# CIBERSEGURIDAD

## ¿quién nos protege?


**El pasado mes de mayo, el virus Wannacry infectó alrededor de 230.000 equipos en más de 150 países, paralizando la actividad de empresas, organismos y servicios públicos. Los expertos aseguran que es solo un anticipo de lo que viene. ¿Estamos preparados para afrontar esta amenaza global? Seis compañeros que velan por la ciberseguridad en MAPFRE nos lo cuentan.**

TEXTO **MARÍA JESÚS PÉREZ FUENTES Y ANDREA BURGUI** | ILUSTRACIONES **THINKSTOCK**

Ciberriesgos, *spyware, ramsonware*... seguro que últimamente estos términos te resultan muy familiares. Pues bien, la ciberseguridad no es una materia de nueva creación, lleva entre nosotros desde finales de la década de los 90, aunque es ahora cuando se ha colado en la agenda de todos los comités directivos de las empresas a nivel mundial.

En MAPFRE nos tomamos muy en serio la confidencialidad y protección de los datos de nuestros clientes, así como todas aquellas amenazas que puedan poner en riesgo el normal funcionamiento de nuestra actividad. Por eso, contamos con un amplio equipo especializado en este ámbito repartido por todo el mundo, del que hoy te presentamos una pequeña muestra.

"Todos los años oímos noticias sobre incidentes en ciberseguridad que tienen un gran impacto negativo. En ocasiones, las empresas no puede recuperarse del ataque y finalmente, cesan su actividad.

EN MAPFRE EXISTE PLENA COORDINACIÓN ENTRE **LA DIRECCIÓN DE SEGURIDAD Y MEDIO AMBIENTE (DISMA)** Y LOS EQUIPOS LOCALES

Está claro que las brechas de seguridad ya no son una amenaza, sino un hecho", dice **Tuncay**, de MAPFRE SIGORTA, que nos adelanta la situación de vulnerabilidad que se ha hecho tan evidente en los últimos meses.

En un mundo hiperconectado cada vez son más las ciberamenazas a las que se ven expuestas las organizaciones. Ante este escenario global, se ha profundizado en la metodología y procedimientos para llevar a cabo distintos análisis de ciberriesgos que puedan generar una pérdida financiera o de información almacenada, interrumpir el negocio o producir un daño reputacional irreparable.

"Las organizaciones cada día están más expuestas al exterior, por lo que aumenta la superficie de ataque y por tanto, la probabilidad de sufrir un incidente", nos cuenta **Ignacio**, desde la Dirección de Seguridad y Medio Ambiente (DISMA) en Madrid. Además, incluye otro elemento preocupante de esta ecuación: "Aparte de los *malos* de siempre, se han unido mafias, empresas o incluso gobiernos que intentan dañar la reputación de la competencia, robar información u obtener un beneficio rápido. Incluso hay empresas que ofrecen este tipo de servicios paquetizados. Hablamos de la industrialización del cibercrimen, donde todo se compra y se vende".

Precisamente, así surgió el ya famoso *WannaCry*, el software malicioso de tipo *ransomware* que el pasado mes de mayo puso en jaque a las empresas y organismos de medio mundo.

"El principal reto consiste en ser capaces de proveer un nivel de protección homogéneo, global e integral en todo el Grupo, adecuado a las necesidades de negocio de la compañía (...) Ser capaces de coordinar respuestas tempranas y coordinadas es clave para minimizar el impacto

de estos ataques", explica **Juan Manuel**, de MAPFRE USA.

"Yo diría que actualmente el foco está puesto en el Internet de las Cosas (IoT), porque cada vez tenemos más dispositivos con conexión a Internet, y muchos de ellos salen al mercado con posibilidades acotadas o inexistentes de actualización y/o parcheo de seguridad. Esto hace que, ante el descubrimiento de una brecha de seguridad, se pueda acceder a ellos y ser utilizados remotamente por gente malintencionada", afirma **Gustavo**, de MAPFRE ARGENTINA.

**Yuli**, de MAPFRE PERÚ, nos cuenta que a diferencia de Europa, el foco de los ataques en su país, generalmente son las personas y las pymes. "Pero si hablamos de grandes empresas, el principal objetivo son las del sector financiero o cajeros automáticos".

Tanto ella, como Tuncay e Ignacio, afirman que Wannacry ha sido el mayor reto al que se han enfrentado a lo largo de su carrera.

"Las empresas tradicionales cuentan con una gran obsolescencia tecnológica, siendo grandes elefantes difíciles de mover", dice **Omar** desde Madrid. "Todos estos ataques requieren que los equipos de seguridad trabajen de forma coordinada, compartiendo

EN SEGURIDAD, SE APLICAN CRITERIOS COMUNES EN TODAS LAS EMPRESAS DEL GRUPO, PERO, A LA VEZ, SE GARANTIZA LA FLEXIBILIDAD NECESARIA PARA ADECUARSE A LAS NECESIDADES PARTICULARES DE CADA COMPAÑÍA A NIVEL LOCAL

información para hacerles frente y protegiendo a sus clientes y procesos de negocio".

