- **Expediente Nº: E/09932/2020**

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 esta Agencia de una brecha de seguridad de datos personales por parte del Responsable del Tratamiento CORPORACION RTVE, se ordena a la Subdirección General de Inspección de Datos que valore 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 en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 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:

Fecha de notificación de la brecha de seguridad de datos personales: ******FECHA.1***.

Resumen de la notificación: sustracción de un ordenador portátil y de un dispositivo *pen drive* no cifrados que contenían datos personales de sus empleados.

Documentación aportada: No consta documentación adjunta a la notificación de la presente brecha de seguridad.

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

- ***La investigada manifiesta que el ***FECHA.2 su Director de Área de Explotación y Medios Artísticos sufrió la sustracción de ordenador portátil y de un dispositivo pen drive no cifrados con datos personales vinculados a la entidad.***

- ***La investigada aporta copia de denuncia de los hechos ante la Policía Nacional en su dependencia de Madrid-Latina, del día ***FECHA.2 bajo atestado ***ATESTADO.1***.

- ***En la copia de la denuncia se aprecia que el citado Director aparcó su vehículo en la explanada de aparcamiento público y gratuito de la ***DIRECCIÓN.1 en ***ZONA.1 (Madrid), a las 14:30 horas del ***FECHA.2,***

tal que cuando volvió a por él, el cortavientos trasero derecho estaba fracturado y se había accedido al maletero del mismo, de donde se sustrajo su mochila, la cual contenía el ordenador portátil y el dispositivo pen drive involucrados en la presente brecha de seguridad.

- ***La investigada expresa ser informada de los hechos el 21/11/2020 y aporta copia del correo electrónico recibido por parte del Director involucrado.***

- ***La investigada alega que en el ordenador portátil no hay almacenamiento de datos personales, pero sí en el dispositivo pen drive, el cual contiene datos personales de empleados de su entidad en formato Excel.***

- ***La investigada informa que no cuenta con la certeza absoluta de la materialización efectiva de la brecha de confidencialidad, puesto que no conoce si se ha tenido acceso definitivamente a los datos personales por parte de un tercero ilegítimo, aunque decide notificarlo finalmente a la AEPD.***

- ***El 25/11/2020, la investigada establece una monitorización en la deep web, por parte de su unidad de ciberseguridad, de los archivos sustraídos, con la generación de informes periódicos sobre el estado de la misma, al efecto de contemplar el impacto sobre tratamientos posteriores, o reclamación por terceros. La investigada aporta copia de las comunicaciones por email para la implantación de esta medida.***

- ***El 27/11/2020, la investigada remitió apercibimiento al Director respecto a los hechos acontecidos, especialmente señalando la necesidad de ceñirse a la normativa correspondiente para el tratamiento de datos personales (encriptado, forma de entrada y salida de datos personales, …). La investigada aporta copia de correo electrónico remitido.***

- ***El 30/11/2020, la investigada recibe del Director un correo electrónico en que confirma que no disponía de dato personal alguno en su ordenador portátil sustraído puesto que trabajada todo en las carpetas compartidas de la corporación y en su usuario en OneDrive.***

- ***El 22/12/2020, la unidad de ciberseguridad de la investigada da traslado del último "Informe sobre Monitorización de filtraciones tras incidente de seguridad", del que aporta una copia. Dicha unidad de la investigada concluye no haber identificado en la sucesivas revisiones y búsquedas que se haya producido una fuga de información objeto de su investigación. La citada unidad añade que todas las búsquedas hasta esa fecha han dado un resultado negativo, por lo que no se ha podido identificar una publicación de los contenidos buscados ni indexadas en Google ni en Pastebin.***

- ***El 29/01/2021, la unidad de ciberseguridad de la investigada proporciona actualización del "Informe sobre Monitorización de filtraciones tras incidente de seguridad" en que sigue sin haberse identificado fuga de información involucrada en la presente brecha de seguridad.***

Respecto de las causas que hicieron posible la brecha:
La investigada señala la causa en el robo producido a un trabajador de su entidad, en el que, entre otros enseres y daños en las cosas, se sustrajo el ordenador portátil y el dispositivo pen drive con datos personales no cifrado.
La investigada expresa que el no cifrado del pen drive con datos personales es un error humano del empleado, de carácter aislado y fortuito.

Respecto de los datos afectados:
La investigada señala que los datos implicados se corresponden con:

- ***XXXX empleados de su entidad***
- ***Identificativos:***
  - ***Nombre y apellidos.***
  - ***Número de matrícula de empresa (número de empleado).***
- ***Detalles de empleo:***
  - ***Ocupación tipo y adscripción a Unidad.***
  - ***Asignación a programas con fechas, horarios y ubicaciones.***
  - ***Vigencias de programas con un campo de observaciones donde aparece información sobre tasa de recursos***

La investigada presenta un breve análisis del incidente de seguridad en el que se determina que los datos de los afectados son de escaso riesgo, y que no existen datos de comportamiento, datos de sistemas, financieros y/o económicos, ni datos sensibles por lo que entiende que no entraña un alto riesgo para sus derechos y libertades, por lo tanto, concluye que no resulta necesaria la comunicación a los afectados.
La investigada manifiesta no tener conocimiento de la utilización por terceros de los datos contenidos en el pendrive objeto de la presente brecha de seguridad.
La investigada informa no tener conocimiento respecto de publicación de datos personales afectados por el incidente en internet ni de la indexación por los motores de búsqueda.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo:
La investigada expresa que la presente brecha de seguridad se trató de un hecho aislado y puntual, y que ha emprendido diversas acciones para que no se repitan, entre las que destaca la formación y concienciación en protección de datos personales de sus empleados.

