- **Procedimiento Nº: E/11546/2019**

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 por la recepción de un escrito de notificación de brecha de seguridad de datos personales remitido por el Delegado de Protección de Datos de la entidad NISA NUEVAS INVERSIONES EN SERVICIOS, S.A., con NIF: A46036984 (en adelante NISA) en el que informan a la Agencia Española de Protección de Datos (en adelante AEPD) que sobre las 23 horas del día 22/11/2019, el personal de sistemas que se encontraba de guardia, ubicado en un hospital de Valencia, recibe aviso de incidencia detectada por el servicio de diagnóstico por imagen. Tras analizar la incidencia verifican que afecta al servidor de radiología centralizada, comprobando que algunos archivos necesarios para la ejecución del servicio están encriptados y/o renombrados con extensión “ryk”, afectando a otros servidores de otras ocho entidades sanitarias/hospitalarias.

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: 25 de noviembre de 2019

ENTIDADES INVESTIGADAS

NISA NUEVAS INVERSIONES EN SERVICIOS, S.A., con NIF A46036984 y con domicilio en AVENIDA VALLE DE LA BALLESTERA, NUM 59 - 46015 VALENCIA (VALENCIA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 14 de enero de 2020 se requiere información a NISA y de la respuesta recibida con fecha 4 de febrero de 2020 se desprende lo siguiente:

    1.1. Los sistemas del Grupo Nisa están instalados en un Centro de Procesamiento de Datos ("CPD") propiedad del Grupo empresarial Nisa, situado en Alcalá de Henares (Madrid) y gestionado por Telefónica de España (en adelante Telefónica). Días antes de ocurrir el incidente, se había formalizado un nuevo contrato de migración de los servidores con el mismo proveedor, sin embargo, las labores de migración no se habían iniciado cuando ocurrió la incidencia.

    1.2. El alcance la Brecha de Seguridad de datos personales notificada el 25 de noviembre de 2019 se extiende a varias entidades del Grupo. Se ha detectado

que el ciberataque afectó a otros tratamientos no identificados de inicio, siendo éstos referidos a la aplicación de gestión de Nóminas de los empleados de los centros afectados (Programa Meta4) y el fichero en el que se alojaban la recogida de huella de los empleados, medio que se había seleccionado para cumplir con la obligación legal del control de la jomada laboral.

En relación con la aplicación de gestión de nóminas (Meta4), el ataque del virus *ransomware* provocó la pérdida de información de nóminas de los meses de octubre y noviembre, no obstante, se recuperó la totalidad de la información, bien a través de las copias de seguridad, bien generando de nuevo la información de forma manual. Por otro lado, desde enero de 2020, el sistema Meta4 se ha dejado de utilizar, manteniéndose a los únicos efectos de la obligación de conservar los datos por los plazos legalmente establecidos.

En cuanto a los datos biométricos de huella dactilar, no son los relativos al patrón completo de la huella dactilar de los empleados, sino que la información consiste únicamente en un identificador único generado a partir de la aplicación de un algoritmo de cifrado sobre determinadas posiciones de la huella dactilar, siendo por tanto imposible la reconstrucción de la huella dactilar a partir de la información tratada.

La afección del virus *ransomware* se ha limitado al cifrado de la información anteriormente citada, dejando la misma inutilizable.

Manifiestan que no ha habido filtración de datos a terceros ajenos, limitando el impacto sobre los interesados (empleados) únicamente al inconveniente de la nueva recogida de los datos.

Respecto de la cronología de los hechos

1.3. Sobre las 23 horas del día 22/11/2019, el personal de sistemas que se encontraba de guardia, ubicado en el hospital Valencia, recibe aviso de incidencia detectada por el servicio de diagnóstico por imagen. Tras analizar la incidencia verifican que afecta al servidor de radiología centralizada, comprobando que algunos archivos necesarios para la ejecución del servicio están encriptados y/o renombrados con extensión “ryk”, afectando a otros servidores que afectan a las otras sociedades del Grupo.

