EQUIPO SIC – José M. Vera, Ana Adeva

¿Qué hay de nuevo, viejo?

En España operan cerca de cuarenta prestatarias de servicios de ciberseguridad gestionada españolas y extranjeras. Algunas –se pueden contar con los dedos de una mano– fueron pioneras a finales del siglo XX y primeros del XXI en esta actividad, ya se dedicaran en exclusiva a la ciberseguridad, ya la incluyeran como una de sus líneas de oferta TIC. Y todavía con menos dedos se pueden contar los MSSPs que solo se dedican a tal menester.

Hoy, el mercado de MSSPs es amplio y variado: tiene actores de todos los tipos: grandes (operadores de telecomunicaciones, *big four*, empresas de IT e integradores) y pymes, con un catálogo muy completo que aspira a atender las necesidades en todos los escenarios o con uno muy especializado en algunos frentes y en nube; prácticamente todos disponen de la macroherramienta principal de un MSSP, el SOC (en paralelo y bien separado de los servicios de CERT), y no pocos tienen varios centros en distintos países para prestar servicios a sus clientes multinacionales (también para ganar posición en estos mercados domésticos). Y cuando esto no es suficiente para acompañar a los grandes contratistas, estos prestatarios firman acuerdos de colaboración con otros MSSPs para una cobertura más amplia y rápida.

Como en todo mercado explosivo (y el de los servicios de ciberseguridad lo lleva siendo años), hay una cierta sobreoferta específicamente de proveedores de seguridad gestionada. Sin embargo, las empresas que conforman la "creme de la creme" suelen exhibir rasgos diferenciales que todo buen contratista no motivado exclusivamente por el precio debería apreciar, más allá de las referencias y la fortaleza financiera; a saber: capacidades tecnológicas propias refinadas orientadas a la gestión del servicio con intervención del cliente si así se ha contratado; un equipo de especialistas estable en todas las actividades que componen la cadena de valor del servicio gestionado; tener posibilidad de auditar los procesos del servicio en base al alcance del mismo; y garantías reales de poder prestar servicio ante situaciones de crisis en las que el número de clientes afectados rebase cierto umbral o los afectados sean organizaciones de grandes dimensiones y/o concentrados en sectores estratégicos.

Aunque ya tratado con anterioridad en otras ediciones de la revista y en eventos *ad hoc* de SIC, a modo de puesta al día, en las siguientes páginas se repasa el panorama actual y evolutivo de los MSSPs aunque sin ánimo de conformar una guía ni de elaborar una taxonomía de los mismos y, por supuesto, sin meter el dedo en el futuro a medio plazo, en el que el imperio de la nube, el 5G, la convergencia IT-OT-IoT, la conformación de entidades inteligentes y el avance de la robotización y la domótica le darán a la seguridad gestionada otra vuelta de tuerca.

* Es posible obtener una versión en pdf de este especial rellenando el formulario disponible en www.revistasic.com

Ciberseguridad gestionada por terceros: tecnologías a la carta, automatización, orquestación e inteligencia para apoyar el día a día y la toma de decisiones de los CISOs

"La vida es el proceso de pasar de la certeza absoluta a la completa ignorancia", decía irónicamente el actor Richard Dreyfuss, protagonista de Tiburón, una idea exportable al mundo digital, cada vez más complejo de proteger. Al igual que las empresas confían 'en terceros' para tener luz, agua, red de ordenadores, telecomunicaciones o cubrir necesidades relacionados específicamente con su área de actividad, también la contratación de ciberprotección gestionada a los proveedores de servicios de seguridad gestionada (MSSPs según el acrónimo en inglés) se ha convertido en una práctica de externalización de rápida consolidación en grandes clientes (no en la pyme) por sus evidentes ventajas (especialización, eficiencia, pago por uso…) frente a formulas exclusivas "in house". El tema, ya abordado con intensidad por SIC en ediciones pasadas de su revista y eventos concernidos, aunque enfila hacia su madurez, aún sigue precisando de puesta al día. En las siguientes páginas se da buena cuenta de ello.

