- **Procedimiento N.º: E/09159/2020**

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 brecha de seguridad de datos personales por parte del Responsable del Tratamiento MAPFRE ESPAÑA COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A. relativa a ransomware que afecta a los servidores del responsable, 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: A la vista de la citada notificación de quiebra de seguridad de los datos personales, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, teniendo conocimiento de los siguientes extremos:
Fecha de notificación de la brecha de seguridad de datos personales: 16 de agosto de 2020.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:
MAPFRE ESPAÑA COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A. (en adelante, la investigada)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 14 de diciembre de 2020 se solicitó información al investigado. De la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

Mapfre es una empresa multinacional española dedicada al sector del seguro y reaseguro, con presencia en 40 países.

Respecto de la cronología de los hechos

En algún momento, probablemente a finales de julio, el atacante obtiene las credenciales de una colaboradora externa que accede a su puesto virtual en remoto. La hipótesis más probable es que su ordenador particular fuese infectado con un malware (seguramente tras una campaña de phishing), malware que posteriormente capturó su contraseña cuando accedió a MAPFRE.

• 1 de agosto:
Primer acceso ilegítimo mediante las credenciales de una usuaria de MAPFRE al puesto virtual de MAPFRE.

• Del 1 al 7 de agosto:
Se producen diversos accesos desde distintos países e intentos de conexión a otros servidores y equipos para hacerse con credenciales de usuarios privilegiados.

• 6 de agosto:
Mediante el uso de distintas herramientas de hacking, el atacante obtiene las credenciales de un usuario privilegiado.

• 7 de agosto:
El atacante mediante el uso de herramienta sofisticadas de hacking obtiene las credenciales de un administrador de dominio.

• Del 7 al 11 de agosto:
El atacante emplea diversas técnicas para analizar la red de comunicaciones, servidores de ficheros y los recursos compartidos y realiza varios intentos de ex filtración de información que son bloqueados por los elementos de seguridad desplegados en la red de MAPFRE.

• 14 de agosto:
18:41 - El atacante se conecta a la red de MAPFRE, y a las 19:40 comienza a distribuir el ejecutable “map.exe” asociado al ransomware utilizado Ragnar Locker, sobre la lista de servidores.

21.04 - El atacante: ejecuta remotamente el fichero “map.exe” y se inicia el proceso de cifrado en todos los equipos donde se desplego el archivo “map.exe”

21:11 – Se identifica por monitorización el fallo de múltiples aplicaciones y se activa el protocolo establecido de Alto Impacto. Se reciben las primeras alarmas al Centro de Control General de MAPFRE y una vez se tiene conocimiento se realiza un escalado de la situación.

21.15 -Tras detectar incidencia en sistemas de monitorización del CPD de ******LOCALIDAD.1*****, se abre procedimiento de gestión de incidentes mediante una call de personal técnico.

21:20 – Desde el área de Seguridad se activa el Comité de Crisis.

21:30 – Se activan los planes de Continuidad de Negocio.

21:35 –Se activa una call permanente con personal de las áreas de Seguridad y Tecnología.

Se identifica el incidente como un posible ataque de Ransomware y se dan las primeras
instrucciones para contener y evitar la propagación del ataque:

- o Apagado de todos los servidores no considerados imprescindibles.
- o Sacar de línea la copia de backup, y aislar determinados segmentos de red.
- o Cortar las conexiones desde MAPFRE hacia el resto de terceras empresas.
- o Limitar el número de conexiones remotas a un reducido número de usuarios.

22:30 – empiezan a llegar las primeras personas del equipo de seguridad de MAPFRE a Majadahonda, así como de tecnología al CPD de ******LOCALIDAD.1***.

23:00 – se cambia la validación del ******SOFTWARE.1*** de ******SISTEMA.1*** a ******SISTEMA.2*** (autenticación en la nube).

Los sistemas de validación con ******PLATAFORMA.1*** se encuentran en ******LOCALIDAD.1*** y están afectados por el ciber ataque, se aplica el sistema de DR pasándolo a ******PLATAFORMA.1***, recuperándose los accesos al correo para toda la organización.

