
DATA

# 24 HORAS CLAVE FRENTE AL CIBER-ATAQUE

TEXTO **JAVIER FERNÁNDEZ** | FOTOGRAFÍAS **ISTOCK**

# 14 DE AGOSTO, VIERNES:

## 20:00

**La media España que se lo ha podido permitir está de vacaciones e intenta convivir con unas medidas que ahora sabemos que fueron demasiado relajadas frente al covid-19.** Para las aseguradoras es la víspera a uno de los días con mayor movimiento de tráfico del año, el cambio de quincena siempre es un momento estresante para la mayoría de las empresas relacionadas con el servicio en carretera. Un año más, MAPFRE lo tiene todo previsto y el servicio está preparado para responder a las necesidades de los clientes.

SE TRATA DE **UN ATAQUE DE RANSOMWARE QUE BUSCA ENCRIPTAR LA INFORMACIÓN** PARA IMPEDIR LA OPERATIVA DE LA COMPAÑÍA, Y NO HA SIDO LANZADO CONTRA MAPFRE POR CASUALIDAD

**UN AÑO ANTES,** AGOSTO DE 2019, **CIBERDELINCUENTES INTERNACIONALES COMIENZAN A PREPARAR EL ATAQUE** CONTRA MAPFRE, CREAN UNA HERRAMIENTA DE **HACKING A MEDIDA** CONTRA MAPFRE, UN VIRUS ESPECÍFICO

## 21:04

**Se lanza un ciberataque masivo contra MAPFRE en España.** Cualquier compañía de nuestro tamaño detecta y neutraliza cada día cientos de miles de eventos similares que buscan acceder de alguna manera al interior de los sistemas. Pero éste enseguida se ve que es diferente. Se trata de un ataque de *ransomware* que busca encriptar la información para impedir la operativa de la compañía, y no ha sido lanzando contra MAPFRE por casualidad.

**Un año antes, agosto de 2019, ciberdelincuentes internacionales comienzan a preparar el ataque contra MAPFRE.** Toman las primeras decisiones de compras de dominios que permitan aproximarse a la compañía. También crean una herramienta de *hacking* a medida contra MAPFRE, una herramienta nueva para que no pueda ser detectada por los sistemas antivirus actuales, un virus específico para atacar con él a una única compañía en España. Todo esto lo hemos conocido después, gracias al análisis forense realizado por MAPFRE en colaboración con las principales firmas internacionales especializadas en combatir los ciberdelitos. Los ataques de *ransomware* se incrementaron un 500 por cien en 2019, principalmente contra grandes compañías multinacionales, instituciones de todo tipo e incluso gobiernos.

El escudo de protección de MAPFRE es 24x7x365. En cuanto el ataque se activa, un experto del Centro de Operaciones de Seguridad de Majadahonda lo detecta y pone en marcha el protocolo de análisis de alertas que, en seguida, evidencia la gravedad del problema y da la señal de alarma.

## 21:11

**El Director del Centro de Operaciones de Seguridad de MAPFRE es informado del ataque y empieza la movilización de los equipos frente al mismo,** según lo previsto en el Plan de Gestión de Crisis y Continuidad de Negocio porque el ciberataque es uno de los riesgos analizados y modelizados para poder actuar de manera inmediata cuando se producen. Minutos más tarde se activa el Comité Corporativo de crisis y, dado que el primer impacto se detecta en España, también se moviliza el Comité de Crisis de MAPFRE

España porque, no es por casualidad, el ataque busca dejar ciega a la compañía uno de los días más críticos en la prestación del servicio, especialmente las asistencias en carretera.

Fue una noche muy larga la de aquel viernes, los profesionales de MAPFRE no dudan en interrumpir sus vacaciones y conectarse o presentarse en Majadahonda para combatir el ataque de manera coordinada entre todas las áreas implicadas. Una maquinaria probada y engrasada es la mejor garantía de que va a funcionar cuando más se necesita, y el tiempo juega a la contra porque el virus empieza a encriptar equipos y sistemas lo que, en una compañía altamente digitalizada, supone quedarse "ciego" en tu capacidad de responder al cliente.

