- **Procedimiento Nº: E/08399/2020**

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 violación de seguridad de datos personales (en adelante brecha de seguridad) por parte del Responsable del Tratamiento FREEPIK COMPANY, S.L., 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 objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de la brecha de seguridad de datos personales:

1. ******FECHA.1***.
2. ******FECHA.2***.
3. ******FECHA.3***.
4. ******FECHA.4***.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

FREEPIK COMPANY, S.L, con CIF B93183366 y domicilio en C/ ******DIRECCIÓN.1, ***LOCALIDAD.1***.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Respecto de la empresa.

- FREEPIK COMPANY, S.L. (en adelante Freepik) es una compañía que proporciona recursos gráficos a sus usuarios. Es responsable de las webs ******URL.1*** y ******URL.2***.

- Freepik ha notificado en cuatro ocasiones por dos brechas de seguridad.

- Resumen de las notificaciones

PRIMERA NOTIFICACIÓN:

Con fecha ***FECHA.1** se presenta una notificación de brecha por parte de Freepik a través del servicio de correos por no poder realizarse a través de la sede electrónica de la AEPD.

En esta notificación se pone de manifiesto que se ha recibido un correo electrónico de un tercero (en adelante hacker) en el que les informa que dispone de una relación 500.000 usuarios y contraseñas de las cuentas de Freepik exigiendo un pago para no publicar este contenido en la *dark web* y procederá a informar a los usuarios de estos hechos utilizando el mail que obra en su poder.

Freepik solicita evidencias y el hacker les facilita un listado con 30.000 mails de usuarios de la compañía.

En un primer análisis se comprueba que 29.978 usuarios de los 30.000 del listado corresponde a usuarios y contraseñas fácilmente disponibles en la *dark web* como consecuencia de otras filtraciones a empresas. No obstante 23.704 también son usuarios de la compañía.

Freepik considera que los datos que puede disponer el tercero, además de las credenciales de usuario, corresponden a datos de uso de la plataforma (descargas, autores,…) y datos de carácter no obligatorios de nombre, localización, cargo, cuentas en redes sociales, y en caso de clientes Premium datos de facturación de NIF ya que los datos de la tarjeta de pago no están disponibles.

Manifiestan que comunicarán la brecha a los afectados y no informan sobre posibles afectados en otros países de la Unión Europea ya que desconocen la ubicación de los titulares de las direcciones de correo.

SEGUNDA NOTIFICACIÓN:

Con fecha ***FECHA.2** se recibe una ampliación de la notificación anterior en la que Freepik verifica que 23.704 de las 30.000 direcciones de correo electrónico del listado facilitado por el hacker, son usuarios de Freepik y que no se ha podido concluir la ubicación correspondiente a cada dirección de correo electrónico revisada, por lo que, de forma exclusivamente preventiva, se ha optado por seleccionar todos los Estados miembros de la UE con posibles afectados.

Asimismo, Freepik manifiesta que no se ha detectado ni hay evidencias de accesos inusuales ni sospechosos de forma masiva a las cuentas de los usuarios ni que estas se encuentren comprometidas.

Dicho análisis ha permitido detectar, en cambio, un acceso muy alto procedente de varias direcciones IP a las URL de Freepik que permite saber si un email determinado está registrado en Freepik (pero que no implica un acceso a las cuentas correspondientes). Dichos intentos de acceso, tras la implementación de las medidas de seguridad adicionales llevadas a cabo por Freepik a raíz de este incidente, se han visto reducidos drásticamente.

Freepik ha comprobado que después de cotejar 2.711.162 direcciones de correo electrónico y contraseñas, se ha encontrado únicamente 171.280 usuarios con contraseñas expuestas en la *dark web*.

En consecuencia, Freepik consideran que el hacker se ha limitado a realizar un barrido en la web de Freepik para comprobar qué direcciones de correo electrónico (usando las que están disponibles en los citados listados) se encuentran registradas en Freepik.

En esta notificación aportan justificante de presentación de la brecha remitida por correo de fecha ******FECHA.1*** (documento nº1), listado de intentos de acceso a Freepik (documento nº 3) donde figura una relación de accesos y direcciones IP, protocolo de notificación de brechas de seguridad (documento nº 2), Informe Registro de Incidencia. Análisis de Riesgos (documento nº 4).

TERCERA NOTIFICACIÓN:

Con fecha ******FECHA.3*** se recibe una nueva notificación de ampliación de la información anterior en la que se pone de manifiesto que, con fecha 18 de junio de 2020, Freepik recibe correos electrónicos, del mismo u otro atacante, que asegura haber detectado una vulnerabilidad en el código de la página web ******URL.2***, página titularidad de Freepik, que le ha permitido acceder a datos personales de usuarios de la web y se ofrece, a cambio de una recompensa, a solucionar la vulnerabilidad.

Freepik, el 26/06/2020 verifica que efectivamente existe una inyección de SQL en el código de la web ******URL.2*** a través de la cual se ha accedido a las direcciones de correo electrónico de usuarios.

