HÉROES DEL CIBER ATAQUE

TEXTO **VIOLETA MATEO**
FOTOGRAFÍAS **MAPFRE, ISTOCK**

En el mundo corporativo, las cosas no suceden por casualidad, ni porque alguien, por muy jefe o jefa que sea, las desee. Suceden porque están planificadas como hemos visto en la crónica del ciberataque y, sobre todo, porque hay personas que las ejecutan. Y en MAPFRE sabemos mucho de personas que cuidan de... la compañía. Todos los empleados de MAPFRE hemos sido parte de la solución frente al ataque informático de agosto en España protegiendo la reputación de la compañía y ayudando desde nuestra responsabilidad a superar la crisis. Pero hay algo más de 200 profesionales que han estado especialmente vinculados a todo lo que pasó a partir de ese 14 de agosto. Son un equipo multidisciplinar de héroes que están representados por la visión de los siguientes compañeros de las áreas y unidades más directamente implicados. Este es su relato.

VISITA LA INTRANET GLOBAL
ESPACIO PERSONAS → MI DÍA A DÍA → SEGURIDAD DE LA INFORMACIÓN

De: MAPFRE
Para: Héroes
Asunto del mensaje: URGE – Ataque de Ransomware

NO HUBO UN SOLO DÍA EN EL QUE NO RECIBIÉSEMOS OFRECIMIENTOS DESINTERESADOS DE AYUDA

Cuando comenzó el ataque, los servicios del Si24 se vieron afectados y se declaró Incidencia de Alto Impacto. A partir de ese momento ya estábamos informados de que algo ocurría a través de las comunicaciones oficiales de incidencias y de WhatsApp. En menos de 10 minutos ya teníamos montado el comité de crisis de incidencias y una vez detectada la severidad del incidente, este se extendió al resto de Grupos de la ACTP, ACS y TI de España. Nuestra dedicación fue total, independientemente de las vacaciones, todas las personas del equipo disponibles se incorporaron al grupo de trabajo a lo largo de ese fin de semana con el objetivo de recuperar el servicio a nuestros clientes lo antes posible.

Esta crisis nos ha hecho más fuertes, porque ahora somos más conscientes de puntos fuertes y debilidades. Debemos convertir estas últimas en oportunidades para seguir aumentando nuestra resiliencia.

MAPFRE tenía ya una estrategia definida de evolución del puesto de trabajo y movilidad definida por Personas y Organización y las áreas de TI durante este 2020. A causa de la pandemia por la covid19 y el ciberataque, se ha demostrado que era acertada, por ello destaco el plan desarrollado con anterioridad y por supuesto el trabajo de todos los compañeros de área de puestos de trabajo, sin los cuales y sin su esfuerzo, este hito no habría sido posible.

CARLOS MUÑOZ
DIRECTOR DE TECNOLOGÍA
DELIVERY UNIT DATACENTER

Durante los días más duros tras el ciberataque no hubo uno solo en el que no recibiésemos ofrecimientos desinteresados de ayuda y palabras de aliento por parte de compañeros de MAPFRE. Esto sin duda ha sido parte del éxito en la recuperación de los servicios y demuestra que somos una gran compañía formada por personas fieles, colaboradoras y generosas. Por esto es MAPFRE una gran compañía.

SE NOS PLANTEÓ DE LA NOCHE A LA MAÑANA UN NUEVO RETO Y FUIMOS CAPACES DE RESOLVERLO

Escuchar "ciberataque" fue como cuando un médico te da un mal diagnóstico, no tienes ni idea de qué hacer pero tienes claro que debes confiar en él. Y así hicimos, nos pusimos en manos de nuestros compañeros de tecnología. Seguimos todas sus indicaciones, probábamos qué funcionaba y qué no, solo disponíamos de teléfono. Y vienen a nuestras cabezas los servicios críticos, ¿qué pasa con urgencias médicas? ¿y decesos? ¿y asistencia en carretera? ¿y urgencias en el hogar? La única solución era buscar los datos de los proveedores en Google a través de nuestros teléfonos móviles. Y así pasamos esa primera noche. El trabajo en equipo, la implicación y el compromiso fueron las claves.

