- **Procedimiento N.º: E/03835/2020**

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: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de brecha de seguridad de los datos personales remitido por ESCUELA DE EMPRESARIOS, FUNDACIÓN DE LA COMUNIDAD VALENCIANA en el que informan a la Agencia Española de Protección de Datos que, con fecha 23/04/2020 detectaron la publicación de datos personales de sus alumnos en un portal web de compartición de conocimiento ajeno a su entidad.
Documentación aportada:
- Informe de detalle referido al incidente.
- Listado de 27 alumnos de 2016 en que aparecen sus fotos, nombre y apellidos, empresa en que trabaja, puesto laboral, teléfono de contacto y cuenta de correo electrónico de contacto, el cual se encontraba publicado en *documentop.com* y suponen datos personales afectados en esta brecha de seguridad.
- Repetido listado de 27 alumnos también de 2016 en que aparecen sus fotos, nombre y apellidos, empresa en que trabaja, puesto laboral, teléfono de contacto y cuenta de correo electrónico de contacto, el cual se encontraba publicado en *documentop.com* y suponen datos personales afectados en esta brecha de seguridad
- Listado de 23 alumnos de 2017 en que aparecen sus fotos (no de todos ellos/as), nombre y apellidos, empresa en que trabaja, puesto laboral, teléfono de contacto y cuenta de correo electrónico de contacto, el cual se encontraba publicado en *documentop.com* y suponen datos personales afectados en esta brecha de seguridad.

SEGUNDO: En fecha 4 de mayo de 2020, la Directora de la Agencia Española de Protección de Datos 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, teniendo conocimiento de los siguientes extremos:

Fecha de notificación de la brecha de seguridad de datos personales: 25/04/2020.

ENTIDAD INVESTIGADA

ESCUELA DE EMPRESARIOS, FUNDACIÓN DE LA COMUNIDAD VALENCIANA (en adelante, la investigada), con NIF G97250013 y domicilio en La Marina de Valencia-Muelle de la Aduana s/n, Edif. Edem-46024 Valencia (Valencia).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Con fecha 01/06/2020 se solicitó información a la investigada y de la respuesta recibida de la investigada el 17/06/2020 se desprende lo siguiente:

Respecto de la empresa.

- La investigada se identifica como la responsable del tratamiento de los datos personales en que se ha producido la brecha de seguridad.
- La investigada dispone de delegada de protección de datos y así consta reflejado en la Agencia Española de Protección de Datos (en adelante, AEPD).
- La investigada ha contado con los servicios de una entidad de consultoría especializada, para la resolución de la presente brecha de seguridad. ******EMPRESA.1*** (con NIF ******NIF.1***), en adelante, su consultora.

Respecto de la cronología de los hechos

Todo según manifestaciones de la investigada:

- 23/04/2020 (11:00 horas): La investigada detecta la publicación de dos listados, con datos de 50 de sus alumnos, referidos como “ABC del Negocio en Internet” de 2016 y de 2017 en la web *documentop.com*. Se trata de unos listados elaborados por la investigada que son facilitados a los alumnos a efectos de que se conozcan entre ellos y a los profesores, a efectos de que puedan desarrollar su actividad docente.
- 23/04/2020 (11:30 horas): La investigada contacta con el equipo de seguridad de su consultora para solicitar apoyo en la investigación de este incidente y averiguaciones sobre la publicación de dichos listados.
- 23/04/2020 (12:00 horas): La investigada proporciona todas las evidencias al equipo de respuesta a incidentes de su consultora.
- 23/04/2020 (13:30 horas): Se realiza la primera reunión entre el equipo de respuesta a incidentes de su consultora y la investigada en la que se decide:
    - La investigada contactará con el portal para solicitar la retirada inmediata de los archivos.
    - La investigada solicita a su consultora la realización de un pentest contra la infraestructura propia para determinar posibles vulnerabilidades que permitan tener acceso a este tipo de información y reforzar así sus medidas de seguridad. Se trata de una auditoría que facilita una visión global sobre el estado en el que se encuentra la investigada.
    - La investigada solicita a su consultora la realización de un ejercicio de vigilancia digital con el fin de determinar si se encuentran más archivos de este estilo publicados en otras páginas y reforzar así sus medidas de seguridad, lo que implica una búsqueda por indexación.