Freepik manifiesta que se desconoce la fecha en la que se inyectó el código malicioso, pero se han detectado accesos a través de la URL afectada desde el 09/02/2020 hasta el 28/05/2020.

En total, se calcula que podrían haberse comprometido 8.310.630 cuentas de usuarios, de las cuales:

- Con acceso exclusivo a la dirección de correo electrónico: se calcula que el hacker ha podido obtener acceso 4.535.716 cuentas, ya que estas cuentas de usuario tienen contraseña federada con Google o Facebook;

- Acceso a la dirección de correo electrónico y al hash de la contraseña: se calcula que el Atacante ha podido tener acceso a la dirección de correo electrónico y hash de 3.774.914 cuentas, de las cuales: 3.545.677 presentan un cifrado y 229.237 presentan también un cifrado con un tipo diferente.

Freepik considera que hay indicios para entender que este incidente está relacionado con la brecha de seguridad notificada inicialmente por Freepik a la Agencia con fecha ******FECHA.1***, complementada por medio de notificación adicional de fecha ******FECHA.2***, ya que los accesos detectados del hecker coinciden sustancialmente con las fechas del incidente anterior.

En esta notificación se adjuntan los siguientes documentos:

- Medidas preventivas aplicadas antes de la brecha.

- Medidas tomadas para solucionar la brecha y minimizar el impacto sobre los afectados.

CUARTA NOTIFICACIÓN:

Con fecha ******FECHA.4*** se recibe una nueva notificación de ampliación de la información de la brecha notificada el ******FECHA.3*** sobre la web ******URL.2***, en la que se informa sobre los resultados de la compañía de seguridad contratada para el estudio de la brecha (empresa de ciberseguridad israelí según documento aportado por Freepic) y consideran que el atacante es el mismo en ambas brechas de seguridad, aportando copia de un correo remitido por "*HACK MAN***"** en el que les informa que acaba de encontrar vulnerabilidad en dos nuevas bases de datos, recibido por la empresa el 19 de junio.

En la documentación aportada por Freepik se desprende lo siguiente:

<u>En relación con la brecha de la web</u> ******URL.1***:

La entidad ha aportado Registro de Incidencias y Análisis de Riesgo donde figura:

- La brecha fue detectada el 18 de mayo de 2020 y estiman que el inicio de la misma pudo producirse el 15 de mayo de 2020.

- El 18 de mayo recibieron un correo del hacker en el que se exige el pago para no publicar en la *dark web* información sobre 500.000 usuarios de la web de ******URL.1***.

- El hacker remite un listado con 30.000 direcciones de correo electrónico de las cuales 23.704 corresponden a usuarios de la web.

- Después de cotejar más de dos millones de direcciones de correo electrónico y contraseñas han detectado 171.280 contraseñas expuestas en la *dark web.*

- Respecto de los datos afectados: credenciales de acceso y datos identificativos de clientes, usuarios y suscriptores.

- Con anterioridad a la brecha, la entidad disponía de las siguientes medidas:

    - Todas las contraseñas que introducen los usuarios se almacenan *hasheadas* lo que hace prácticamente inviable el acceso ni siquiera por fuerza bruta.

- Se incentiva el uso de "*login sociales*", por Google / Facebook / Twitter, que hace que las credenciales en ningún momento se almacenen en Freepik.

- Se monitoriza el uso "*atípico"* de las cuentas para detectar casos en los que un atacante se hace con el control de una cuenta y la usa para descargar masivamente contenido en Freepik.

- Medidas posteriores implantadas:

  - Limitación del número de pruebas de acceso por minuto que se puede hacer de una contraseña, para dificultar pruebas masivas.

  - Eliminación de la posibilidad de conocer si un email pertenece a un usuario registrado si no se conoce también la contraseña.

  - Integración de un *Captcha* de Google en el proceso para dificultar pruebas de usuario y contraseñas de forma automatizada.

  - Análisis de la posibilidad de incluir en el futuro un proceso de 2 Factor Autenticación.

  - Se han establecido medidas de seguridad que no permiten que los usuarios empleen contraseñas que figuren en el listado del *"1.000.000 contraseñas más comunes"*.

  - Se han implantado medidas de seguridad que no permiten el uso de contraseñas empleadas anteriormente por ese mismo usuario en Freepik.

  - Fomento del empleo por parte de los usuarios de identidades federadas.

- Freepik manifiesta que según el Análisis de Riesgo previsto en la Guía para la notificación de brechas de seguridad publicado por la Agencia, no es necesario comunicar a los afectados.

En relación con la brecha de la web ******URL.2***:

Freepik ha aportado (en su última notificación de brecha) informe realizado por la empresa de ciberseguridad contratada al efecto en el que figura:

- El 18 de junio de 2020, Freepik recibió mails de un atacante *"**XXXXXXXX**"* informando de la existencia de una puerta trasera y vulnerabilidades en los servicios que le habían permitido acceder a datos personales de los usuarios y ofreciendo la posibilidad de solucionarlo a cambio de una retribución.

- El 26 de junio se confirma la existencia de una inyección de SQL a través de la cual se había tenido acceso a direcciones de correo electrónico de los usuarios.