Este ciberataque ha provocado que durante un periodo no hayamos prestado el servicio que deseamos y esto es esencial, pues el servicio al cliente entre las compañías se diferencia por pequeños matices y sin duda la consistencia y la fiabilidad es uno de ellos.

La verdad es que, visto ahora, fueron momentos emocionantes, se nos planteó de la noche a la mañana un nuevo reto y fuimos capaces de resolverlo. Quiero destacar en esta parte el apoyo que nos prestaron los equipos del Centro de Competencias de Operaciones y del SAU, sin ellos no hubiéramos podido conseguirlo.

ELISA POMEDA
DIRECTORA DE ATENCIÓN TELEFÓNICA DE MAPFRE ESPAÑA

En este mundo tan tecnológico, donde tenemos muchas rutinas robotizadas y empezamos a resolver algunas situaciones mediante inteligencia artificial no podemos olvidar que valores como responsabilidad, compromiso y lealtad que solo radican en las personas, son los valores que nos permitirán salir de estas situaciones críticas y complicadas.

EL MÚSCULO SE ENTRENA

A partir de ese viernes por la noche, éramos pocos los que estábamos trabajando en agosto, por lo que tuvimos que avisar a la "caballería". La respuesta de los compañeros fue espectacular, faltó tiempo para que se pusieran en marcha para empezar a trabajar en todas las líneas que teníamos abiertas.

2020 ha sido un año muy complicado en el que por desgracia ha habido que poner en práctica todo lo que hasta ahora solo se había ensayado en formato de pruebas, nunca en situaciones reales, y que ni en el planteamiento más pesimista podíamos suponer que iba a ocurrir con ese nivel de impacto. Aun así, hay una lectura muy positiva: la base de procedimientos que existe (planes de contingencia a todos los niveles, que se ensayan de forma periódica), de conocimiento (del complejo entorno tecnológico y del servicio que presta a negocio), sumados a la capacidad de reacción de toda la compañía nos ha hecho superar ambas situaciones. No creo que esto haya sido una casualidad ni cuestión de suerte, ya que el músculo se entrena y en ambos casos nos ha pillado "en forma", más en el caso de agosto con la situación previa vivida con la covid-19.

Recomiendo visitar el espacio que hay en la Intranet Global, en la sección "Espacio Personas > Mi día a día > Seguridad de la información", donde hay información muy útil para ayudarnos a entender qué tipo de amenazas de seguridad existen y cómo podemos ayudar como usuarios a reducir al máximo todo este problema.

JUAN MANUEL GARCÍA
DIRECTOR DE TECNOLOGÍA. DELIVERY UNIT. PUESTO DE TRABAJO Y COLABORACIÓN DCTP

No todo ha funcionado a la primera ni como nos hubiera gustado desde el inicio, pero ha sido mucho más fácil con la ayuda y el apoyo de todos. Lamentablemente este tema de los ciberataques ha venido para quedarse y nos tocará hacer piña en más ocasiones.

SER RÁPIDOS Y TRANSPARENTES FUE UNA DE LAS GRANDES DECISIONES QUE SE TOMARON

Me acuerdo como si fuese ayer. Estaba con mis hijos dando un paseo un poco antes de las 10 de la noche del 14 de agosto y en ese momento entró el correo de Guillermo Llorente con un asunto bastante descriptivo "URGE – Ataque de Ransomware" y antes siquiera de llegar a abrir el correo ya tenía una llamada para mantener una reunión a las 10. A partir de ahí todo se desencadena de forma muy rápida y vuelvo a Madrid a toda prisa para ayudar en todo lo que estuviese en mi mano.

