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final:

(…)

Respecto de las causas que hicieron posible la brecha,

(…)

Respecto de los datos afectados,

(…)

Respecto de las medidas de seguridad implantadas,

(…)

Respecto de la notificación con posterioridad a las 72 horas,

(…)

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

(…)

FUNDAMENTOS DE DERECHO

I
Competencia

En virtud de los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y resolver este procedimiento.

II
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales por el MITES.

El MITES realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El artículo 4 apartado 12 del 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 una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de disponibilidad; puesto que los datos personales no pueden ser tratados de forma legítima porque se han destruido, perdido o cifrado.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, 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, respectivamente.

III
Artículo 32 del RGPD

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"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 presente caso, en el momento de producirse la brecha de seguridad, no consta que el MITES no dispusiese de medidas de seguridad razonables en función de los posibles riesgos estimados.

A estos efectos, el MITES, ***(…).***

La brecha de seguridad, categorizada como de disponibilidad, se produce como consecuencia de ataque ransomware que han comprometido las credenciales de acceso a los servicios, ***(…).***

Sufrido dicho ataque como medida de contención se tomó la decisión conjunta de apagar todo el parque informático y desconectar la red del MITES de Internet y la Red SARA, provocando la indisponibilidad temporal de los servicios ofrecidos por ambos Organismos.

Si bien y puesto que se disponía de copias de seguridad de determinadas aplicaciones,
la indisponibilidad se redujo al período transcurrido entre el apagado y la restauración de la copia de seguridad, con lo que los servicios fueron entrando en proceso de restauración progresiva.

En consecuencia, no existen evidencias de no que se ha actuado de forma diligente una vez conocida la brecha de seguridad y que las medidas adoptadas con posterioridad al incidente aquí analizado no fueron adecuadas.

IV
Artículo 33 del RGPD

El Artículo 33 "*Notificación de una violación de la seguridad de los datos personales a la autoridad de control*" del RGPD establece:

"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."

En el presente caso, consta que el MITES sufrió una brecha de seguridad de los datos personales, el 9 de junio de 2021 y que no informó a esta Agencia.

El MITES manifiesta que ***(…).***

En consecuencia, inicialmente, no se pudo determinar hasta qué punto existía un riesgo para los derechos y libertades de los afectados, por lo que sabiendo que, si es improbable dicho impacto, no hay que notificarla a la autoridad de control.

Por todo ello, no existe vulneración del artículo 33 del RGPD.

V
Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, 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 MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL con NIF ***NIF.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