El de los MSSPs es un nicho de mercado que goza hoy de buena salud, en el que los jugadores provienen de distintos ámbitos de actividad: operadores de telecomunicaciones, grandes compañías de IT, proveedores de servicios de Internet, integradores, empresas especializadas en servicios de seguridad en nube, consultoras…

Para 2022, se espera que crezca más de un 16% anualmente, moviendo 36.000 millones de euros, según Allied Market Research. La razón es que los costes de la ciberseguridad, a causa de amenazas más complejas, automatizadas y dirigidas, harán que las empresas prefieran optar más por la seguridad 'administrada' y 'como servicio'… y dedicar los máximos recursos al negocio.

SUMARIO

Qué es un MSSP

Según la firma analista Gartner, "un proveedor de servicios de seguridad gestionada (MSSP) proporciona supervisión y administración de dispositivos y sistemas de seguridad, de forma subcontratada", destaca en su diccionario de terminología la consultora. "Sus servicios incluyen la gestión de los cortafuegos, sistemas de detección de intrusiones, de las redes privadas virtuales, de escaneo de vulnerabilidades y de servicios de antivirus. Los MSSP utilizan centros de operaciones de seguridad de alta disponibilidad (ya sea de sus propias instalaciones o de otros proveedores de centros de datos) para proporcionar servicios 24x7, diseñados para reducir la cantidad de personal de seguridad operacional que una empresa necesita para contratar, capacitar y retener con el fin de mantener un nivel de ciberseguridad aceptable".

1 Los servicios de seguridad gestionada, la mano derecha del CISO

Cuando, en 1876, **Alexander Graham Bell** inventó el teléfono no era consciente de que, aparte de comunicar al mundo, estaban dando pie al primer gran servicicio gestionado: la telefonía fija. Nueve años después, la compañía **AT&T** comenzó a ofrecer a los usuarios este servicio a través de una cuota fija.

El origen de los MSSP empezó a mediados de los años 90, cuando los operadores de telecomunicaciones y proveedores de servicios de Internet (ISP) ofrecían seguridad a través de la gestión de los cortafuegos de terceros que vendían. Después, se pasó a prestar monitorización y administración remota de servidores y redes por parte de los proveedores de servicios de aplicaciones (ASP). Su trabajo sentó las bases de las empresas que ofrecían soporte en remoto para la infraestructura de TI de los clientes.

Madurez MSSP

Tras casi tres décadas de vida, la consultora **Gartner** cree que el mercado de los proveedores de seguridad gestionada está "maduro", con un volumen de negocio que rondó los 9.500 millones de euros en 2018. Y continuará creciendo. La ciberseguridad está pasando de ser una compra a un 'alquiler', incluyendo su gestión.

La externalización de servicios es una constante en la economía actual por lo que crece el número de empresas que recurren a ella por su buena relación calidad/precio. En un mundo cada vez más complejo, los MSSP ofrecen actualizaciones continuas de software de seguridad, capacidades y servicios bajo demanda de los que gran parte de las empresas no pueden disponer de forma interna por su elevado coste. A los servicios de gestión de hardware y software tradicional se suman ahora los de 'caza de amenazas', gestión de incidentes, forensía... La clave es ofrecer monitorización continua, detección temprana y respuesta ante amenazas.

Su oferta se incrementa más allá de la oferta clásica de supervisión de eventos de seguridad en el perímetro de la empresa, lo que está dando lugar a servicios gestionados en la nube (tanto SaaS, como IaaS), en entornos conectados (IoT) e industriales (ICS/SCADA).

Así pues, la 'ciberseguridad en remoto' gestionada por terceros especializados va a convertirse en la gran protagonista del mercado: ya se puede subcontratar el SOC virtual (vSOC), el responsable de seguridad (vCISO), de Protección de Datos (vDPD), etc. "Continuamente nos enfrentamos a nuevos riesgos, cada vez más sofisticados, y es muy complicado para un responsable de ciberseguridad gestionarlos todos: porque están en la nube, en la cadena de suministro, en socios...Para hacerles frente hay que ofrecer una respuesta diferente que te permita tener una primera, segunda y tercera línea de ciberprotección, flexible y dinámica", comenta el Chief Information & Innovation Officer (CIIO) de **AON**, **Pablo Montoliú**.