23.30 Desde el área de Seguridad, se inicia una ronda de contactos con los equipos de seguridad de los principales socios de negocio, a fin de informarles de la situación.

15 de agosto:

00.30 – Empiezan a llegar personal interno de refuerzo a los edificios de los Contact Center para la atención a los clientes.

00:45 - se empiezan a recuperar puestos de trabajo virtuales (VDIs de Contingencia).
Se mantiene activo el Comité de Crisis para análisis inicial de impacto y la toma de decisiones al respecto. Durante los siguientes días se mantendrán reuniones diarias de seguimiento, así como un constante contacto. En paralelo se mantendrán reuniones diarias del resto de comités de crisis de entidades subordinadas priorizando la contención de ciberataque, así como la prestación del servicio al cliente. Se confirma la disponibilidad e integridad de la copia de backup. Se empieza a trabajar en la estrategia a seguir para la recuperación de los equipos y servicios.
Se confirma la no afectación de los servicios ubicados en las distintas cloud.
Se contacta con ******EMPRESA.1*** para obtener su apoyo en gestión del incidente dada que la principal afectación ha sido en sus sistemas operativos.
Se establece un plan de refuerzo para impedir eventuales nuevas intrusiones, entre las que se incluye el reseteo de contraseñas de administradores, la reducción de usuarios administradores, el refuerzo del Directorio Activo, un incremento inmediato del nivel de seguridad de las herramientas de seguridad, fortificación de la seguridad en puestos y servidores, aumento de las capacidades de monitorización, detección y respuesta, etc.

04:18 Se consigue identificar y aislar el malware, y se envía a ******EMPRESA.2*** para su análisis.
Se trabaja estrechamente con el proveedor de antivirus ******EMPRESA.2***, quien informa que ha conseguido actualizar su plataforma antivirus para garantizar que detecta el malware enviado por MAPFRE. La parametrización por defecto del antivirus permite la limpieza del malware de los equipos.

08.30 Empieza a llegar personal de refuerzo de proveedores externos a nuestros Contac center para posibilitar la atención a los clientes. Durante todo el día, las

distintas líneas de atención al cliente están activas y operando, aunque sin los estándares de calidad habituales, que irán mejorando rápidamente en los próximos días.

Se contacta con el INCIBE (Instituto Nacional de Ciberseguridad) y CCN – CERT (Centro Criptológico Nacional) para informarles del ciberataque y con el objetivo de garantizar la difusión.
Se contacta con la Dirección General de Seguros y Fondos de Pensiones para informar del ciberataque.
Se publica en la página web de MAPFRE (apartado sala de prensa) un comunicado oficial sobre el incidente.

16 de agosto:
Se notifica el ciberataque a la Agencia Española de Protección de Datos.
Se contacta con ******EMPRESA.3*** para recabar su apoyo en la línea de actuación encaminada a identificar una posible propagación del incidente a las entidades MAPFRE fuera de España.
Por el impacto en los puestos físicos se toma la decisión de restaurar el servicio de puesto de trabajo para empleados en Windows Virtual Desktop (WVD) y se comienzan a montar todos los puestos que se necesitan.
Tras las conversaciones con los mismos, se comienza a abrir las comunicaciones con los distintos socios de negocio en España

17 de agosto:
Se siguen mejorando los tiempos de respuesta en la atención a clientes. En ese lunes, se abren, con la normalidad propia del periodo vacacional, las oficinas de MAPFRE en toda España, que posibilitan un nuevo canal de atención a clientes.
Se presenta denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.
Se amplían las medidas de refuerzo de la seguridad, entre las que se encuentra el refuerzo de la protección de los backup y la extensión a todos los colectivos de usuarios de la autenticación mediante doble factor para los accesos remotos a los sistemas.
De igual modo, se continúan analizando y gestionando la progresiva reapertura de las comunicaciones con terceros y con las entidades MAPFRE en otros países, para verificar que dichas aperturas no suponen un menoscabo en la seguridad de las compañías implicadas.
Tras la valoración del impacto se comienza a definir el plan de recuperación del parque físico de puestos.
El cuarto día tras el ciberataque se dispone ya de ***XXXX*** puestos virtuales instalados que se añaden a los equipos fijos no afectados (una minoría) y los equipos portátiles disponibles (en su inmensa mayoría no fueron afectados).