Hemos aprendido que no estábamos preparados para un atacante de estas características, de hecho nadie lo está en ningún lugar del mundo, por lo que nos ha tocado mejorar con carácter de urgencia nuestras capacidades de seguridad. Y por supuesto, la importancia de tener planes de contingencia robustos y probados. El ataque que sufrimos fue mucho más que un incidente tecnológico y podría haber afectado a nuestra reputación y a la confianza que depositan en MAPFRE nuestros clientes. Ser rápidos y transparentes con lo que nos estaba ocurriendo fue una de las grandes decisiones que se tomaron. Me gustaría pedir a los empleados comprensión y paciencia porque esta situación nos va a hacer incrementar varios de nuestros controles de seguridad. Como se ha podido ver, tenemos adversarios con muy mala idea que están esperando cualquier error o vulnerabilidad para hacer un daño real a MAPFRE. El año 2020 está siendo tremendamente exigente para toda la compañía. Nadie habría podido prever una pandemia a nivel mundial y un ataque de *ransomware* el mismo año. Desde el punto de vista del despliegue tecnológico para permitir trabajar en casa, recuerdo esos días muy intensos en los que varios compañeros de la Dirección Corporativa de Seguridad realizaron un trabajo espectacular.

CHEMA GARCÍA RODRÍGUEZ
SUBDIRECTOR DE SEGURIDAD. ARQUITECTURA TECNOLÓGICA DE SEGURIDAD

No puedo estar más agradecido y orgulloso de las personas con las que trabajé durante esos días tan intensos. El nivel de compromiso, la dedicación, la comprensión de la situación, la paciencia, etc., de las distintas áreas —seguridad, tecnología, negocio— y de los proveedores externos fue asombrosa y me hace estar tremendamente orgulloso del lugar en el que tengo que trabajar.

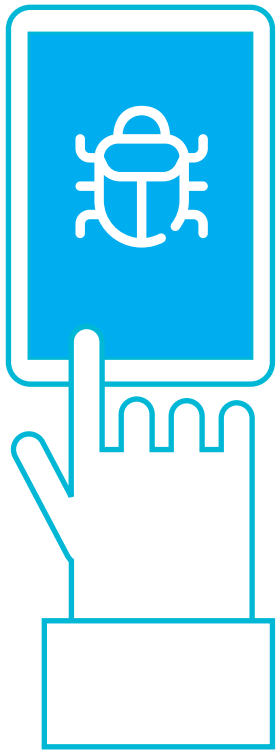
¿POR QUÉ SE PRODUJO ESTE CIBERATAQUE Y POR QUÉ FUE EN ESE MOMENTO CONCRETO?

Nos lo explica muy bien **Daniel Largacha,** director del SOC Global

"En los inicios de Internet el cibercrimen estuvo muy enfocado en el sector bancario por la facilidad de monetizar los ataques, robaban claves de acceso y ya podían obtener un rédito económico. Sin embargo, con el tiempo el sector bancario se ha robustecido mucho y el cibercrimen ha buscado nuevas formas de monetizar los ataques. En esta búsqueda han encontrado un filón en otras empresas pues fuera del sector bancario la madurez de la ciberseguridad es inferior. Además, hay una gran dificultad de trazabilidad de los cibercrímenes, tanto por la aparición de las criptomonedas como por la falta de una legislación o acuerdos globales que faciliten la persecución de estos ataques. Y por último las empresas ahora tienen una enorme dependencia de la información digital y las redes.

Esto ha propiciado un nuevo modelo de crimen, en el que los cibercriminales cifran la información y servidores de las empresas y les solicitan un dinero para que estas la puedan recuperar. Todo estaba perfectamente pensado, no es casual que el ataque a MAPFRE ocurriera un viernes de agosto por la tarde, pues sabían que la disponibilidad de efectivos para poder hacer frente a esta situación iba a ser menor que en cualquier otra época.

Y como nos matiza Carlos Muñoz, sabían que su amenaza era grande pues el ataque iba a "Afectar a la reputación de MAPFRE, al dejar sin servicio a nuestros clientes en fechas en que la mayoría utilizan el vehículo y la probabilidad de necesitar nuestros servicios aumenta de manera exponencial."



ESTA VIVENCIA NOS HA UNIDO Y REFORZADO MUCHO MÁS COMO EQUIPO

Primer minuto de sorpresa (por el tipo de ataque, *ransomware*), preocupación y luego, lo de siempre: a remangarse. En mi caso ese día empezaba mis vacaciones con mi familia y lo que hicimos fue cancelar mis planes y acondicionar de urgencia las infraestructuras de la casa en que veraneábamos para el teletrabajo ya que la cobertura es muy mala en esa zona, hasta poder organizarnos para volver a Madrid.