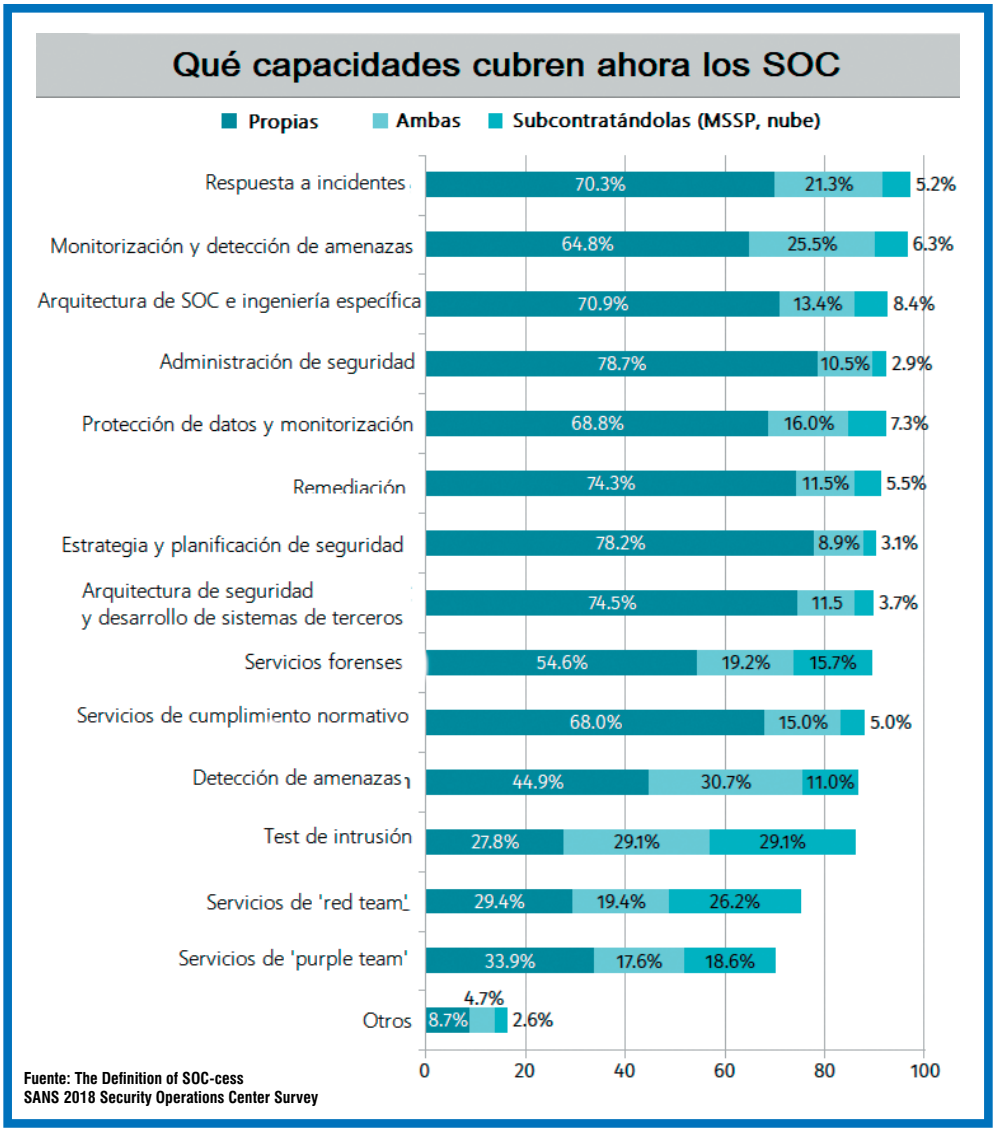
Automatizar lo rutinario

Pero no es un reto sencillo. "La adopción de servicios gestionados conlleva la transferencia de una parte del control de la segu-

ridad a una tercera parte. Por eso, determinar qué, cuándo y cómo es vital", destacan especialistas de **Deloitte**. "Las nuevas tecnologías, como la automatización e inteligencia artificial, están transformándolo todo y, también, el mundo de la ciberseguridad, donde será inviable optar por tenerlo todo 'en casa'", añade en uno de sus informes sobre MSSP. De otra parte, los jugadores "que se centren en la automatización de la seguridad y las funciones de detección y respuesta estarán preparados para el éxito basado en integrar elementos de automatización y orquestación para ofrecer servicios con un alto margen de mejora y adaptación a una gran base de clientes", afirma la consultora Gartner.