• 19 de agosto:
Se decide el despliegue de las herramientas de seguridad de ******SOFTWARE.1***, (…), Defender ***(…)*** y ******PLATAFORMA.1 (…)***, que posibilitan una más completa monitorización y mejoran la capacidad de respuesta, así como el agente ******AGENTE.1*** para identificar cualquier indicio de afectación o persistencia del virus en los equipos.
Asimismo, se define y aprueba el plan de fortificación del ecosistema ******ECOSISTEMA.1*** con la colaboración de esa compañía.

• 20 de agosto:
Se empieza a gestionar la entrega a socios, equipos de seguridad de empresas que nos los solicitan y organismos gubernamentales los IOC (Indicator Of Compromise) con la información esquematizada del ataque obtenida durante el análisis forense por parte de MAPFRE, a fin de poder identificar si sus sistemas también han sido comprometidos con el mismo ataque y para detener eventuales ataques a sus redes.

23 de agosto:
Una vez superada la fase más crítica de la contención y respuesta al ciberataque, se coordinan la implantación del resto de las acciones de refuerzo de la seguridad en el resto de los países.

• 01 de septiembre:
A esa fecha se dispone ya de + ***XXXXX puestos*** virtuales instalados, con lo que se da prácticamente cerrada esa línea de trabajo asociada a la dotación de equipos virtuales al colectivo de empleados y delegados.

• 02 de septiembre
Se inicia con el procedimiento de recuperación de los puestos virtuales correspondientes a los proveedores de tecnología

• 13 de septiembre
Al estar ya prácticamente todos los elementos de la red del CPD restaurados, se da por finalizado el seguimiento y se establece un procedimiento para la gestión de las incidencias que surjan.

• 21 de septiembre:
Nueva comunicación con la AEPD para proporcionar mayor información y estado de situación a la fecha indicada, dado lo muy avanzado del análisis forense y trabajos de recuperación.

23 de septiembre:
Se da por finalizada la recuperación de los puestos físicos ubicados en oficinas y edificios propiedad de MAPFRE y en oficinas delegadas.
Finalización de las investigaciones y acciones necesarias que permiten concluir con un muy alto grado de certeza que la red es segura, que no existe persistencia de actividad de los atacantes en la misma y dar por resuelta la brecha.

• 12 de octubre
Se da por cerrada la línea de trabajo de recuperación de puestos virtuales de proveedores

• 26 de octubre
Tras la comprobación de los últimos servidores, se da por cerrada la línea de trabajo asociada a la identificación tanto de posibles accesos de los usuarios empleados por los atacantes a las carpetas confidenciales de red, como de actuaciones anómalas en estas, no encontrándose evidencia alguna en estos sentidos, y concluyéndose el no acceso de los atacantes a las mismas

• 28 de octubre:

Comunicación a la AEPD del cierre de la brecha una vez finalizado el análisis forense del incidente.

• 13 de noviembre:
Cierre con éxito de los trabajos de la fase de refuerzo de confianza del Plan de Refuerzo, con lo que se puede garantizar la erradicación de cualquier tipo de credencial que los atacantes hubieran podido crear.

Respecto de las causas que hicieron posible la brecha
Un atacante altamente especializado empleó tiempo y herramientas muy sofisticadas para perpetrar el ataque. Para ello, entre otras, crearon una muestra específica del virus que fuera indetectable para el software antivirus que MAPFRE dispone. La muestra de virus utilizada en el ataque no estaba disponible ni era conocida en VirusTotal6 el día 15 de agosto.
Adicionalmente, la necesidad de adoptar medidas para adaptarse a la situación de pandemia creada por el COVID 19, provocó la adopción de diversas formas de trabajo en remoto para el personal de MAPFRE que aumentaron la superficie de exposición de nuestra red al conllevar el uso de equipos personales para acceder a los puestos de usuario, lo que permitió la captura de un identificador y contraseña válidos para acceder a la red de MAPFRE en el puesto personal de un usuario.