**LOS PROFESIONALES DE MAPFRE NO DUDAN EN INTERRUMPIR SUS VACACIONES Y CONECTARSE O PRESENTARSE** PARA COMBATIR EL ATAQUE

**LA DIRECCIÓN CORPORATIVA DE SEGURIDAD Y EL ÁREA CORPORATIVA DE TECNOLOGÍA Y PROCESOS SE OCUPAN DE LA PRIMERA ACCIÓN,** IDENTIFICAR EL VIRUS, ANALIZAR EL ALCANCE, CONTENER SU EXPANSIÓN. **ESTA DESCONEXIÓN GENERAL PERMITE ACOTAR EL VIRUS EN ESPAÑA**

**Contener, Operar y Responder son las tres estrategias que empiezan en paralelo.** La Dirección Corporativa de Seguridad y el Área Corporativa de Tecnología y Procesos se ocupan de la primera acción, identificar el virus, analizar el alcance, contener su expansión... la primera medida es aislar el *data center* cortando todas las comunicaciones con el exterior, y con el centro de recuperación frente a desastres. Había que apagar sistemáticamente todos los sistemas hasta conocer con detalle el grado de impacto y poder articular una respuesta. Esta desconexión general es la que permite acotar el virus en España, al aislar la operativa del resto de los países.

## 02:30

**Operaciones también se activa y coordina en España una respuesta alternativa rápida para poder atender a los clientes al día siguiente.** Los equipos están apagados y/o contaminados, luego no sirven para la gestión habitual con los clientes, hay que reforzar el SI24 y habilitar procedimientos alternativos, pasadas las dos y media de la madrugada ya del sábado el sistema está montado y operativo. En apenas cuatro horas se han habilitado conexiones de voz en los *call centers* para poder atender a los clientes y las personas de Operaciones que estaban trabajando en remoto se desplazaron a los edificios de MAPFRE para poder atender las llamadas. Los servidores de aplicaciones se empiezan a recuperar inmediatamente utilizando el sistema de *backup* que contenía toda la información protegida y que no había sido vulnerado demostrando su fortaleza técnica.

## 03:00

**Ya tenemos el antivirus. A** pesar de que era una nueva modalidad de virus, específico contra MAPFRE y evolucionado y afinado durante meses hasta encontrar una puerta de entrada, en apenas seis horas ya se cuenta con el antivirus que es imprescindible para empezar la tarea progresiva de ir recuperando equipos y sistemas de la forma más segura. Se priorizan estos segundos y, en general, toda la tecnología relacionada con la atención al cliente, que es la clave de ese fin de semana.

## 08:00

**Los ciudadanos han comenzado sus desplazamientos masivos fundamentalmente por carretera, comienzan los primeros siniestros.** El SI24 está reforzado, pero tiene limitaciones que le impiden responder de manera habitual y los tiempos de espera se alargan.

Las primeras horas son especialmente complejas, pero MAPFRE cuenta ya con un entorno seguro que permite empezar a restaurar de forma priorizada servidores y equipos. Se reúne el Comité de Crisis Corporativo y se tiene una primera foto del impacto. Las medidas de contención han funcionado pero el daño es profundo en España. El servicio a los clientes se está prestando, no con normalidad, pero sí se está prestando gracias sobre todo a la respuesta articulada desde Operaciones de MAPFRE España y al compromiso de todas las personas relacionadas con la atención al cliente.

**EN APENAS SEIS HORAS YA SE CUENTA CON EL ANTIVIRUS**

**DENTRO DE LAS PRIMERAS 24 HORAS** Y UNA VEZ QUE SE TIENE UN ANÁLISIS ESTABLE DEL IMPACTO, **SE COMUNICA MASIVAMENTE A LA OPINIÓN PÚBLICA** POR TODOS LOS CANALES

LA DIRECCIÓN CORPORATIVA DE SEGURIDAD HA COORDINADO **MÁS DE 200 COMUNICADOS INFORMANDO SOBRE EL ATAQUE Y SUS CONSECUENCIAS**