"El problema", señala Ignacio, "es que históricamente, se trata de un ámbito en el que se tiende a ser más reactivo que preventivo. Muchas empresas no invierten hasta que no sufren un gran impacto por un incidente de seguridad".

"Siendo sinceros, falta mucho recorrido en las empresas. La seguridad cuando más importa, es cuando tienes un problema y mientras no lo tienes, dan más importancia a potenciar la experiencia digital u otro objetivo empresarial. Hay que encontrar el equilibrio entre seguridad y funcionalidad", añade Omar.

"Afortunadamente, MAPFRE cuenta con un gran equipo de profesionales que permite que, a partir de la coordinación desde la DISMA, la aplicación de criterios comunes, integrales y homogéneos sean una realidad en todas las empresas del Grupo, mientras que garantizamos la flexibilidad necesaria para poder adecuarnos a las necesidades particulares de cada compañía a través de los equipos locales", destaca Juan Manuel, especialmente orgulloso del trabajo que su equipo realiza en Webster, Miami y Puerto Rico.

Aunque con algunas diferencias, nuestros Protagonistas desarrollan en su día a día las siguientes funciones: Monitorización de todo el perímetro de la de red de MAPFRE en el mundo, bloqueo de posibles amenazas, aplicación de medidas de seguridad, mantenimiento continuo de los protocolos de seguridad, gestión y control de usuarios y accesos, análisis de riesgos operacionales de TI y de incidentes de seguridad, control de alertas, o análisis de impacto de negocio, entre muchas otras.

Cualquier amenaza de ciberseguridad debe ser tratada con precaución ya que se puede propagar rápidamente por todo el ecosistema digital y provocar así un fallo sistémico. "El reto es justamente cuidar la confidencialidad, integridad y disponibilidad de la información así como estar preparados para seguir operando en caso de algún incidente importante", destaca Gustavo.

En este sentido, lo que se pretende es que la seguridad de nuestros productos y

### LOS CASOS MÁS MEDIÁTICOS

**Yahoo:** sufrió el robo de más de un millón de contraseñas y datos de cuentas de usuarios en 2013 y 2014, siendo el mayor caso de piratería informática de la historia a una empresa.

**WannaCry:** afectó el pasado mes de mayo a hospitales de la red pública de Reino Unido, a Telefónica en España, así como grandes corporaciones de Rusia, Turquía, Alemania y Vietnam. Se estima que infectó más de 230.000 ordenadores en más de 150 países.

**HBO:** la corporación sufrió el pasado agosto un ataque informático que tuvo como consecuencia el robo de 1,5 terabytes de información, y material inédito de su serie estrella *Juego de Tronos*.

servicios sea percibida como una ventaja competitiva, tal y como nos explica Juan Manuel. "La aplicación de criterios de seguridad en el desarrollo de cualquier iniciativa de negocio ya no es solo una necesidad, sino un factor diferencial frente a nuestros clientes, reguladores y grupos de interés, que cada vez más nos demandan y valoran la seguridad como un elemento clave en los productos que ofrecemos".

En concreto, en el sector asegurador se manejan datos de clientes, protegidos por distintas leyes en materia de protección de datos, por lo que cualquier incidente que pueda suponer una filtración al exterior de los mismos es una amenaza grave, como nos explica Ignacio.

Los ciberseguros y el sector asegurador en general desempeñan un papel fundamental en la economía de cualquier país. La constante evolución digital en la que vivimos, la existencia de un entorno empresarial cada vez más informatizado, digitalizado e interconectado y el incremento del número de siniestros en todo el mundo, hace prever un constante crecimiento de los seguros de ciberriesgos que, presumiblemente, ascenderá a 20.000 millones de euros en unos diez años.

"Debido a la cantidad de pérdidas que generan en el mundo y la incapacidad de respuesta rápida de las empresas ante un incidente como WannaCry, el ciberseguro sería parte de la cultura de prevención de las empresas", apunta **Yuly**.

### SEGURO DE CIBERRIESGO

El pasado mes de marzo MAPFRE lanzó en España un seguro de ciberriesgo para pymes y autónomos que permite hacer frente al robo de datos y de información confidencial.

Además, ofrece protección ante las pérdidas económicas que pueda sufrir un negocio a causa de los daños informáticos, ayuda para hacer frente a una amenaza de extorsión cibernética, asesoría legal y servicio de restauración del software, entre otros.

"Para MAPFRE, los clientes son el primer objetivo, la ciberseguridad está incorporada a nuestro compromiso de calidad y trabajamos siempre para que, pase lo que pase, ellos estén protegidos y nosotros sigamos atendiendo el servicio que prestamos", indica **Guillermo Llorente**, subdirector general de la Dirección de Seguridad y Medio Ambiente de MAPFRE y máximo responsable de seguridad en la compañía.

