**Procedimiento Nº: E/06179/2019**
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:** Con fecha 6 de junio de 2019, TELEFÓNICA SEGUROS SUCURSAL EN ESPAÑA con NIF: W0182798I (en adelante TELEFÓNICA) noticia a la Agencia Española de Protección de Datos que han tenido conocimiento de la posible desaparición de cintas de *backup* que debían ser custodiadas por la empresa de seguridad G4S de Luxemburgo. Las cintas contienen datos personales y éstos pueden ser accesibles. Se estima que la brecha de seguridad se produjo el 11 de marzo de 2019. TELEFÓNICA también ha remitido notificación de la violación de seguridad a la Autoridad de Control de Luxemburgo.

**SEGUNDO:** Con fecha 18 de junio de 2019, la Directora de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos a que procediera a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

### ENTIDADES INVESTIGADAS

***TELEFÓNICA SEGUROS SUCURSAL EN ESPAÑA con NIF W0182798I con domicilio en RONDA DE LA COMUNICACIÓN S/N. EDIFICIO OESTE 2, NUM 0, PISO 2 - 28050 MADRID (MADRID)***

### RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 25 de junio de 2019 se requiere información a TELEFÓNICA y de la respuesta recibida en fecha 9 de julio de 2019 se desprende:

Respecto de la empresa

- La Societé Altaïr Assurances SA et les filiales du Groupe Teléfonica tienen suscrito un contrato con la sociedad STERIA PSF LUXEMBOURG SA (en adelante SOPRA-STERIA) para, entre otros, la realización de copias de respaldo (*backups*) en cintas magnéticas.
- TELEFONICA INSURANCES, S.A. tiene suscrito un contrato con G4S SECURITY SOLUTIONS (en adelante G4S) para el transporte y conservación mediante maletas especiales de documentos informáticos recuperables.
- Mensualmente SOPRA-STERIA se desplaza a los locales de TELEFÓNICA INSURANCE, S.A. en Luxemburgo y realiza las cintas de *backups*.

Finalizado el proceso, el segundo lunes del mes, G4S recoge en las oficinas de TELEFÓNICA INSURANCE, S.A. un maletín con las cintas y los transporta a un depósito de seguridad para su custodia.

TELEFÓNICA ha aportado copia de los contratos con las empresas mencionadas y copia del procedimiento establecido para el transporte de los *backups.* En este procedimiento se incorporan las medidas de seguridad adoptadas en el transporte y el registro de las cintas.

Respecto de la cronología de los hechos.

- El 15 de mayo de 2019, TELEFÓNICA requiere a G4S uno de los maletines (número 1394) donde se guardan los *backups* con el fin de actualizarlos y volverlos a transportar al depósito de seguridad. Tras varias comunicaciones requiriendo el maletín, el 6 de junio de 2019, se solicita información a G4S confirmándose la pérdida del maletín.

En paralelo, se requiere a SOPRA-STERIA información del contenido exacto de las cintas que incluía el maletín.

- El 4 de junio de 2019, se solicita a SOPRA-STERIA que informe sobre la posibilidad de que las cintas de *backups* pudiesen ser leídas por un tercero y la empresa indica que en ningún caso es posible acceder al contenido de por un tercero. No obstante, el día 6 de junio de 2019, informan de que es posible que alguna información (correos electrónicos) pudieran llegar a ser accesibles y legibles por un experto.
- El 6 de junio de 2019 proceden a notificar la posible brecha de seguridad a la Agencia Española de Protección de Datos y a la Autoridad de Protección de Datos de Luxemburgo. Posteriormente, con fechas 13 y 16 de junio de 2019, se notifica a las Autoridades del Reino Unido y de Alemania.
- El 7 de junio de 2019 se recoge un duplicado de las cintas para un análisis forense que lo realiza una empresa independiente LAZARUS COMPUTER FORENSIC.
- Con fecha 2 de julio de 2019, G4S emite el informe definitivo sobre la pérdida del maletín, donde indica que parece improbable que su desaparición venga derivada de un comportamiento interno o externo malicioso. En el informe aportado también se indica que las cámaras de seguridad del muelle de carga/descarga no han registrado ninguna incidencia aunque las imágenes del día 11 de mayo no se han podido examinar al haber pasado más de 30 días.