De hecho, la mayoría de los profesionales de la seguridad de la información en Europa creen que un ataque cibernético comprometerá las infraestructuras críticas en varios países en los próximos dos años, según el informe anual "The Cyberthreat in Europe", publicado el pasado noviembre por **Black Hat**. En el estudio, el 62% confesó que no tiene suficiente personal de seguridad para defenderse adecuadamente contra las ciberamenazas modernas y el 39% consideró que la falta de habilidades requeridas es la razón principal por la cual fallan las estrategias de seguridad. A ello se suma que casi seis de cada 10 expertos encuestados creen que no tienen el presupuesto necesario para defenderse de forma adecuada contra las amenazas actuales y emergentes.

En el sector privado, la principal preocupación es la interrupción del servicio, resalta uno de los últimos estudios de **Bitdefender,** en el que el 55% de los CISO consideran que es su gran riesgo, seguido de los costes de la pérdida de reputación por una brecha de seguridad (45%). En este sentido, un MSSP, como **S21sec**, "apuesta por ofrecer eficiencia ante la escasez de recursos, para hacer frente a un entorno cada vez más dinámico. Y hacerlo innovando a través de una plataforma de servicios, también con tecnología propia. Se trata de ofrecer una respuesta rápida y flexible adaptada al contexto de amenazas cambiantes, pudiendo disponer, según las necesidades del cliente, de capacidades y recursos acordes a su riesgo", indica el CEO de S21sec, **Agustín Muñoz-Grandes**. Un MSSP de valor "debe entender bien la gestión del riesgo, de forma medible y con procesos de mejora continuos", añade.



Fuente: The Definition of SOC-cess
SANS 2018 Security Operations Center Survey

'Palabra' del CCN

Por eso, organismos como el **Centro Criptológico Nacional** (**CCN**) consideran que, más allá de la seguridad tradicional, "ha llegado el momento de apostar menos por productos, como el antivirus, y más por servicios", comentó en la última edición de las Jornadas sobre el Sistema de Alerta Temprana (SAT), el Jefe del Departamento de ciberseguridad del CCN, **Javier Candau**. "La tecnología vale lo que vale el servicio. Ni una cosa más ni una cosa menos. Si no tienes servicio, nada te va a salvar", apostilla el CEO de **Aiuken**, **Juan Miguel Velasco**.

Y es que, en un mundo cada vez más complejo, descentralizado y con creciente exposición a riesgos tecnológicos y de negocio, los MSSP se han convertido en la "nueva alarma de la ciberseguridad", destaca el fundador y CEO de **Herjavec Group**, **Robert Herjavec.** La razón es sencilla: "te permite acceder a un mayor

nivel de seguridad con unos recursos limitados y sin la experiencia, ni talento necesarios".

Crecimiento de futuro

De momento, este mercado está creciendo en torno al 16% cada año. Y en él tienen cabida todo tipo de empresas: desde las que ofrecen seguridad a través de sus Centros de Operaciones de Ciberseguridad (SOC), hasta las que van más allá con inteligencia y respuesta ante incidentes a través de la analítica de grandes cantidades de datos, aprendizaje automático, protección especializada en el mundo OT e IoT, la salud, vehículos, fraude…

De hecho, se espera que los servicios globales de seguridad gestionada supongan, para 2028, un mercado de más de 90.000 millones de euros. No sólo es cuestión de estar seguro: en un mundo hiperregulado también es una forma de cumplir con las normativas.