### PRINCIPALES RIESGOS DE UN CIBERATAQUE

PERFILES

## GUSTAVO LORENZI

GERENTE DE SEGURIDAD INFORMÁTICA Y MEDIO AMBIENTE, MAPFRE ARGENTINA

Este ingeniero en electrónica especializado en Telecomunicaciones lleva once años dedicándose a la ciberseguridad. Actualmente, nos cuenta que sigue formándose para no quedarse *obsoleto* gracias a la formación permanente que le ofrece la DISMA.

Siempre le interesaron los temas de seguridad informática, sin embargo, cuando comenzó su andadura en MAPFRE en 1991, todavía no existía una función específica dedicada enteramente a ello. En un primer momento se dedicó al cifrado de las comunicaciones en las oficinas comerciales, la implementación de sistemas de control de navegación y otras tareas que más tarde le llevaron al área de seguridad de la cual está a cargo hoy en día.

Gustavo considera que el mayor reto de su carrera profesional ha sido la creación y puesta en marcha del departamento de Seguridad de la DISMA en Argentina en 2007.

## YULI MARLENE DE LA CRUZ GIL

ANALISTA DE RIESGO OPERACIONAL DE TECNOLOGÍA DE TI, MAPFRE PERÚ

Yuli se dedicó en un principio al desarrollo de tecnologías de información y redes de informática y fue entonces cuando le picó la curiosidad y comenzó a interesarse por la ciberseguridad, sector en el que lleva trabajando cuatro años.

Afirma que una de las razones por la que le gusta tanto su profesión es porque la tecnología es cambiante, que la obliga a prepararse constantemente. En estos últimos meses, tras los acontecimientos ocurridos en mayo, su principal reto ha sido profundizar en los procesos a corto plazo para poder ofrecer controles adecuados a los nuevos riesgos.

Actualmente, contribuye en la actualización del Plan de Continuidad de Negocio de Perú y en la realización de análisis de impacto de negocio.

## IGNACIO GARCÍA-MONEDERO HIGUERO

RESPONSABLE DE MONITORIZACIÓN Y GESTIÓN DE INCIDENTES DE SEGURIDAD EN EL CENTRO DE CONTROL GENERAL, DISMA, MAPFRE S.A.

Ignacio es licenciado en Ingeniería Informática y lleva 15 años en el sector. Desde entonces, no ha dejado de formarse a través de certificaciones o de forma autodidacta, dedicando, tal y como él dice, "muchas noches" a intentar estar al día de todo lo relacionado con la seguridad informática, sistemas de la información, software libre, etc.

Se incorporó a MAPFRE hace dos años, pero nos cuenta que está sumergido en este *mundillo* desde que tiene uso de razón porque siempre le ha atraído la tecnología. Ignacio califica su día a día como "una locura", pero su labor, como la del resto de compañeros, es esencial para detectar y eliminar amenazas y evitar que tengan impacto alguno en la organización.

## OMAR RODRÍGUEZ SOTO

TÉCNICO DE SISTEMAS DE SEGURIDAD EN EL ÁREA DE RIESGOS E INTELIGENCIA DE LA DISMA, MAPFRE S.A.

Aunque estudió Administración de Sistemas Informáticos y ha obtenido varias certificaciones, Omar considera que los conocimientos más complejos sobre seguridad los aprendió de forma autodidacta trabajando en proyectos de código abierto y como *freelance.*

Omar nos cuenta que su interés por estos temas comenzó como afición a los 12 años, y a partir de ahí invirtió gran parte de su juventud delante de un ordenador, "cuando esto del *hacking* era muy minoritario".

Paradójicamente, también nos explica que de pequeño participaba en *chats* de *hacking* ético, materia a la que se dedica actualmente en MAPFRE, gestionando a un grupo de *hackers* que se encargan de proteger la empresa.

## TUNCAY KEBELI

JEFE DE SEGURIDAD, MAPFRE SIGORTA

Tuncay lleva casi dos años dedicándose a funciones de seguridad en nuestra compañía en Turquía, algo de lo que dice sentirse "feliz y orgulloso". Cuenta con más de 16 años de experiencia en este ámbito, cuyos seis últimos han sido dedicados al campo de la información y de los sistemas de seguridad.

Acerca de su profesión, afirma que decidió dedicarse a ella porque realmente es su vocación. Ante los últimos hechos ocurridos, Tuncay defiende que no importa lo grande o pequeña que sea una empresa, es imprescindible tener un plan para garantizar la seguridad de sus activos.

## JUAN MANUEL MUÑOZ PERALES

DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, MAPFRE USA

Juan Manuel comenzó a trabajar en el ámbito de la Seguridad en 2002. En 2007 se incorporó a MAPFRE, aunque ya previamente había realizado colaboraciones con la compañía.

Actualmente, dirige la función de Seguridad y Medio Ambiente de MAPFRE en Norteamérica, encargándose de, entre otros, gestionar las necesidades, equipos y actuaciones en materia de seguridad.

Juan Manuel destaca que las personas que conforman MAPFRE son el principal y más importante mecanismo de defensa ante las amenazas, y que las campañas de concienciación son esenciales, aparte de las medidas de protección ya configuradas en los equipos y servidores de la compañía.