## 15:00

**MAPFRE es una empresa transparente que establece relaciones de confianza con todos sus grupos de interés.** Suena bien pero no es un *claim,* es un compromiso real frente al que no se tienen dudas. Lo habitual es que las empresas o las instituciones afectadas por este tipo de ataques no lo comuniquen o lo hagan cuando ya no tengan más remedio. MAPFRE respeta sus compromisos y decide actuar con plena transparencia desde el primer momento. Comienza la comunicación de la crisis a los supervisores y organismos reguladores, no consta la fuga masiva de datos, pero se comunica igualmente con la información disponible en cada momento. A las tres de la tarde, es decir, dentro de las primeras 24 horas y una vez que se tiene un análisis preliminar del impacto, se comunica masivamente a la opinión pública por todos los canales. La información y la transparencia se convierten en el mejor aliado para proteger la reputación. La opinión pública entiende que estamos ante un ataque altamente profesional frente al que no está 100% protegida ninguna compañía, institución o gobierno del mundo, y el hecho de comunicarlo representa un compromiso de transparencia que es especialmente valorado. Ese fue el principio, y a lo largo de las semanas siguientes la Dirección Corporativa de Seguridad ha coordinado más de 200 comunicados informando sobre el ataque y sus consecuencias no solo a los organismos preceptivos, sino también en general a todos aquellos que han preguntado a MAPFRE sobre el alcance del ataque.

## DOMINGO 16

**Se empieza a lanzar la segunda oleada de medidas de refuerzo de seguridad al resto de países para proteger frente a esta nueva amenaza y comienza la reconexión segura con ellos, así como con nuestros socios de negocio, mientras se continúa el proceso de recuperar los servidores, bases de datos y sistemas afectados.** Lo más importante: el *backup* está salvado. El protocolo previsto frente a

un ciberataque permitió ejecutar desde el primer minuto decisiones que han permitido salvar la información de la compañía.

Desde el tercer día se aceleró la apertura progresiva de las operaciones y se fue recuperando y estabilizando la operativa con los clientes. También se reinstalaron en dos semanas 18.000 puestos de trabajo distribuidos en más de 3.000 oficinas de MAPFRE, entre otras acciones. A finales de agosto, MAPFRE dio por superada esta crisis en lo que se refiere a su máxima prioridad: la atención a los clientes. Y tomó la decisión de compensar con 100 euros en su renovación a aquellos a los que no pudimos atender con nuestro nivel de excelencia habitual, fundamentalmente durante los primeros días y en relación a las asistencias que hubo que gestionar de forma manual.

Internamente, se sigue trabajando para alcanzar la revisión y recuperación completa. El análisis forense profundo continúa, así como la investigación policial que a nivel internacional combate este tipo de terrorismo, pero el momento crítico de los primeros días se superó y, visto dos meses después, con éxito. Adicionalmente, la compañía contaba con protección aseguradora frente a los ciberdelitos que asumirá parte del coste.

**La rápida actuación acotó el ataque solo a España. La información estaba bien protegida, por lo que ha podido recuperarse. Hay muy pocas compañías con esta capacidad ordenada de respuesta. La reconstrucción posterior de los hechos nos ha mostrado claramente por dónde entraron y por dónde salieron. También permite intuir qué organización delictiva está detrás de este ataque diseñado específicamente contra MAPFRE, pero dejemos que la investigación internacional siga su curso, para que cada vez más instituciones y países puedan coordinar una respuesta global más eficaz frente a este tipo de actuaciones.**

## 5 LECCIONES APRENDIDAS

▶ **La seguridad total no existe.** El ataque se lanzó en agosto, pero los terroristas estuvieron un año preparándolo e invirtiendo cientos de miles de euros solo para atacar a MAPFRE. Y depende de cada uno de nosotros. Un usuario y una contraseña capturados por los atacantes sirvieron como punto de entrada

▶ **Maquinaria engrasada.** La mejor respuesta se consigue estando preparado, pudimos reaccionar rápido y con eficacia porque lo teníamos previsto y analizado en el Plan de Crisis y Continuidad de Negocio.

▶ **Compromiso humano.** Profesionales altamente comprometidos que reaccionaron con total entrega y generosidad desde el primer momento

▶ **Resiliencia de MAPFRE.** Una demostración de la capacidad del negocio para seguir operando en condiciones extremas

▶ **La transparencia como defensa de la reputación.** Informar a nuestros grupos de interés aumentó la comprensión de todos ellos respecto a la crisis que estaba afrontando la compañía