Creo que el mejor aprendizaje es el humano ya que los criminales atacaron MAPFRE y quizás lo que no esperaban era una respuesta institucional, transparente y contundente: MAPFRE no atiende al chantaje. MAPFRE se cierra como una piña, se hace fuerte, rehaciéndose de nuevo con mucho sufrimiento, esfuerzo y dedicación; creo que esto es lo que nos diferencia y lo que quizás no tuvieron en cuenta... no solo han atacado a MAPFRE como ente empresarial, han atacado nuestra CASA a nuestra FAMILIA, eso es lo que nos ha dado la fuerza a todos y con ese sentimiento de pertenencia nos hemos unido para defendernos.

Debemos plantearnos de forma general la necesidad de prepararnos, al nivel que cada uno podamos, para el nuevo escenario tecnológico en el que nos movemos. La mayoría de nosotros, que no somos nativos digitales por la época en la que hemos nacido/crecido, estamos acostumbrados a que la tecnología es algo que no entendemos mucho y que sufrimos en cierta medida. Hay que asumir que la tecnología, para bien y para mal, está en casi todo lo que hacemos y debemos interesarnos por ella para acomodarla adecuadamente dentro de nuestra vida, perdiéndole el miedo y sacándole más provecho.

MARISA MAÍZ LÓPEZ
DIRECTORA SOPORTE USUARIOS
DIRECCIÓN DE OPERACIONES
MAPFRE ESPAÑA

Las personas MAPFRE somos de espíritu fuerte y eso es tener mucho ganado para la lucha de la vida, que es preciosa, pero no lo pone fácil, y el 2020 es un buen ejemplo de ello. Así que no nos queda más remedio que pelearlo.

NO ESPERABAN UNA RESPUESTA INSTITUCIONAL, TRANSPARENTE Y CONTUNDENTE

TODO EL MUNDO APORTÓ EL 200% PARA RESOLVER LOS PROBLEMAS

Los primeros días fueron muy intensos, el ataque tuvo lugar según empezaba las vacaciones y recuerdo una llamada de Daniel Largacha (director del SOC Global) ya por la noche, comentándome que se habían cifrado equipos Windows y que todavía estábamos en el proceso de determinar el impacto operativo. A partir de ese momento nos pusimos manos a la obra y empezamos a tener varias reuniones en paralelo todos los implicados en la gestión del incidente. Aplacé todos los compromisos y estuve disponible día y noche para ayudar a solventar el problema.

Sin duda eligieron agosto porque la gente está de vacaciones y el seguro es crítico en época vacacional, pero aun estando de vacaciones, todo MAPFRE respondió al ataque e hizo lo imposible por dar servicio a nuestros clientes.

Hemos aprendido que podemos salir de un incidente de seguridad importante, incluso en contexto de pandemia mundial y trabajando en remoto. Hemos aprendido que con esfuerzo e implicación, teniendo un equipo humano comprometido y dispuesto a ayudar, se sale adelante aunque existan dificultades.

Es crucial que pongamos nuestro granito de arena en proteger esa información confidencial que sabemos que manejamos, en analizar atentamente ese correo que nos llega o esa web que nos piden abrir. Siempre que desconfiemos de algo, debemos notificarlo a la dirección corporativa de seguridad y medio ambiente por medio de los canales establecidos.

Lo importante es que todo el mundo aportó el 200% para resolver los problemas, y ya solo por eso sabemos que en el futuro ante situaciones difíciles harán lo mismo. Eso es importante y motivo de orgullo de organización, de compañía.

OMAR RODRÍGUEZ SOTO
HACKING ÉTICO Y CIBERINTELIGENCIA
DIRECCIÓN CORPORATIVA
DE SEGURIDAD

Tú no controlas a los atacantes que deciden atacarte, pero sí tus actos. Muchas veces el cambio empieza por uno mismo, cuando estás en una situación complicada en vez de señalar las cosas que fallan, es importante hacer todo lo posible por resolver la situación.