Medidas de minimización del impacto de la brecha y para su resolución
En primera instancia, como medida de precaución, para evitar la propagación del malware al resto de la red, entre otras, se aislaron varios segmentos de esta y se apagaron los sistemas hasta confirmar el alcance de la brecha. Esto, junto al elevado número de equipos y servidores cifrados, supuso una degradación y pérdida temporal del servicio e hizo necesaria la activación del Plan de Continuidad de Negocio a fin de garantizar su prestación.

Consecuencia de ello, desde el momento de la detección, se convocó el Comité de Crisis integrado por los máximos responsables de las principales áreas de la entidad y se creó un Grupo de Trabajo multidisciplinar con los máximos expertos tanto de tecnología como de seguridad del Grupo MAPFRE en la materia.

En paralelo a las tareas de contención del ciberataque, se abrió una línea de trabajo específica para conseguir la restauración de los sistemas y aplicaciones de forma que se recuperara cuanto antes el servicio a clientes y resto de grupos de interés. En este trabajo participó intensamente el conjunto de proveedores que prestan a la compañía servicios tecnológicos relacionados con los sistemas afectados.

De acuerdo a las prioridades establecidas en los PCN, se iniciaron los trabajos para la restauración segura, en un entorno limpio y controlado, de los sistemas de información afectados por el ciberataque y se consiguió restablecer los servicios más críticos de forma rápida.

Paralelamente a la restauración del servicio a los clientes, desde el primer momento de la detección del incidente se inició el trabajo de investigación del ciberataque, con el objetivo de conocer los detalles del mismo en tres líneas diferentes en función del marco temporal y objetivos de las mismas.

Tras la culminación de estos trabajos, se ha constatado la no existencia de evidencias de fugas de información ni de expansión de los atacantes a otros entornos distintos del de los sistemas ubicados en España.

Desde la misma noche del Incidente se contactó por los canales establecido al efecto con el CCN-CERT y el INCIBE, a fin de informarles de lo sucedido, compartir la información disponible sobre el tipo y características del ataque que posibilitara la reducción del riesgo de expansión a otras organizaciones y recabar su apoyo. Asimismo, los hechos se denunciaron ante la Guardia Civil.
Conforme se fueron obteniendo los resultados de los trabajos de investigación antes mencionados, se establecieron líneas de colaboración con otros fabricantes de software y soluciones de seguridad, con el objetivo de establecer un plan de refuerzo de la seguridad cuyo alcance no se limitó exclusivamente a España, sino al resto de países donde está implantado el Grupo MAPFRE.

Este Plan incluyó las siguientes medidas urgentes a corto plazo que se han ido ejecutando al mismo tiempo que avanzaban los trabajos de investigación del Incidente, si bien incluye también medidas a medio plazo que se irán acometiendo en los próximos meses.
- Refuerzo de las medidas específicas de prevención y detección de ataques en la política antivirus
- Incremento de los umbrales de detección y del nivel de protección de la plataforma Antispam
- Ampliación a todos los colectivos de usuarios de la autenticación multifactor para accesos remotos.
- Incremento de capacidades de monitorización, detección y respuesta con la aceleración del despliegue de soluciones ***(…)*** específicas en puestos y servidores
- Incorporación de nuevas reglas específicas de detección en los sistemas de monitorización basadas en la experiencia acumulada
- Aumento de las restricciones a la navegación por Internet.
- Inclusión de los indicadores de compromiso (IoC) relacionados con el ciberataque en la distintas plataformas y filtros de seguridad existentes (FW, IPS, Filtros de Contenido, etc.)
- Elevación del nivel de alerta en los sistemas de prevención de ataques DDoS
- Incremento del nivel de control del uso de usuarios administradores

<u>Respecto de los datos afectados</u>.
Los datos que se han visto vulnerados han sido el identificador de usuario y contraseña de acceso a los sistemas de información de MPAFRE por lo que se trata de datos básicos.
El volumen de Datos se encuentra en el rango de menos de 100.
Manifiestan que el impacto fue prácticamente nulo, dado el periodo vacacional en que sucedió. Los atacantes tuvieron acceso a dos identificadores personales de usuarios, que fueron utilizados únicamente para acceder y moverse por los sistemas de la compañía y, mediante herramientas sofisticadas de hacking, realizar el escalado de privilegios dentro de la red y distribuir el malware específicamente desarrollado para MAPFRE. Esos identificadores de usuarios no tienen aplicación fuera del entorno de sistemas de MAPFRE y quedaron inutilizados tras su bloqueo y el cambio de contraseñas asociadas a los mismos.