Al momento de notificar la brecha de seguridad a la AEPD, la infección del virus había sido neutralizada y los servidores protegidos. Asimismo, se habían iniciado medidas adicionales para evitar el contagio de nuevo por ese virus, u otros virus similares, en los servidores y la mayor parte de los equipos del Grupo.

Respecto de las causas que han hecho posible la incidencia

1.4. La causa por la que el ataque consiguió atravesar las medidas de seguridad establecidas se debe a la ejecución de un archivo adjunto a un correo electrónico malicioso (que no fue bloqueado por el servicio de correo limpio) en uno de los equipos de la red, abriendo paso al virus tipo *ransomware*, que se fue desplazando lateralmente por los equipos conectados a la misma red y, una vez alcanzada la propagación suficiente, ejecutó un software de encriptación de los archivos.

Número de clientes afectados por la incidencia.

1.5. Se ha ido recuperando de manera paulatina gran parte de la información afectada y se ha reanudado inmediatamente la actividad ordinaria, bien mediante la recuperación de los sistemas o mediante el uso de procesos analógicos en caso contrario.

Tipología de datos afectados.

1.6. Los datos afectados hacen referencia a dos categorías de interesados: Clientes/pacientes y Empleados. En el caso de Clientes/pacientes, los datos afectados son relativos a la identidad y datos de salud (Historia y Documentación Clínica), mientras que, en el caso de Empleados, los datos afectados son los relativos a identidad, detalles de la nómina y datos biométricos (patrón de identificación elaborado a partir de posiciones parciales de la huella dactilar).

Respecto de si se tiene conocimiento de la utilización por terceros de los datos personales obtenidos a través del ataque

1.7. Una de las primeras medidas que se tomaron, además de aislar los servidores para detener la propagación y eliminar la amenaza, fue la de analizar el tráfico de red de las 48 horas anteriores al incidente de los servidores afectados constatándose que no hubo tráfico sospechoso. Se amplía este análisis revisando el tráfico de red desde el 10/07/2019 no detectándose tráfico sospechoso, descartando por tanto la filtración de información a terceros ajenos.

Respecto de las acciones tomadas con objeto de minimizar los efectos

1.8. En relación con la solución de la incidencia, se contactó inmediatamente con Telefónica para recurrir a sus servicios expertos en materia de ciberseguridad y resolución de ciberincidentes.

Una vez contenida la propagación del virus, para recuperar la disponibilidad de los sistemas y protegerlos frente a futuros ataques se tomaron las siguientes medidas:

- Contratación de un servicio de conexión remota para retomar la actividad en determinados servicios que lo requerían (por ejemplo, radiología o laboratorio). Aportan copia de la oferta y autorización interna por el director general.
- Contratación de un nuevo y más amplio servicio de correo limpio y antispam con Telefónica. Aportan contrato y aceptación de este por correo electrónico.
- Actualización continua del firewall para incluir el listado de servidores maliciosos recomendado por el CCN-CERT y posteriores actualizaciones, previniendo el contagio de virus conocidos.

- Contratación de otro sistema de seguridad con antivirus, antispyware, firewall, control de aplicaciones y prevención de intrusos que protege los servidores y máquinas mediante aprendizaje inteligente, que además de detectar amenazas conocidas, detecta comportamientos anormales en las máquinas conectadas al sistema de seguridad, alertando de las anomalías e incluso deteniendo los procesos en los que se detectan comportamientos anormales que puedan evidenciar un ataque informático.
- Contratación de servicios ad-hoc con los proveedores para el restablecimiento de los sistemas de gestión documental y diagnóstico por la imagen afectados por el ataque, y la implantación de una solución alternativa en tanto se recuperaba la operativa ordinaria. Aportan los contratos con ambos proveedores.

