- **Procedimiento Nº: E/00351/2021**

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 JOB DIGITAL NETWORKS SL, con número de registro de entrada ******REGISTRO.1*** relativa a la comunicación con fecha ******FECHA.1***, por parte de empresa de ciberseguridad externa que ha aparecido en Twitter la oferta de compra de una BBDD perteneciente a su empresa, 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: A la vista de la citada notificación de quiebra de seguridad de los datos personales, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, teniendo conocimiento de los siguientes extremos

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

JOB DIGITAL NETWORKS SL con CIF B66583907

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 9 de febrero de 2021 se solicitó información a JOB DIGITAL NETWORKS SL. De la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

JOB DIGITAL NETWORKS, S.L.U. es una sociedad mercantil perteneciente al Grupo Eurofirms, que gestiona el portal de empleo ******PORTAL.1***, cuya finalidad es que demandantes empleo (candidatos) se den de alta en el portal para que poder apuntarse a las diversas ofertas de empleo publicadas por empresas o, que éstas puedan consultar según sus necesidades los currículos de los candidatos.

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

El ***FECHA.2** un trabajador de ***PORTAL.1** publicó por error cuatro archivos de código fuente que contenían claves de acceso a Amazon Web Services (AWS) para una cuenta de servicio utilizada para procesamiento de datos (es decir, una cuenta no asociada a ninguna persona).

El mismo día llegó a ***PORTAL.1** una notificación por email de Amazon Web Services (AWS) indicando que una clave de acceso había sido expuesta en público. En cuanto se leyó el email reenviado, se retiró el código publicado en el repositorio. ***PORTAL.1** comprobó que el código no estaba indexado en buscadores.

El 29 de diciembre de 2020 se publicaron dos posts en el foro de ***FORO.1** indicando que disponían de un archivo con datos de usuarios de ***PORTAL.1**. Hasta el ***FECHA.1** la compañía no tuvo conocimiento de ello.

El ***FECHA.1** llegó a ***PORTAL.1** un email de una empresa de seguridad notificando que se había puesto a la venta una base de datos de usuarios de ***PORTAL.1**. El mismo día ***PORTAL.1** comprobó en el foro en cuestión la veracidad de dicho email. Todos estos hechos permiten la detección de la brecha de seguridad.

El ***FECHA.1** se activa el protocolo de brecha de seguridad de la empresa que implica la realización de las siguientes acciones para su resolución:

El día 8 de enero de 2021 ***PORTAL.1** se puso en contacto con los autores de las entradas del foro para explorar la adquisición de los datos sustraídos. Se negocian los siguientes aspectos:

• Eliminar el archivo filtrado y no ponerlo más a la venta

• Borrar las entradas del foro donde se publicó el filtrado

• Conocer el mecanismo de acceso utilizado para confirmar si los hechos anteriores son correctos y asegurar que no vuelva a ocurrir el mismo filtrado

Al llegar a un acuerdo, los autores eliminaron las entradas del foro el día 9 de enero de 2021.

El mismo día 8 de enero de 2021 se eliminó la generación del archivo de traspaso filtrado y se verificó la imposibilidad de acceder al mismo, con lo que se impidieron accesos no autorizados adicionales.

Paralelamente el 9 de enero de se realiza denuncia ante los Mossos de Escuadra.
El 15 de enero de 2021 por la tarde (a partir de las 16:00) se cambiaron las credenciales de acceso al Data Warehouse (destino final de los datos filtrados).

El 18 de enero de 2021 a las 9:15 (aproximadamente) se cambiaron las credenciales de acceso a la base de datos transaccional (origen de los datos filtrados).

El 19 de enero de 2021 a las 15:16 se ratificó con la persona que ha obtenido de forma no autorizada los datos la forma en que accedió a los mismos. Además, se verificó que ha eliminado cualquier rastro de los datos filtrados.

Respecto de las causas que hicieron posible la brecha

La publicación el ******FECHA.2*** de cuatro archivos de código se produjo en un repositorio de uso habitual en ******PORTAL.1***. Normalmente estos repositorios se configuran como privados, pero en este caso se marcó el repositorio de forma accidental como público. Estos archivos contenían credenciales y rutas de acceso para una cuenta de servicio (es decir, no ligado a una persona) utilizado por procesos de tratamiento de datos.

Respecto de los datos afectados.

El fichero filtrado contiene ***XXXXXXX*** registros, tanto de usuarios particulares como de empresas. Esta información procede de un volcado parcial de datos de usuario, realizado como parte del proceso de traspaso habitual de datos a sistemas de Business Intelligence.
Los datos almacenados en el fichero de datos son:
Nombre y apellidos, género, fecha de nacimiento, número de teléfono, correo electrónico, dirección IP de registro, coordenadas y nombre de la ubicación del usuario, dirección web de la fotografía de perfil, descripción resumida del perfil “acerca de mí”, experiencia laboral, educación, idiomas.

Adicionalmente, el archivo contiene contraseñas ofuscadas y tokens de acceso al portal ******PORTAL.1***.

El archivo filtrado tiene contraseñas ofuscadas, de forma que no es probable una recuperación de las contraseñas originales.

Los tokens de acceso, también presentes en el archivo de datos, se han hecho expirar y ya no son efectivos. Por tanto, no es posible realizar un acceso al portal de ******PORTAL.1*** en nombre de los usuarios incluidos en el archivo.

