

**Procedimiento N°: E/06301/2019**

940-0419

## **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 tras la recepción de un escrito de notificación de quiebra de seguridad remitido por la entidad **YOUNOW, INC.** (en adelante *YouNow*), con NIF **74369412Q**, en el que se informa a la Agencia Española de Protección de Datos que con fecha 13/02/2019 han tenido conocimiento, a través de un periodista del diario *The Register* sobre la venta de datos relacionados con el servicio de *YouNow* a través de la Internet oscura.

El correo electrónico del periodista contenía un archivo adjunto que incluía una muestra de datos de diez usuarios cuyos datos supuestamente fueron obtenidos de los servidores de *YouNow*. Según el periodista, el ataque informático tuvo lugar en octubre de 2017.

**SEGUNDO:** La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de notificación, teniendo conocimiento de los siguientes extremos:

### **ANTECEDENTES**

Fecha de notificación de quiebra a la AEPD : 17 de abril de 2019

### **ENTIDADES INVESTIGADAS**

*YOUNOW, INC. con NIF 74369412Q con domicilio en 5TH AVENUE, NUM 245 - NUEVA YORK.USA.*

### **RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN**

#### **Respecto de las causas que han hecho posible la incidencia**

- *YouNow* ha llevado a cabo una investigación interna exhaustiva, pero no ha podido determinar la causa de la brecha de seguridad notificada y la forma en que el pirata informático supuestamente obtuvo los datos de los servidores de *YouNow*.
- Cuando *YouNow* recibió la petición del periodista, muchos meses después de la presunta brecha, la página web que supuestamente vendía los datos contenidos

en los servidores de *YouNow* ya no estaba activa, y los datos ya no se encontraban disponibles.

- Debido al significativo lapso de tiempo entre la presunta brecha (octubre de 2017) y la toma de conocimiento de la misma por parte *YouNow* (febrero de 2019), *YouNow* no ha podido confirmar de manera concluyente y afirmativa que los datos supuestamente vendidos en la internet oscura proviniesen de los servidores de *YouNow*. Además, no existen datos forenses disponibles para que *YouNow* investigue y determine cómo el pirata informático obtuvo acceso a los datos.

**Respecto las acciones tomadas con objeto de minimizar los efectos adversos y acciones realizadas para la resolución final de la incidencia**

- Tan pronto como *YouNow* tuvo conocimiento de la presunta brecha, *YouNow* activó de inmediato su Procedimiento de Respuesta a Brechas de Seguridad (cuya copia aportan) y adoptó las siguientes acciones en las siguientes fechas:
  - o El 14 de febrero de 2019, el entonces Delegado de Protección de Datos de *YouNow* nombró un equipo de investigación.
  - o El equipo realizó una evaluación del daño potencial que podría causar a los usuarios de *YouNow* la presunta publicación de sus datos. El equipo ha determinado que el daño potencial fue bajo. La evaluación se basó en los siguientes factores:
    - Los datos que supuestamente se obtuvieron eran básicos y no sensibles como nombres, ID de redes sociales públicas y correos electrónicos;
    - La falta de contraseñas de usuario o tokens de acceso a *YouNow*.
    - Los datos que supuestamente se obtuvieron no incluían ningún número de identificación nacional, como números de pasaporte / documentos de identidad, datos de seguridad social o cualquier información que pudiera ser utilizada para robos de identidad;
    - Los datos que supuestamente se obtuvieron no incluían datos financieros o monetarios, como números de tarjetas de crédito, números de cuentas bancarias, etc., que pudieran ser utilizados para fraudes financieros.
  - o Debido al resultado de la evaluación realizada por el equipo y la incertidumbre acerca de cómo se obtuvieron los datos, el equipo decidió mantener los sistemas de *YouNow* en funcionamiento y diseñar un plan de acción a corto y largo plazo.
  - o Se informa a la plantilla de *YouNow* acerca de la brecha de seguridad y se celebra una sesión informativa.
  - o Para los distintos productos de *YouKnow* se cambian contraseñas, se revocan calves de acceso y se activa la autenticación multifactor.
  - o Debido a que la investigación interna no determina la vulnerabilidad por la que se produjo el ataque, el 25/06/2019 se reabre un programa de recompensas de *YouNow* y se incorporan 25 investigadores de seguridad que encuentran una vulnerabilidad, la cual es resuelta el 19 de agosto de 2019.