TELEFÓNICA ha aportado copia de las actuaciones realizadas con G4S (correos electrónicos intercambiados y visitas a la empresa) desde el 13 de mayo hasta el 7 de julio de 2019 respecto del incidente. En una de las visitas se verificaron las medidas de seguridad.

TELEFÓNICA ha aportado copia de las comunicaciones mantenidas con SOPRA-STERIA desde el 13 de mayo hasta el 7 de julio de 2019 respecto del incidente. Asimismo, ha aportado un correo electrónico remitido por SOPRA-STERIA el 8 de julio donde se informa de que se han perdido 21 cintas de *backups* correspondientes a diversos *backups* mensuales de los años 2019, 2018, 2017, 2016 y 2015. En dicho informe también se indica que estas cintas no estaban encriptadas y contienen

imágenes de las máquinas virtuales. No obstante, estaban protegidas contra el *malware* criptográfico.

Respecto de los datos afectados

- Las cintas de *backups* contienen información de los servidores de correo y ficheros de la oficina de TELEFÓNICA en Luxemburgo (concretamente, correos electrónicos y hojas Excel con información de clientes y empleados relacionados). En dichos servidores existen aproximadamente datos personales de:
    - 15.600 afectados en España
    - 10.600 afectados en Reino Unido
    - 250 afectados en Alemania
    - 40 afectados en Luxemburgo
- La categoría de los datos afectados es la siguiente:
    - Clientes: nombre, apellidos, dirección de correo electrónico, dirección postal, número de DNI. En algunos casos se incluye fotocopia de DNI y cuenta bancaria.
    - Empleados y directivos: nombre, apellidos, DNI (fotocopia), cuenta bancaria, dirección postal, contrato de trabajo, contrato de seguro de salud, contrato de plan de pensiones.
- TELEFÓNICA considera que los datos sensibles pueden estar en el contenido de los correos electrónicos por lo que han procedido a revisar un total de 6.694 correos (quedando pendientes aproximadamente 500) y han detectado datos de salud en 14 de ellos, fotocopias de DNI en 144 casos, datos bancarios en 47 y fotocopias del DNI junto con datos bancarios en 20 casos.
- TELEFÓNICA, después de realizar un análisis de los hechos y valoración del riesgo, concluye que existen varios tipos de afectados en función de la naturaleza de los datos comprometidos: afectados con datos de contacto básicos, afectados con fotocopia de documento de identidad, afectados con número de cuenta corriente, afectados con ambos tipos de datos y afectados con datos de salud.

Por ello, la notificación individual se va a realizar a las personas potencialmente afectadas cuyos datos comprometidos hayan sido la fotocopia del DNI o el número de cuenta y aquellos cuyos datos comprometidos tengan que ver con la salud.

- El Equipo de Respuesta ante Incidencias de Seguridad Informáticas (*Computer Security Incident Response Team -CSIRT-)* del Grupo Telefónica en España y Reino Unido (*Cyber Emergency Response*), ha procedido a realizar una monitorización continua con el fin de detectar información sobre el eventual tráfico de dichos datos en Internet, en la *deep web* y en la *dark web*, sin que hasta la fecha haya aparecido evidencia alguna en este sentido. Se indican también todas las áreas de monitorización incluidos los posibles grupos de *hackers*.

TELEFÓNICA manifiesta que la permanente vigilancia sobre estos espacios de tráfico de información permitiría activar un protocolo con el fin de reforzar el proceso de notificación a los interesados para mitigar inmediatamente el impacto que sobre los mismos pudiera potencialmente tener el incidente.

Respecto de las acciones tomadas para minimizar el impacto sobre los afectados

- Desde el día 10 de junio, fecha en la que se puso a disposición de la empresa LAZARUS COMPUTER FORENSIC los *backups,* no se ha conseguido recuperar la información debido "*en buena medida por la utilización de compresión en el proceso de la copia, de la obsolescencia de los equipos de backup utilizados en origen y de la dificultad de identificar el software de recuperación idóneo para la misma*". Además, los buzones de la aplicación de correo electrónico se encuentran protegidos con usuario y contraseña.