Las coordenadas y la ubicación incluidas en los datos son válida hasta ciertos niveles de precisión (ciudad, barrio, pero no calle y número). Adicionalmente, sólo refleja la ubicación deseada para la búsqueda de ofertas de empleo en el portal de ******PORTAL.1***. En ambos casos las coordenadas se fijan con la edición del perfil y no de forma continua. Es decir, estas coordenadas no reflejan la posición geográfica real del usuario de ******PORTAL.1***.

Respecto del resto de datos personales, son informaciones disponibles dentro del propio portal de ******PORTAL.1***, accesibles para las empresas mediante un registro gratuito y realizando búsquedas en el espacio habilitado para empleadores tras la aceptación de las condiciones de uso y la política de privacidad. Por tanto, es información puesta a disposición del portal ******PORTAL.1*** por los propios usuarios.

Manifiestan que, dada la recuperación del archivo filtrado, no se prevén consecuencias para los afectados.

No se ha tenido constancia posterior del uso de los datos por parte de terceros.

Dado que se han recuperado los datos y no se ha producido un uso no autorizado, no se ha considerado necesario comunicarlo a los afectados.

Respecto de las medidas de seguridad implantadas

Con anterioridad a la brecha:

Firewall que impide el acceso a servicios de computación desde direcciones IP no autorizadas. Existen diferentes configuraciones de firewall para dar acceso a varios conjuntos de servicios. Acceso a máquinas virtuales mediante archivos de credenciales del que sólo disponen personas seleccionadas, y que se mantienen en ordenadores locales. Política de dar a cada cuenta los accesos que necesita y ninguno más. Claves de acceso secretas para usuarios de servicio del sistema de computación. Ofuscación de contraseñas almacenadas en base de datos. Caducidad de los tokens de acceso.

Motivo por el cual las medidas de seguridad implantadas no han impedido el incidente:

Partiendo de la publicación accidental del código fuente, disponer de las credenciales de la cuenta de servicio de los servicios de computación en la nube permite acceder a algunos sistemas. La cuenta de servicio dispone de acceso limitado a los servicios de computación, de forma que no puede crear, cambiar o eliminar configuraciones ni servicios. Únicamente dispone de accesos de lectura a algunos servicios. Entre ellos se incluye el sistema de archivos en la nube que, es el lugar por donde se produjo la filtración de datos.

Con posterioridad a la brecha:

-Se han cambiado las credenciales de la cuenta de servicio, de forma que las publicadas en el código fuente ya no son operativas.

Se ha eliminado la posibilidad de acceso al archivo filtrado del sistema de almacenamiento en la nube.

Adicionalmente, se han cambiado las contraseñas de las bases de datos transaccional y Data WareHouse. Como medida adicional, se ha creado un usuario específico para acceder a la base de datos transaccional con motivo de análisis de datos.

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

JOB DIGITAL NETWORKS fue adquirida en el 2019 y, tanto desde su adquisición, como según la información facilitada por los empleados actuales que trabajaban con anterioridad a la compra de la empresa, no se tiene constancia de ninguna brecha de seguridad ni filtración de datos en todo el tiempo de vida de la empresa, desde 2015.

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.

La empresa afirma contar previamente a la brecha, con las siguientes medidas de seguridad de los tratamientos, firewall que impide el acceso a servicios de computación desde direcciones IP no autorizadas, contando con diferentes configuraciones de firewall para dar acceso a varios conjuntos de servicios, acceso a máquinas virtuales mediante archivos de credenciales del que sólo disponen personas seleccionadas, y que se mantienen en ordenadores locales, política de dar a cada cuenta los accesos que necesita y ninguno más, claves de acceso secretas para usuarios de servicio del sistema de computación, ofuscación de contraseñas almacenadas en base de datos y caducidad de los tokens de acceso. De todo ello se desprende que con anterioridad, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados.

La brecha fue posible, por la publicación, en un repositorio BitBucket, que se configuró por error como público, de cuatro archivos de código que contenían credenciales y rutas de acceso.

En cuanto al impacto, los datos que se han visto vulnerados son: nombre y apellidos, género, fecha de nacimiento, número de teléfono, correo electrónico, dirección IP de registro, coordenadas y nombre de la ubicación del usuario, dirección web de la fotografía de perfil, descripción resumida del perfil "acerca de mí", experiencia laboral, educación e Idiomas. Además el archivo, contiene contraseñas ofuscadas y tokens de acceso al portal.

El volumen de Datos se encuentra en el rango de 4.000.000, no teniendo constancia de su uso por terceros, ni se prevee que pueda producirse, ya que se ha recuperado el archivo. Asimismo al contar con contraseñas ofuscadas y al haber hecho expirar los tokens, no parece posible, realizar accesos el portal en nombre de los usuarios.

Para evitar que estos hechos se vuelvan a repetir, se eliminan todas las credenciales de acceso en el código fuente, se usan servicios de provisión segura de credenciales y almacenamiento seguro (gestores de secretos o variables de entorno de usuario) de

las credenciales mínimas para acceder al servicio proveedor de credenciales, se eliminan
los archivos temporales de traspaso una vez realizado el mismo y se auditan los archivos almacenados en sistemas de archivo y eliminándose los no necesarios.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia, no obstante y una vez detectada ésta, se produce una diligente reacción al objeto de notificar a la AEPD, realizar la denuncia ante la policía e implementar medias para eliminarla.
Por último, se recomienda elaborar un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada.

III

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:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a JOB DIGITAL NETWORKS SL con CIF B66583907 .
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