  Desconocen la fecha en que se produjo la inyección de SQL pero tiene constancia de accesos a través de la URL comprometida desde el 9 de febrero al 28 de mayo de 2020.
- El 30 de junio contrataron a la empresa de ciberseguridad para la realización de un análisis forense y tomar las medidas necesarias.

- Se calcula que podrían haberse comprometido 8.310.630 cuentas de usuarios, de las cuales:

o Con acceso exclusivo a la dirección de correo electrónico el hacker ha podido obtener dirección de correo de 4.535.716 cuentas, ya que estas cuentas de usuario tienen contraseña federada con Google o Facebook

o Con acceso a la dirección de correo electrónico y al hash de la contraseña: se calcula que el hacker ha podido obtener tener acceso a la dirección de correo electrónico y hash de 3.774.914 cuentas.

o Han comunicado la brecha a los afectados por mail con tres tipos de comunicaciones:

  - Grupo 1. Afectados que solo se ha comprometido la dirección de correo electrónico y no requiere ninguna acción por parte del usuario.

  - Grupo 2. Afectados a los que se ha visto comprometida la dirección de correo y el *hash* de la contraseña informando que deben cambiar la contraseña facilitando un enlace para ello.

  - Grupo 3. Afectados a los que se ha visto comprometida la dirección de correo y el *hash* de la contraseña con un encriptado

diferente se les informa que pueden crear una contraseña si lo creen conveniente facilitando un enlace para ello.

- Consideran que es el mismo atacante que el de la brecha anterior y aportan copia de un correo electrónico que manifiestan haber recibido el 19 de junio de 2020 donde les informa que ha encontrado una nueva vulnerabilidad que atañe a dos bases de datos.

  Asimismo, aportan mensajes mantenidos con un atacante *(****EMAIL.1)* el 25 de febrero y del 9 de mayo al 19 de junio en el cual se interesa de la posibilidad de revender el contenido.

  Freepik ha detectado, después de estudiar los *logs,* que el 10 de febrero se terminó una descarga pequeña de direcciones de correo y hash de contraseñas y el 28 de mayo finaliza una tercera descarga.

  En los mensajes del 11 de mayo al 6 de junio remite mensajes amenazantes y el 21 de mayo se comienzan los mensajes con la empresa de ciberseguridad.

  - Las Medidas implantadas con anterioridad a la brecha son las mismas que las tomadas con la brecha descrita anteriormente.

Respecto de las medidas implantadas con objeto de minimizar el impacto y resolver ambas incidencias se adjunta en un anexo ya que están catalogadas como confidenciales.

Freepik ha aportado los siguientes documentos:

- Notificación de brechas de seguridad (Protocolo nº1 RGPD- documento 2)
- Protocolo de notificación de brechas.
- Análisis de Riesgos de la brecha.

Freepik manifiesta que han implantado las siguientes medidas con posterioridad las brechas:

- Aplicación de los procedimientos de gestión de ciberseguridad en todos los procesos comerciales de la entidad.
- Sistemas de concienciación y formación a empleados.
- Seguimiento, análisis y mejora continua de aplicación es infraestructuras.
- Incorporación de prácticas de desarrollo seguro en ciclos vitales.

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 una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad, como consecuencia del acceso indebido por terceros ajenos a la base de datos de Freepick.

De las actuaciones de investigación se desprende que Freepik disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Asimismo, Freepik ha afrontado de forma diligente la identificación, contratación con una empresa de ciberseguridad, corrección de la brecha, análisis y clasificación del supuesto incidente de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, minimizar el impacto, comunicar a los afectados e implementar nuevas medidas razonables y proporcionales para evitar que se repita la supuesta incidencia en el futuro.

En consecuencia, Freepik disponía de forma previa de medidas técnicas y organizativas razonables y proporcionales en función del nivel de riesgo para evitar este tipo de incidencia.

No constan reclamaciones ante esta AEPD por parte de los clientes afectados.

Por último, cabe señalar que la documentación generada de todo el proceso de detección, contención, respuesta, recolección y custodia de evidencias ante una posible brecha de seguridad de los datos personales es importante de cara a comunicaciones a las posibles partes interesadas tanto de carácter interno o externo, y para la elaboración de un informe final que tras su análisis permita extraer conclusiones. Este informe final, elaborado tras el seguimiento y cierre de este tipo de incidentes y su impacto, es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos futuros. El uso de esta información servirá para prevenir la reiteración de hechos similares.

III

En el presente caso, la actuación de Freepik como entidad responsable del tratamiento, ha sido razonable y proporcional con la normativa sobre protección de

datos personales e implantó nuevas medidas de seguridad proporcionales al riesgo evaluado para evitar la repetición de incidentes similares en el futuro.

IV

Por lo tanto, se ha acreditado que la actuación de la investigada como entidad responsable del tratamiento ha sido adecuada y proporcional 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 FREEPIK COMPANY, S.L, con CIF B93183366 y domicilio en C/ ******DIRECCIÓN.1, ***LOCALIDAD.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