### **Respecto de si tiene conocimiento de la utilización por terceros de los datos personales obtenidos a través de la brecha**

- Tras la conclusión de la investigación interna, YouNow no ha encontrado evidencia de que un tercero utilice datos personales obtenidos a través de la presunta brecha, o que los datos sean indexados por algún motor de búsqueda.

### **Respecto a la política de seguridad**

- Antes de la brecha de seguridad, YouNow tenía implementadas las siguientes medidas de seguridad:
  - o Clústeres VPC en AWS, con reglas de acceso de seguridad muy estrictas: lista blanca de IP y acceso VPN únicamente;
  - o Caducidad de contraseña en AWS cada tres meses, no permitir la reutilización de contraseña o contraseñas débiles;
  - o Bastiones para acceder a los servidores utilizando SSH;
  - o Cifrado de la base de datos;
  - o Administración de contraseñas de Dashlane para todas las cuentas de trabajo;
- Como resultado de la brecha de seguridad, YouNow ha actualizado su política de seguridad para incluir: (algunos datos se han omitido por motivos de confidencialidad encontrándose disponibles para los interesados en el expediente)
  - o Autenticación obligatoria de dos factores;
  - o Inicio de sesión único obligatorio (SSO) para Slack;
  - o Cambio automático de contraseña para todas las cuentas de YouNow Gmail cada cierto tiempo predeterminado;
  - o Política de revocación y actualización de clave de acceso cada cierto tiempo predeterminado;
  - o Análisis de todos los sistemas internos en busca de claves de acceso / contraseñas filtradas cada cierto tiempo predeterminado;
  - o Activación de un sistema de detección de intrusiones para identificar cualquier actividad inusual en la cuenta de AWS de YouNow y en todos sus activos, y creación de alarmas en torno a cualquier evento de gravedad media y superior.
- Aportan copia del del Registro de Actividad de los tratamientos donde se ha producido la incidencia.
- Aportan documentos de evaluación de Impacto y análisis de riesgos realizados
- copia del Procedimiento de Respuesta a Brechas de Seguridad de YouNow. Este procedimiento ha sido implementado en la empresa.

## **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**

En el presente caso se debe señalar que la supuesta quiebra de seguridad se produjo dos años antes de tener conocimiento de la misma, lo que ha dificultado las investigaciones internas al haber desaparecido la web maliciosa que supuestamente recopilaba datos de los servidores de *YouNow* y posteriormente los vendía en la internet oscura.

En estas condiciones, debe señalarse que la entidad afectada inició actuaciones de investigación y revisó los servidores en busca de anomalías de seguridad de forma diligente. También implantó nuevos equipos físicos y lógicos al objeto de elevar el nivel de seguridad del sistema de información contra posibles intrusiones indebidas y promovió otras iniciativas procedimentales e informativas entre sus empleados. Entre ellas, hay que destacar la puesta en marcha de un programa de recompensas en el que se incorporaron 25 investigadores de seguridad en busca de vulnerabilidades en el sistema de información.

Por otro lado, no constan denuncias de los usuarios afectados ni otras acciones de las que se pueda inferir perjuicios a terceros.

### **III**

Por lo tanto, se ha acreditado que la actuación de *Younow* como entidad responsable del tratamiento de los datos personales de sus usuarios, 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 *YOUNOW, INC. con NIF 74369412Q con domicilio en 5TH AVENUE, NUM 245 - NUEVA YORK.USA.***



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