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

- ***La investigada expresa que desde marzo de 2018 acometió un plan de adecuación a la nueva normativa de protección de datos que consistió, principalmente, en la formación y concienciación del personal en dicha materia:***
    - ***5 sesiones formativas para Directivos y responsables (4 en Madrid y 1 en Barcelona).***
    - ***Creación del "Portal de Protección de datos" ubicado en su intranet.***
    - ***Elaboración de un Boletín Informativo sobre protección de datos.***
- ***La investigada informa que hasta septiembre de 2020 se proporcionó formación en protección de datos:***
    - ***Específica, en 12 sesiones presenciales.***
    - ***Técnica, en 2 sesiones.***
    - ***Para el área de compra, en 1 sesión virtual.***
- ***La investigada posee dos procedimientos, de los que aporta copia, que consisten en:***
    - ***Procedimiento de cifrado de ***CIFRADO.1 (enero 2019)***
    - ***Guía de uso seguro de los medios informáticos (***GUÍA.1 – enero 2019).***
- ***La investigada manifiesta haber creado un portal de ciberseguridad en el que se realizan actividades de concienciación, difusión y conocimiento de los protocolos en seguridad en la información. La investigada aporta copia de publicaciones en dicho portal.***
- ***La investigada relata que el 08/05/2020 remitió a los trabajadores, mediante comunicación interna de la que aporta copia, las "Recomendaciones de seguridad de equipamiento y de datos en situaciones de movilidad y teletrabajo".***
- ***La investigada aporta copia del registro de actividades del tratamiento, en que reseña como afectada la actividad "Empleados" en la presente brecha de seguridad, aunque especifica que sólo sus datos identificativos y de detalle del área al que pertenecen.***

- ***La investigada aporta copia de análisis de riesgos aplicado a sus actividades del tratamiento, en la que el riesgo asociado a la actividad "Empleados" requiere de evaluación de impacto relativa a protección de datos.***

- ***La investigada aporta copia de la evaluación de impacto relativa a protección de datos, creada el 23/05/2019 y modificada por última vez en abril de 2020, en que el tratamiento "Empleados" resulta de riesgo medio, pero con riesgo residuales de valor medio que, según su versión, les hace aplicar un plan de tratamiento de riesgos que lo mantiene en un riesgo minimizado.***

- ***La investigada dispone, y aporta copia, de la Norma 1/2020 (de febrero de 2020) sobre Protección de Datos, Garantía de los Derechos Digitales y Confidencialidad de la información (publicada en su Intranet corporativa como política de seguridad), en la que destaca el artículo 6 de obligaciones para su personal en la materia. La investigada añade que dicho documento posee un anexo como procedimiento de brechas de seguridad, del cual aporta una copia.***

- ***La investigada expresa no estar adscrita a código de conducta o certificación en materia de protección de datos a fecha 24/12/2020.***

Respecto de las medidas de seguridad de tipo preventivo frente a la posible repetición en el futuro de la brecha de seguridad:
La investigada sostiene que durante el año 2021 dispone planificadas diferentes acciones sobre concienciación y formación, entre las que cuenta con un curso sobre conceptos básicos de Protección de Datos dirigido a todos los trabajadores de su entidad y otro más avanzado para todos aquellos empleados que tratan datos personales. La investigada añade que, con ocasión de la celebración del Día Europeo de la Protección de Datos, el 28/01/2021, aprovechará para realizar determinadas acciones de concienciación en la materia que se están preparando.

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 de confidencialidad.

III

La seguridad del tratamiento” viene regulada en el artículo 32 del RGPD, que 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”.

III

CORPORACION RTVE señala la causa de la brecha es el robo producido a un trabajador de su entidad, en el que se sustrajo el ordenador portátil y el dispositivo pen drive con datos personales no cifrado. Además, expresa que el no cifrado del pen drive con datos personales es un error humano del empleado, de carácter aislado y fortuito. Esta empresa posee dos procedimientos de los que aporta copia que consisten en el cifrado de ***CIFRADO.1 (enero 2019) y una guía de uso seguro de los medios informáticos (GUÍA.1-enero 2019) para sus empleados.***

CORPORACION RTVE presenta un breve análisis del incidente de seguridad en el que se determina que los datos de los afectados son de escaso riesgo, y que no existen datos de comportamiento, datos de sistemas, financieros y/o económicos, ni datos sensibles por lo que entiende que no entraña un alto riesgo para sus derechos y libertades, por lo tanto, concluye que no resulta necesaria la comunicación a los afectados. Manifiesta no tener conocimiento de la utilización por terceros de los datos contenidos en el pendrive objeto de la presente brecha de seguridad.

Asimismo, informa no tener conocimiento respecto de publicación de datos personales afectados por el incidente en internet ni de la indexación por los motores de búsqueda.

CORPORACION RTVE sostiene que durante el año 2021 dispone planificadas diferentes acciones sobre concienciación y formación, entre las que cuenta con un curso sobre conceptos básicos de Protección de Datos dirigido a todos los trabajadores de su entidad y otro más avanzado para todos aquellos empleados que tratan datos personales.

De conformidad con lo indicado en los párrafos anteriores y con la información de la que se dispone en este momento, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

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 CORPORACIÓN DE RADIO Y TELEVISIÓN ESPAÑOLA S.A., con CIF A84818558 y domicilio en ******DIRECCIÓN.1*** - ******LOCALIDAD.1*** (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.

940-010921
Mar España Martí
Directora de la Agencia Española de Protección de Datos