- **Procedimiento Nº: E/01823/2020**

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 investigación se inician por la notificación de quiebra de seguridad de datos personales remitidos por la entidad VIÑARAS PREMIUM, S.L., con NIF B45884210 (en adelante Grupo Viñaras), en el que informan a la Agencia Española de Protección de Datos que el 2 de octubre de 2019, al acceder a la aplicación utilizada para realizar el trabajo, la estructura de ficheros alojados en el mismo servidor no funcionan y se comprueba que han sido cifrados por completo.

**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 quiebra: 30 de septiembre de 2019

### ENTIDADES INVESTIGADAS

VIÑARAS PREMIUM, S.L., con NIF B45884210 y domicilio en Crta. Madrid Toledo, Km. 63,200 de Olías del Rey (Toledo).

### RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 12 de noviembre de 2019 se requiere información a la entidad notificante de la quiebra, de la que se desprende lo siguiente:

   Respecto de la cronología de los hechos

   - El lunes 30.09.2019, al llegar los primeros trabajadores a la empresa 8:00, se dan cuenta de que la aplicación utilizada para realizar el trabajo (Quiter) y la estructura de ficheros alojados en el mismo servidor, no funcionan.

     Se accede al servidor y se comprueba que ha sido cifrado por completo.

     Se aísla (desconexión de la red) dicho servidor y se comprueba si hay más equipos afectados y se realiza la misma acción.

   - Mediante consenso de los responsables y tras valorar el impacto en la empresa, se decide adquirir un nuevo servidor para poder empezar a trabajar con normalidad lo antes posible con un servidor que no haya sido vulnerado.

A su vez, se decide formatear todos los equipos de la empresa, puesto que han estado expuestos a la infección y es posible que tengan alguna “puerta abierta” que facilite otro ataque.

- El miércoles 23.10.2019 se retoma la actividad de la empresa, trabajando ya bajo el servidor nuevo.

Respecto de las causas que han hecho posible la incidencia

A partir del jueves 19.09.2019 se detecta que se está recibiendo una oleada de emails con documentos adjuntos en forma de documentos Word que enmascaran troyanos, puesto que, al abrirlos, no se abría nada. Dichos emails, llegan utilizando nombres de remitentes conocidos y redactados con textos que bien te hacen creer que estas tratando con clientes o proveedores habituales.

Al informar de la apertura de los documentos adjuntos al departamento de informática, se advierte que la dirección del remitente no coincide con la de la persona/empresa de contacto verídica. Se procede a aislar dicho ordenador de la red y se somete a un análisis profundo y limpieza del mismo. En prevención, también se procede a avisar al resto de compañeros de la empresa de dicha oleada y que extremen la precaución.

El lunes 23.09.2019, se advierte que están llegando emails utilizando el nombre de la persona que abrió el primer email falso el jueves anterior. Se procede a formatear dicho equipo y a cambiar la contraseña del correo.

En esa semana, con las personas que también abrieron dichos correos maliciosos, se realizó el mismo protocolo. Pese a las advertencias, hubo más casos de aperturas de dichos emails no notificados al departamento correspondiente y por lo tanto, infectados y exponiendo al resto equipos de la red.

Respecto de la categoría de los datos afectados

Los tipos de datos afectados es muy amplia, ya que todos los documentos y archivos contenidos en el servidor y equipos afectados, quedó encriptado.

Datos de clientes y empleados, básicos, de contacto, económicos financieros, identificativos y de localización.

Respecto de las acciones tomadas para minimizar la incidencia

Desde el jueves 19.09.2019 que se conoció el primer caso, se procedió al aislamiento y limpieza del equipo con antivirus y antispyware. También se pone en conocimiento de la empresa que gestiona el servicio del email de dicha aleada y se les envía en documento que viene adjunto en los emails en forma de documento Word.

Según se fueron conociendo los casos siguientes, el procedimiento fue el mismo con todos los equipos de los que el departamento iba teniendo conocimiento.

Al conocer la recepción de emails utilizando los nombres de nuestros compañeros, se procede a cambiar las contraseñas de los emails y a formatear dichos ordenadores.

Respecto de la resolución final de la incidencia

Tras tomar la decisión de no volver a utilizar el servidor comprometido, se adquiere un nuevo servidor donde volver a montar, con total confianza de no tener puertas abiertas, todo el sistema para el correcto funcionamiento de la empresa, eliminando las posibles brechas de seguridad que se habían detectado en el anterior, como puede ser el tener las conexiones remotas habilitadas.

Una vez recibido el nuevo servidor (11.10.2019), se instala el S.O. y se configura acorde a las necesidades de la empresa.

Se contacta con la empresa responsable de Quiter Autoweb para la instalación de la aplicación y se restaura la copia de datos.

Los equipos clientes, tras el cambio de disco, también son configurados con todas las medidas posibles para evitar otro posible ataque.

Miércoles 23.10.2019, se retoma la normalidad.

Utilización por terceros de los datos personales obtenidos a través del ataque

Una vez revisados los sistemas de Información, se determina que no ha existido modificación y/o supresión alguna respecto de los datos existentes.

No se tiene conocimiento de ningún tipo de uso de datos por parte de un tercero. Nadie se ha puesto en contacto con la entidad al respecto ni tampoco han aparecido los datos en ningún tipo de indexación por buscadores.

Procedimiento establecido ante brechas de seguridad

El procedimiento establecido ante brechas de seguridad consiste en notificar a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales.

Política de seguridad

Se ha contratado a una empresa externa para el mantenimiento y seguridad de los sistemas informáticos incorporándose antivirus (Panda) que permiten incrementar las medidas de seguridad del sistema

El mantenimiento de los sistemas de información corre a cargo del propio departamento de informática de la empresa, al cual, se le tuvo en cuenta, en todo momento, para la toma de las decisiones oportunas para que el impacto fuese el menor posible.

Aportan copia del Registro de Actividad de los tratamientos donde se ha producido el ataque, en el que figuran los siguientes tratamientos:

- Tratamiento: Clientes. Finalidad: gestión de la relación con los clientes.
- Tratamiento: Empleados. Finalidad: gestión de la relación laboral con los empleados.
- Tratamiento: Candidatos. Finalidad: gestión de la relación con los candidatos a un empleo en la empresa.

- Tratamiento: Proveedores. Finalidad: gestión de la relación con los proveedores.

No aportan información sobre el análisis de riesgos de los tratamientos, aunque se aporta copia del documento de seguridad diseñado para tratamientos de datos personales de bajo riesgo.

## 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 quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una posible brecha de disponibilidad, como consecuencia del encriptado de la información residente en el sistema de información del Grupo Viñaras.

De las actuaciones de investigación se desprende que la entidad Grupo Viñaras disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo bajo, dada la categoría de datos tratados.

Asimismo, la entidad Grupo Viñaras disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, 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 e implementar nuevas medias razonables y oportunas para evitar que se repita la supuesta 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.

No constan reclamaciones ante esta Agencia de los afectados.

En consecuencia, consta que la entidad Grupo Viñaras disponía de forma previa de medidas técnicas y organizativas razonables, en concreto prevención a ataques

mediante el uso de sistemas de *fuerza bruta,* en función del nivel de riesgo para evitar este tipo de incidencia. No obstante, se recomienda la realización de un informe final sobre el incidente notificado. 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 ahora analizada.

**III**

Por lo tanto, se ha acreditado que la actuación de Grupo Viñaras 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 VIÑARAS PREMIUM, S.L., con NIF B45884210, y domicilio en Crta. Madrid Toledo, Km. 63,200 de Olías del Rey (Toledo).

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