- 23/04/2020 (17:30 horas): Se realiza una segunda reunión entre las anteriores partes, la investigada indica que ha preparado la comunicación que realizará con la página web y que ha compartido con el equipo de su consultora para su validación previa a su presentación.

  Por otra parte, su consultora indica a la investigada que, de las comprobaciones efectuadas, no se evidencia la existencia de ningún otro documento propio que se encuentre publicado y que no se haya publicado de forma voluntaria por la investigada.

  Se informa asimismo que no será posible determinar quién ha introducido los documentos en el portal, a menos que este portal facilite la información de quién subió estos archivos.

  Respecto de la realización del pentest (auditoría) contra la infraestructura de la investigada para determinar sus posibles vulnerabilidades y reforzar su seguridad, deberá emplear un tiempo proporcional a la infraestructura de ésta y coordinarse con la organización. Estos ejercicios se repetirán en el tiempo para mejorar su seguridad.

  La investigada en muestra de su responsabilidad proactiva manifiesta que está interesada en la realización de esta prueba por lo que la coordinación con su consultora se iniciará el lunes 27 de abril.

  Asimismo, la investigada manifiesta que habiendo realizado la evaluación del incidente siguiendo las indicaciones de la "Guía para la notificación y gestión de brechas de seguridad" de la AEPD, no concurren los requisitos para la comunicación del incidente a la esa autoridad, pero en cumplimiento del principio de accountability y responsabilidad proactiva va a proceder a su comunicación, para una mayor garantía, por lo que solicita la emisión de informe sobre las actuaciones realizadas hasta la fecha para su presentación dentro del plazo de 72 horas previsto para ello.

  Su consultora realiza este mismo análisis y concluye que no existe obligación, de acuerdo con los criterios de la AEPD, pero está de acuerdo con que su comunicación implica una muestra de los principios que deben regir en el cumplimiento de la normativa en materia de protección de datos. La investigada aporta "Informe de análisis de necesidad de notificación" a la AEPD, elaborado por su consultora en fecha 24/04/2020 en que motiva la no necesidad de la notificación y la negativa repercusión de la marca por no hacerlo.

- 18/05/2020: Tras diversos trabajos preparatorios y de coordinación entre la investigada y su consultora se inicia la auditoría (un "test de intrusión") a los efectos de verificar el estado de seguridad propia ante posibles ataques externos. El test se realiza durante los días 18, 19, 20, 21, 22, 25 y 26 de mayo de 2020.

- Meses de abril y mayo: Se continúa con la comunicación a la página web *documentop.com* y, tras diversas comunicaciones, se comprueba que se ha

procedido por parte de ésta a la eliminación de los documentos. El incidente se considera cerrado.

- 27/05/2020: Se emite informe por parte de su consultora acerca de los resultados de la auditoría ("test de intrusión" o *pentest*) en el que no se evidencia que dichos documentos hayan podido ser obtenidos por un tercero de la infraestructura de la investigada. Se comprueba que fueron publicados por un usuario registrado como "Guest" en fecha 30/09/2017 y del que no se ha podido obtener la identidad, pues la página web no la ha facilitado.

Respecto de las causas que hicieron posible la brecha de seguridad e información sobre la recurrencia de eventos similares acontecidos en el tiempo

La investigada aporta un "Informe ejecutivo del test de intrusión" realizado por su consultora en fecha 27/05/2020 en que expone que se trata de una publicación efectuada por un usuario registrado en la página web *documentop.com* que se efectuó el 30/09/2017. Los listados de alumnos afectados por esta brecha de seguridad estaban disponibles para alumnos y profesores a través de la aplicación de Moodle (Campus), manifestando, en dicha auditoría, la no constancia de posible acceso a los sistemas de la investigada para obtener la información implicada en la brecha de seguridad.