MAPFRE comunicó públicamente esta situación a las pocas horas de conocerla, los cual, según manifiestan, demostró ser uno de los aspectos que permitió minorar también el impacto del ciberataque ya que tanto clientes, como colaboradores, empleados y proveedores tuvieron una actitud y actuación crucial en la gestión de la crisis.

Comunicados realizados al efecto:
- Comunicado publicado en la web
- Locución que se puso en el Contact Center y que informaba a todo aquel que llamaba sobre lo ocurrido.
- Mensaje utilizado en las redes sociales
- Comunicados del ***CARGO.1 ***(A.A.A.)***
- Comunicados del ***CARGO.2 (***B.B.B.)***
- Comunicado a empleados de MAPFRE
- Comunicados realizados a la AEPD

Respecto de las medidas de seguridad implantadas con anterioridad la brecha
La gestión de estos identificadores de usuarios se encuentra recogida en el Tratamiento “Gestión de los datos personales utilizados para generar los Usuarios para el acceso a los sistemas de MAPFRE”. Este tratamiento se realiza por MAPFRE SA, en particular por el COAS (Centro Operaciones de Accesos e Identidades), órgano integrado en el SOC GLOBAL para distintas entidades del Grupo MAPFRE, entre ellas MAPFRE ESPAÑA. Dicho tratamiento se encuentra descrito en detalle en los documentos asociados a la Evaluación de Impacto.
Para el Tratamiento “Gestión de los datos personales utilizados para generar los Usuarios para el acceso a los sistemas de MAPFRE”, al ser uno de los tratamientos que existían antes de la entrada en aplicación del RGPD, se realizó el análisis asociado a la regularización del Impacto de Seguridad y Privacidad del cual adjuntan copia y donde se efectúa una evaluación de los distintos aspectos, así como de las medidas de seguridad a fin de confirmar que dicho tratamiento de datos no supone un impacto alto.
Aportan hoja Excel de detalle con la descripción del tratamiento y las medidas de seguridad.
Posteriormente, se procedió a elaborar una Evaluación de Impacto en la protección de datos personales de este tratamiento, incluyendo la identificación de los riesgos asociados al mismo del cual adjuntan copia.
Por otra parte, con motivo de la crisis del Coronavirus, y la necesidad de posibilitar el trabajo en remoto a la práctica totalidad de la plantilla de MAPFRE, se realizó una reevaluación del riesgo y se definió un plan específico de refuerzo de la ciberseguridad, denominado Plan de Reconfiguración de CiberSeguridad, que es de aplicación a todos los tratamientos realizados y, en particular está asociado al tratamiento que nos ocupa (Tratamiento “Gestión de los datos personales utilizados para generar los Usuarios para el acceso a los sistemas de MAPFRE”). Aportan extracto de la presentación realizada al Comité Ejecutivo de MAPFRE. Adicionalmente se estableció un plan de concienciación específico asociado a esta situación.
En abril del 2018 se aprobó, la realización de las auditorías de cumplimiento del RGPD y se definió un Plan de Auditorías que cubriera a todas las entidades MAPFRE sujetas al RGPD. Para llevar a cabo estas auditorías en el marco antes definido, que son de cumplimiento del RGPD y no únicamente de cumplimiento de las Medidas de

Seguridad, la Dirección General de Auditoría Interna de MAPFRE se apoyó en un tercero especializado en la materia, la empresa ******EMPRESA.4.***
MAPFRE ESPAÑA se encuentra adherida, tras participar activamente en su elaboración, a la "Guía para el tratamiento de los datos personales por aseguradoras" elaborada por UNESPA que, aunque no es un código de conducta propiamente dicho, es un mecanismo de autorregulación y contempla la necesidad de cumplir con una serie de principios específicos en materia de privacidad y protección de datos.
MAPFRE ha decidido adoptar el RGPD como norma de referencia en materia de Privacidad y Protección de Datos y disponer de unas BCRs en el Grupo. Para ello, en julio pasado se aprobó tanto la licitación del proyecto como la creación de un Grupo de Trabajo específico para el desarrollo de estas BCRs.