ME PARECIÓ ADMIRABLE LA VALENTÍA DE MAPFRE HACIENDO PÚBLICA LA SITUACIÓN

Me impactó muchísimo y será un momento que recordaré siempre. Imagínate, en plenas vacaciones era difícil creer la llamada que estaba recibiendo, pero a pesar de esa sensación de incredulidad y de incertidumbre nos pusimos manos a la obra casi sin pensarlo para minimizar el daño y colaborar con el resto de equipos. Era algo con lo que no contaban los ciberdelincuentes.

En MAPFRE ya estábamos preparando un nuevo modelo para abordar nuestro desempeño de forma remota y presencial, y gracias a ello las ideas estaban avanzadas, aunque ese cambio hemos tenido que acelerarlo de forma exponencial.

Es fundamental seguir las indicaciones y recomendaciones en los distintos canales de nuestra Dirección de Seguridad Corporativa, ellos son los verdaderos expertos en esta materia. Y es nuestra responsabilidad como empleados cumplir y fomentar estas normas ya que estoy convencida de su efectividad.

Me pareció admirable la valentía de MAPFRE haciendo pública la situación por la que estábamos pasando; me siento muy orgullosa de pertenecer a esta gran familia.

PATRICIA MOCHALES SEN
DIRECTORA DE TECNOLOGÍA. TI GESTIÓN TERRITORIAL, IMPLANTACIONES Y WORKPLACE

Jeff Bezos dijo una vez: "Si decides hacer solo las cosas que sabes que van a funcionar, dejarás un montón de oportunidades encima de la mesa". En torno al puesto de trabajo se ha implantado en MAPFRE una tecnología nueva que nos ayudará si así lo requiere este futuro que sigue presentándose incierto; creemos en ella y trabajamos sin descanso para que todos prestemos el mejor servicio a nuestros clientes.

KEEP CALM AND LAUGH

ESTA SITUACIÓN NOS HA DEJADO MOMENTOS DE PROFESIONALIDAD, DEDICACIÓN Y SOLIDARIDAD INCREÍBLES

La verdad es que las vacaciones ya eran un poco extrañas por la situación actual, pero la primera reacción fue de cierta incredulidad. ¡Después de pasar esos meses tan complicados nos estaba pasando algo así! Para mí lo peor fue la incertidumbre de las primeras horas, la información sobre el alcance real se obtenía de forma más lenta de lo que todos queríamos y nuestra obsesión era recuperar la normalidad cuanto antes y con la garantía de que no volviéramos a ser atacados.

ALFREDO G. CASTAÑEDA SARACHAGA
ACTP - SIC - TECNOLOGÍA DE RED Y CONTACT CENTER

En estos momentos tan duros, además de mantener la calma nunca hay que perder ni la capacidad de autocrítica ni el sentido del humor. Lo primero nos encamina a la excelencia, y lo segundo nos ayuda a relativizar las cosas ¡y nos hace más felices!

Pero no quedaba otra, así que apretamos los dientes y todo el equipo se implicó al 100% aportando lo mejor de sí mismos, ¡un ejemplo de dedicación!

¡Hemos aprendido muchísimo! Parece duro decirlo, porque no deseamos a nadie que pase por ello, pero desde un punto de vista estrictamente profesional esta situación nos ha enriquecido enormemente: nos ha dejado momentos de profesionalidad, dedicación y solidaridad increíbles y hemos ganado un nivel de conocimiento de este tipo de problemas, e incluso de nuestro propio ecosistema interno, que nos prepara aún mejor para afrontar el futuro.

Por desgracia, la protección total no existe, por ello, la labor divulgativa que realizan nuestros compañeros de la Dirección Corporativa de Seguridad es magnífica para entender las mejores prácticas y actitudes que todos debemos adoptar en nuestro ámbito tanto profesional como personal y familiar.

DANIEL LARGACHA
DIRECTOR DEL SOC GLOBAL

Me gusta ser positivo, y además creo que de todo se aprende. Yo me atrevo a afirmar que de este ataque hemos salido mucho más fortalecidos de antes, la experiencia y los medios que MAPFRE ha dispuesto nos permiten afrontar el futuro desde una posición mucho más favorable y optimista.