Respecto de las acciones tomadas para la resolución final de la incidencia

1.1. La operativa afectada por la indisponibilidad de los sistemas que sufrieron el ataque se encuentra restaurada, bien por la recuperación de la funcionalidad de los sistemas, bien por la sustitución de dicha operativa con procesos analógicos, en tanto se reestablece la funcionalidad de los escasos sistemas que se encuentran todavía inoperativos.

Respecto de la notificación realizada a los clientes afectados.

1.2. Debido a (i) el elevado número de potenciales afectados (en torno a los dos millones); (ii) la imposibilidad material de determinar cuáles de los potenciales afectados habían sufrido efectivamente las consecuencias del ataque (pérdida de disponibilidad de información clínica); (iii) el esfuerzo desproporcionado que hubiese supuesto contactar con todos ellos de manera individual, ya que no solo no estaban identificados de manera concreta los afectados, sino que la forma de contactar hubiese diferido entre unos y otros, al no contar en todos los casos con la dirección de correo electrónico, suponiendo el correo postal un esfuerzo notablemente mayor; y (iv) la inexistencia de acciones que los interesados hubiesen podido realizar de cara a mitigar las consecuencias del ataque, dada la naturaleza del ataque (un virus informático que afecta a los sistemas centrales de la entidad encriptando la información), se consideró como la mejor y más eficiente opción la de una comunicación pública utilizando como medios las diferentes páginas web de los centros afectados.

Respecto de la seguridad de los tratamientos de datos con anterioridad a la incidencia de seguridad

1.3. Aportan la siguiente documentación:

- Registro de Actividades de los tratamientos afectados de cada una de las sociedades.
- Evaluación Impacto sobre el tratamiento identificado como "Prestación de la asistencia sanitaria y gestión, custodia y archivo de la Historia Clínica".
- Evaluación Impacto sobre el tratamiento identificado como "Atención de solicitudes de Historia Clínica / Informes / Resultados".
- Evaluación Impacto sobre el tratamiento identificado como "Control de la jornada laboral".

- Análisis de Riesgos y necesidad de EIPD del tratamiento identificado como "Nóminas".
- Documento de Seguridad y Anexos al Documento de Seguridad.

Se encuentra en proceso de desarrollo una nueva política de medidas de seguridad que recoja las novedades introducidas por el RGPD y aúne y homogeneice todas las prácticas, estándares, medidas y procedimientos de las distintas entidades que han ido incorporándose a raíz de su crecimiento en los últimos años, cada una de ellas con un sistema de cumplimiento propio en materia de protección de datos y seguridad de la información.

No obstante, sí existen numerosas medidas de seguridad implantadas en el Grupo Nisa señaladas en el Documento de Seguridad y otras.

En relación con el procedimiento de gestión y notificación de brechas de seguridad, continua vigente el procedimiento existente con anterioridad a la aplicación del RGPD pero se está trabajando desde hace meses en un nuevo procedimiento en línea con las novedades introducidas por el citado Reglamento.

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."*

El artículo 33 del RGPD señala lo siguiente:

"Notificación de una violación de la seguridad de los datos personales a la autoridad de control

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.

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 el presente caso, consta una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de disponibilidad, como consecuencia del encriptado de la información residente en el sistema de información del Grupo empresarial NISA.

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

Asimismo, Grupo empresarial NISA 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 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 personas afectadas.

Asimismo, consta la comunicación a los interesados conforme dispone el art 34.3.c) del RGPD.

En consecuencia, consta que el Grupo empresarial NISA disponía de forma previa de medidas técnicas y organizativas razonables en función del nivel de riesgo para evitar este tipo de incidencia. No obstante, se recomienda a las entidades afectadas del Grupo empresarial NISA 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 del Grupo empresarial NISA en calidad responsable del tratamiento ha sido acorde y proporcionada 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 NISA NUEVAS INVERSIONES EN SERVICIOS, S.A., con NIF A46036984 y con domicilio en AVENIDA VALLE DE LA BALLESTERA, NUM 59 - 46015 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.

Mar España Martí
Directora de la Agencia Española de Protección de Datos