La investigada informa no haber tenido constancia de la existencia de hechos similares y/o análogos a la presente brecha de seguridad con anterioridad. La investigada aporta "Informe del incidente" en detalle, elaborado por su consultora en fecha 24/04/2020, en que describe no haber localizado en el momento de la detección del incidente otros hechos similares ni eventos análogos.

Respecto a los datos afectados

La investigada identifica como datos personales implicados en la brecha de seguridad a datos meramente identificativos y no sensibles, de carácter profesional de 50 alumnos. En concreto, los datos contenidos en los archivos son:

- Números de teléfono profesional.
- Nombres completos.
- Dirección de correo electrónico profesional.
- De estas 50 personas, 37 aparecen con fotografía.

La investigada manifiesta no tener conocimiento de que se haya utilizado la información por terceros, habiéndose efectuado la búsqueda por indexación según consta en un "Informe ejecutivo del test de intrusión" realizado por su consultora en fecha 27/05/2020.

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

La investigada aporta un “Informe de medidas de seguridad” catalogado como CONFIDENCIAL, que representa un análisis conforme al marco de control del Anexo A de la ISO 27001, realizado en fecha 11/06/2020 por su consultora. En dicho informe se relatan y detallan las medidas de seguridad implantadas en la investigada y se ha catalogado como de contenido RESTRINGIDO por esta AEPD.

La investigada aporta copia parcial del Registro de las Actividades de Tratamiento en las que se enmarcan los datos personales comprometidos, en concreto el tratamiento “Formación Directiva” donde se aprecia entre los fines del tratamiento *“Proporcionar al Profesor y a los alumnos un listado de los componentes del curso.”*

La investigada aporta copia del análisis de riesgos que contiene un análisis GAP de situación frente a buenas prácticas de la ISO 27001. Asimismo, dicho documento contiene los riesgos detectados y la gestión de estos, así como la situación actualizada en la que se encuentra la investigada al respecto. El citado archivo incluye gráficos representativos de la situación de la investigada respecto a los riesgos inherentes, los riesgos actuales y los riesgos residuales.

La investigada aporta copia de la evaluación de impacto relativa a la protección de datos (en adelante, EIPD) aplicada al tratamiento “Formación directiva”, a pesar de que del análisis de riesgo asociado se obtuvo “riesgo medio”, la investigada expresa tener un fuerte compromiso con el cumplimiento de la normativa en materia de protección de datos y con el fin de minimizar al máximo los riesgos del tratamiento. Junto a esa EIPD, la investigada aporta un plan de acción elaborado para profundizar y mejorar en las conclusiones obtenidas.

Respecto de las medidas de minimización del impacto de la brecha de seguridad y de las acciones tomadas para la resolución final de la brecha

La investigada relata el siguiente conjunto de medidas tomadas para la minimización del impacto y resolución final de la presente brecha de seguridad:

- Se solicitó a su consultora la realización de las tareas de investigación a efectos de conocer la existencia de otros posibles incidentes no identificados y no se localizó ninguno. La investigada aporta “Informe del incidente” en detalle, elaborado por su consultora en fecha 24/04/2020.

- Se solicitó por la organización en reiteradas ocasiones la eliminación de los documentos de la web *documentop.com*. La investigada aporta copia de los correos electrónicos y las solicitudes enviadas a la web para la eliminación de contenidos, en fechas 23/04/2020 y 24/04/2020.

- Se solicitó por parte de la investigada la realización de una auditoría (test de intrusión o *pentest*) a efectos de comprobar la seguridad propia. La investigada aporta un “Informe ejecutivo del test de intrusión” realizado por su consultora en fecha 27/05/202.

- Se ha iniciado un plan de acción para llevar a cabo las recomendaciones efectuadas en la auditoría realizada. La investigada aporta un plan de acción respecto al test de intrusión con implantación hasta junio de 2021.