TENEMOS QUE PROTEGER A LA EMPRESA DE LAS CIBERAMENAZAS

En mi caso estaba con un permiso de paternidad y ya desde los primeros momentos me podía imaginar la gravedad de la situación así que, sin esperar mucho a tener una foto completa, hice las maletas, me despedí de mi familia, activé a mi equipo y puse rumbo a Majadahonda.

Lo cierto es que lidiar en este tipo de situaciones es parte de mi trabajo. Todos los que trabajamos en ámbitos en los que se gestionan crisis, de cualquier tipo, sabemos que, aunque remota, existe la posibilidad de que te tengas que activar en cualquier momento. Afortunadamente para mí, MAPFRE decidió hace un tiempo disponer de personas preparadas para enfrentarse a ese tipo de escenarios.

Este tipo de situaciones te pone enfrente de un espejo y te hace ver tus debilidades, pero también tus fortalezas. MAPFRE ha demostrado que tiene un equipo humano y unos medios que le otorgan una enorme capacidad de recuperación. Esto nos ha permitido sobreponernos en un tiempo más que razonable.

De la misma forma que protegemos a nuestra empresa de otros riesgos (clientes no rentables, la competencia del sector, malos proveedores, etc.) tenemos que proteger a la empresa de las ciberamenazas.

El confinamiento fue un gran reto para MAPFRE y otro ejemplo de su capacidad para adaptarse rápidamente a un entorno cambiante.

Este escenario también nos tocó vivirlo en primera línea y, al igual que en el ciberataque, me impresionó la capacidad, profesionalidad y disposición del equipo humano. Diferentes áreas se alinearon y se coordinaron para conseguir un objetivo muy ambicioso y retador: conseguir en apenas dos semanas que toda una empresa pudiera teletrabajar a nivel global. No me canso de afirmar que me siento muy orgulloso de trabajar en una empresa con este grandísimo equipo.

LIDIAR EN ESTE TIPO DE SITUACIONES ES PARTE DE MI TRABAJO

ELENA MORA GONZALEZ
DIRECTORA DE PROTECCIÓN Y PRIVACIDAD DEL DATO

Hay que conseguir que todos los empleados sean auténticos *firewall* humanos que impidan la entrada de los ciberdelincuentes y para eso es imprescindible la concienciación e implicación de todos en el cumplimiento de las normas y políticas de la compañía.

NO ERA EL MOMENTO DE PREOCUPARSE SINO DE OCUPARSE DE LA SITUACIÓN

Ese momento es difícil de describir, de los que quedarán grabados en mi memoria. Aunque todos los que trabajamos en seguridad somos conscientes de que situaciones de este tipo pueden ocurrir, no esperas que lleguen a materializarse y menos aún que te pille en medio de las vacaciones.

En mi caso, me encontraba con mi familia en Oviedo y ese viernes, cuando recibí la llamada, me invadieron pensamientos y sentimientos muy diferentes. Lo primero en que pensé fue en el efecto sobre los sistemas operativos y la disponibilidad de la información y, a la vez, otro aspecto prioritario: la protección de los datos de nuestros clientes y cómo este hecho podía afectar a dichos datos y a la reputación de la compañía.

Teníamos claro que no era el momento de preocuparse sino de ocuparse de la situación. La rapidez en la respuesta es el factor clave y primordial en la gestión de estas crisis.

Es fundamental el trabajo en equipo y contar con unos compañeros como los que tenemos, con una profesionalidad increíble, pero sobre todo con un nivel de compromiso y calidad humana difícilmente superable. Gracias a todo esto, hoy podemos estar hablando de esta situación en pasado.

Una de las enseñanzas ha sido que lo improbable puede ocurrir y que hay que estar preparado para lo impensable. La capacidad de reacción y adaptación debe ser cada vez mayor y los tiempos de respuesta cada vez más cortos.

De ahí la importancia de tener unos buenos planes de contingencia y continuidad de negocio. Planes que, con y sin coronavirus, siempre han estado y tienen que estar sujetos a un proceso de actualización y mejora continua. Los ciberdelincuentes están siendo extremadamente creativos al idear nuevas formas de aprovecharse de los usuarios y hacen un mayor uso de tecnologías cada vez más novedosas.

EMPLEADOS "FIREWALL" QUE IMPIDAN LA ENTRADA DE CIBERDELINCUENTES