Respecto de las medidas implementadas con posterioridad la brecha
Una vez finalizada la gestión del incidente se definieron un conjunto de actividades que permitieran garantizar la erradicación de cualquier tipo de acceso que los Threat Actors hubieran podido obtener.
Las investigaciones realizadas por los distintos equipos que formaron parte en la gestión del incidente nunca evidenciaron la creación de una credencial maestra (generalmente denominada Golden Ticket) o similar. No obstante, aplicando los máximos criterios de prudencia y dado que el Threat Actor tuvo accesos de administración al Dominio ******DOMINIO.1*** del entorno ******ENTORNO.1*** se tomó la decisión de ejecutar los protocolos necesarios que garantizaran la erradicación de cualquier puerta trasera que se hubiera podido crear.
Este conjunto de medidas se enmarcó en el Plan de Fortificación del entorno ******ENTORNO.1*** y se ejecutó de forma inmediata a la finalización de los trabajos de gestión del incidente que se reflejan el grafico anterior. Los trabajos dentro de esta fase se realizaron de forma conjunta para todos los dominios críticos identificados

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."

De las actuaciones de investigación se desprende que, con anterioridad a la brecha de seguridad, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados, en abril del 2018 se aprobó la realización de las auditorías de cumplimiento del RGPD y se definió un Plan de Auditorías que cubriera a todas las entidades MAPFRE sujetas al RGPD e incluso se han reforzado estas medidas con motivo de la situación de pandemia, que exige posibilitar el trabajo remoto a gran parte de la plantilla.

Es reseñable que la empresa ha participado activamente la elaboración, de la "Guía para el tratamiento de los datos personales por aseguradoras" elaborada por UNESPA que, aunque no es un código de conducta, si es un mecanismo de autorregulación y contempla la necesidad de cumplir con una serie de principios específicos en materia de privacidad y protección de datos.

En cuanto al impacto, los datos que se han visto vulnerados han sido, el identificador de usuario y contraseña de acceso a los sistemas de información de MAPFRE, que tratándose datos básicos, no tienen aplicación fuera del entorno de sistemas de MAPFRE y quedaron inutilizados tras su bloqueo y el cambio de contraseñas asociadas a los mismos.

El volumen de Datos se encuentra en el rango de menos de 100 y el impacto ha sido casi nulo, pues los intentos de exfiltración fueron detectados y evitados, lo que unido a la rapidez para hacer público el ciberataque permitió la eficaz actuación de clientes, trabajadores, colaboradores y proveedores, minimizando los efectos del ciberataque.
No constan reclamaciones ante esta Agencia por parte de terceros.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia, lo que ha permitido la rápida identificación, análisis y clasificación de la brecha de seguridad de datos personales.

Por lo que respecta a su actuación tras la identificación de la amenaza, cabe calificarla, como de diligente reacción, con una rápida notificación tanto al Incibe como al CCN-CERT y a la Guardia Civil, así como una serie de notificaciones sobre la evolución de la incidencia a la AEPD, junto a una rápida comunicación con clientes, colaboradores, proveedores y empleados que posibilitó una eficaz reacción contra el ataque.

En relación con las medidas adoptadas para minimizar el impacto y eliminar las posibles lagunas en la seguridad que hubiese dejado el ataque, se procedió a la ejecución del Plan de Fortificación del entorno ******ENTORNO.1***.

III

En el presente caso, la actuación de la investigada como entidad responsable del tratamiento, ha sido diligente 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 MAPFRE ESPAÑA COMPAÑIA DE SEGUROS Y REASEGUROS S.A., con NIF A28141935 y con domicilio en CARRETERA DE POZUELO, Nº 50, 28222 MAJADAHONDA (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.

940-0419

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