- Se va a continuar con la ejecución del Plan de Acción previsto en la EIPD aportada por la investigada. En él constan las fechas de ejecución de las medidas que han sido implantadas, así como aquellas en las que se implantarán las medidas pendientes.

- Se contactó con los profesores vía telefónica a los efectos de informar sobre la circunstancia acaecida el mismo día de la detección del incidente y solicitar información al respecto, el 23 de abril de 2020.

Respecto de las medidas implementadas con posterioridad a la brecha

La investigada aporta "Informe de análisis de necesidad de notificación" a la AEPD, elaborado por su consultora en fecha 24/04/2020, en que concluye respecto al impacto que pudiera tener la brecha de seguridad sobre los derechos y libertades de los interesados para conocer si suponía un alto impacto, siendo el resultado de este "bajo", no siendo necesario presentar la notificación a la AEPD. De todas formas, en aras de un cumplimiento proactivo de la normativa de protección de datos la investigada expone haber comunicado el incidente a la AEPD, pero no a los interesados, pues debido al bajo impacto del incidente de seguridad sobre los derechos y libertades de los interesados afectados, lo entendió como no obligada a llevarla a cabo, alegando lo dispuesto en el artículo 34 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*.

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, como consecuencia de la publicación de datos personales de alumnos en un portal web de conocimiento ajeno a su entidad.

El artículo 32 del RGPD señala lo siguiente:

"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.".

El citado artículo contempla que "*el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".* En consecuencia, no adopta una relación cerrada de medidas técnicas y organizativas, sino que éstas deberán ser las apropiadas en función del nivel de riesgo previamente analizado.

Añade el artículo 33 del RGPD que: "*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.". Y el apartado 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".*

En consecuencia, se trata de determinar si las medidas técnicas y organizativas eran las adecuadas al nivel de riesgo predeterminado, así como la diligencia en la reacción ante una brecha de seguridad y, en su caso, las medidas adoptadas para evitar que en el futuro pueda repetirse una incidencia de similares características que pueda comprometer los derechos y libertades de los interesados.

De las actuaciones de investigación se desprende que la entidad investigada, en calidad de responsable del tratamiento, disponía de medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencia, pero, sin embargo, de forma excepcional se produjo la incidencia ahora analizada. Aporta un informe de medidas de seguridad realizado por su consultora en el que se detallan las medidas de seguridad implantadas, así como Registro de Actividades de Tratamiento, Análisis de Riesgos y copia de la Evaluación de Impacto aplicada al tratamiento "formación directiva", a pesar de que del análisis de riesgo asociado se obtuvo riesgo medio.

Consta que la investigada ha solicitado la eliminación de los documentos en la web y solicitado a su consultora la realización de tareas de investigación a efectos de conocer la existencia de otros posibles incidentes, no localizándose ninguno.

Asimismo, la entidad investigada disponía de protocolos de actuación para afrontar el incidente, lo que ha permitido la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, comunicar, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro, a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y el Delegado de Protección de Datos.

Por último, no consta hasta la fecha que los datos personales de los alumnos (números de teléfono profesional, nombres completos, dirección de correo electrónico profesional y fotografía) contenidos en la web hayan sido objeto de tratamiento posterior por terceros ajenos, ni constan reclamaciones ante la AEPD por los afectados.

En consecuencia, se debe concluir que la entidad investigada disponía de medidas técnicas y organizativas razonables y proporcionales al nivel del riesgo para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente y proactiva, mediante la realización de una auditoría (test de intrusión) a efectos de comprobar la seguridad y la iniciación de un plan de acción para llevar a cabo las recomendaciones efectuadas en la auditoría realizada. Además, la entidad investigada dispone de un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto sobre los afectados.

III

Por tanto, la actuación de la entidad 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 ESCUELA DE EMPRESARIOS, FUNDACIÓN DE LA COMUNIDAD VALENCIANA, con NIF G97250013 y domicilio en La Marina de Valencia-Muelle de la Aduana s/n, Edif. Edem-46024 Valencia (Valencia).

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