TELEFÓNICA ha aportado copia del informe emitido por LAZARUS COMPUTER FORENSIC en el que se indica, entre otras las siguientes conclusiones:

o La tecnología de las cintas es obsoleta.

o En las cintas no se indica el tipo de lector compatible. Y para acceder a los datos los dispositivos deben tener su versión exacta.

o Las cintas están comprimidas.

o No se ha podido restaurar.

o La complejidad para acceder a los datos almacenados es muy alta. Se necesita hardware y software especializado así como profundos conocimientos en informática forense.

o En el caso de contar con los dispositivos adecuados y los conocimientos suficiente de informática forense solo se podría acceder a datos parciales en el plazo de al menos dos semanas y los datos obtenidos no son manejables.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- Respecto del transporte de los maletines

Según se encuentra establecido en el protocolo de transporte, todos los meses la entidad SOPRA-STERIA, en los locales de TELEFÓNICA, realiza los *backups* en cinta de la información que se encuentra en los servidores.

Un determinado día del, G4S recoge las cintas, que SOPRA-STERIA ha dejado para su recogida en los locales de TELEFÓNICA la cual ha remitido un correo electrónico a G4S con copia a SOPRA-STERIA indicando los números de maletines que se deben recoger.

El empleado de G4S debe cumplimentar un formulario donde figura el número de maletín, el sello que ha puesto TELEFÓNICA en el envío y el sello que tenía el maletín en la recogida. Además, en el maletín figura el nombre de TELEFÓNICA. (G4S realiza la recogida y la devolución de los maletines).

El empleado de G4S es el encargado de transportar los maletines en el coche de la compañía.

- Respecto de la recepción de los maletines

El vehículo con los maletines se traslada a un espacio de carga/descarga (*bunker)* de G4S custodiado por Guardias de Seguridad para su entrega al empleado de G4S encargado de la recepción. Solo puede permanecer en bunker la descarga de un cliente no pudiéndose solapar con la descarga de otro cliente.

Los maletines se custodian en una Área determinada de la entidad (Data Storage room). Solo el personal de la empresa que trabaja en el área de Alto Riesgo (High Risk zone) puede acceder al área de custodia para depositar o recoger los maletines.

Los maletines se transportan en unos carros por empleados de la entidad.

Tanto el personal de High Risk Zone como los conductores de los carros no pueden tener contacto físico con ellos ya que se utiliza una plataforma de transferencia.

Por contrato TELEFÓNICA se compromete a precintar con sello de plomo todas las maletas que deban ser recogidas por G4S.

- Respecto de las cintas de backups

Las copias de seguridad se realizan mediante una herramienta instalada en un servidor virtual y son copias completas con una determinada rotación antes de su reutilización.

Se identifican por código de barras de carácter interno por lo que no se puede conocer el propietario, el contenido, ni el software utilizado para la grabación.

La infraestructura utilizada para su realización es una tecnología antigua lo que dificulta la existencia de dispositivos compatibles capaces de realizar la lectura.

Respecto de las medias implementadas con posterioridad a la incidencia

- Con motivo del incidente, TELEFÓNICA ha acordado con la empresa SOPRA-STERIA la encriptación de las cintas de *buckups* a partir de junio de 2019. Esta encriptación no se realizará sobre las cintas anteriores que se encuentran archivadas.

## 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, se presume que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una posible brecha de confidencialidad como consecuencia del posible acceso indebido por terceros ajenos a la información contenida en los soportes *backaups* de la entidad. No obstante, en el presente caso, no consta acreditado que la documentación extraviada haya podido ser accedida por terceros.

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

Asimismo, TELEFÓNICA disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, comunicar, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la 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 las agencias colaboradoras en calidad de encargadas, así como el Delegado de Protección de Datos.

Consta también, que con ocasión de la incidencia TELEFÓNICA procedió a notificar la incidencia de seguridad a la Autoridad de Control de Luxemburgo sin que conste información al especto en el sistema de información interno de monitorización europeo.

No constan reclamaciones ante esta Agencia de los afectados.

En consecuencia, consta que TELEFÓNICA disponía de medidas técnicas y organizativas razonables en función del nivel de riesgo para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente procediendo a la encriptación de los soportes *backsups*. Además, TELEFÓNICA elaboró 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 causada previsiblemente por un error puntual.

**III**

Por lo tanto, se ha acreditado que la actuación de TELEFÓNICA 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 ***TELEFÓNICA SEGUROS SUCURSAL EN ESPAÑA,*** con ***NIF W0182798I*** y con domicilio en ***RONDA DE LA COMUNICACIÓN S/N. EDIFICIO OESTE 2, NUM 0, PISO 2 - 28050 MADRID (MADRID)***

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