Además, reducen la complejidad de hacerlas frente siempre con tecnología puntera. Actualmente el 40% de las empresas consideran que el incremento de complejidad tecnológica (por ejemplo, por la evolución hacia la nube) exige excesivos medios técnicos y de personal para que sea rentable hacerlo de forma interna. Así destaca por su flexibilidad –debido a que el proveedor de software gestiona la infraestructura– y permite incorporar sistemas escalables de forma sencilla y rápida, además de evitar el problema de tener que contratar todo tipo de tecnologías y licencias, ya que en gran medida se deja en su mano, siempre, claro está, con respaldo contractual.

Y es que los MSSP, que permiten aunar la ciberprotección en un solo proveedor, conlleva un factor importante de sencillez para la complejidad que supone enfrentarse con decenas de tecnologías a las amenazas más preocupantes. (Obviamente, siempre que esto sea acorde con la política del cliente en lo que toca a mantener la independencia efectiva del MSSP).

Un dato es aplastante: por cada 25% que se gana en funcionalidades con más sistemas de ciberseguridad, se incrementa el 100% la complejidad para gestionarlas. De hecho, el 55% de las compañías encuestadas consideraban este como uno de sus grandes desafíos. Precisamente, en este 2019 se calcula que, entre un 15% y un 18% de los CISO de las principales empresas del **Fortune 500** y **Global 2000**, reducirán el número de soluciones de ciberseguridad para incrementar la facilidad de gestionarlas, según **Cybersecurity Ventures.**

El problema humano

Pero no todo es tecnología: **"**si crees que esta puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología", destacó en la pasada década el conocido criptógrafo, **Bruce Schneier,** algo que todo buen directivo ya se sabía desde hace muchos años antes de la aseveración del mediático 'gurú'. Y es que, a pesar de la automatización y escalabilidad de las soluciones, el valor de lo humano, la pericia y la intuición del analista para mitigar los riesgos más críticos y dirigidos, seguirá marcando el mercado de este tipo de servicios gestionados de ciberseguridad. Precisamente, este es uno de los grandes retos a los que se enfrentan los MSSP: mitigar la falta de personal en la cadena de valor de la ciberseguridad gestionada.

Aportando visión estratégica

La madurez de los MSSP ha propiciado que no se limiten a prestar servicios de ciberseguridad gestionada, sino que, además, también ayuden a crear, adaptar y evolucionar una política y una estrategia de ciberseguridad vinculada al negocio. Por eso, los más avanzados no sólo ofrecen capacidades 'estáticas' sino que incluso son capaces de asesorar, evaluar y probar, especialmente los que proceden del segmento de consultoría. Todo, aplicando tanto tecnologías como procesos, así como análisis que permitan conocer el estado de la seguridad y cómo mejorarla de forma continua para anticiparse a las nuevas amenazas. Por supuesto, las cuestiones que se plantea cualquier cliente ante un proveedor de servicios gestionados sigue siendo la misma de siempre: en caso de sufrir un incidente de seguridad, ¿cuál es la capacidad de reacción de un MSSP? Y, si se produce una 'ciberpandemia', ¿qué lugar ocuparía como cliente en las prioridades de remediación por parte del MSSP? Son dos cuestiones que se tienen en cuenta en los contratos de servicios, aunque nunca mediante un contrato se puedan modificar las condiciones de la cruda realidad.

Ciberseguridad propia vs servicio gestionado

En uno de sus informes sobre los costes de los MSSP, **Kaspersky** destaca que actualmente se pueden encontrar tres tipos de enfoques en ciberseguridad:

1.- Lo de siempre, lo clásico y tradicional de tener los sistemas y expertos contratados por la propia empresa cliente, que supone contar con locales, equipos de apoyo, tecnologías y que es la solución que, a día de hoy, tienen todas las grandes empresas. La clave es el control total sobre todo, a pesar de su coste.

Además, los grandes equipos internos pueden compartir conocimientos, perspectivas y experiencias, discutir las últimas amenazas, tendencias y estrategias. Es lo que se conoce como 'conocimiento de *crowdsourcing*' que, eso sí, no ocurre en departamentos pequeños.

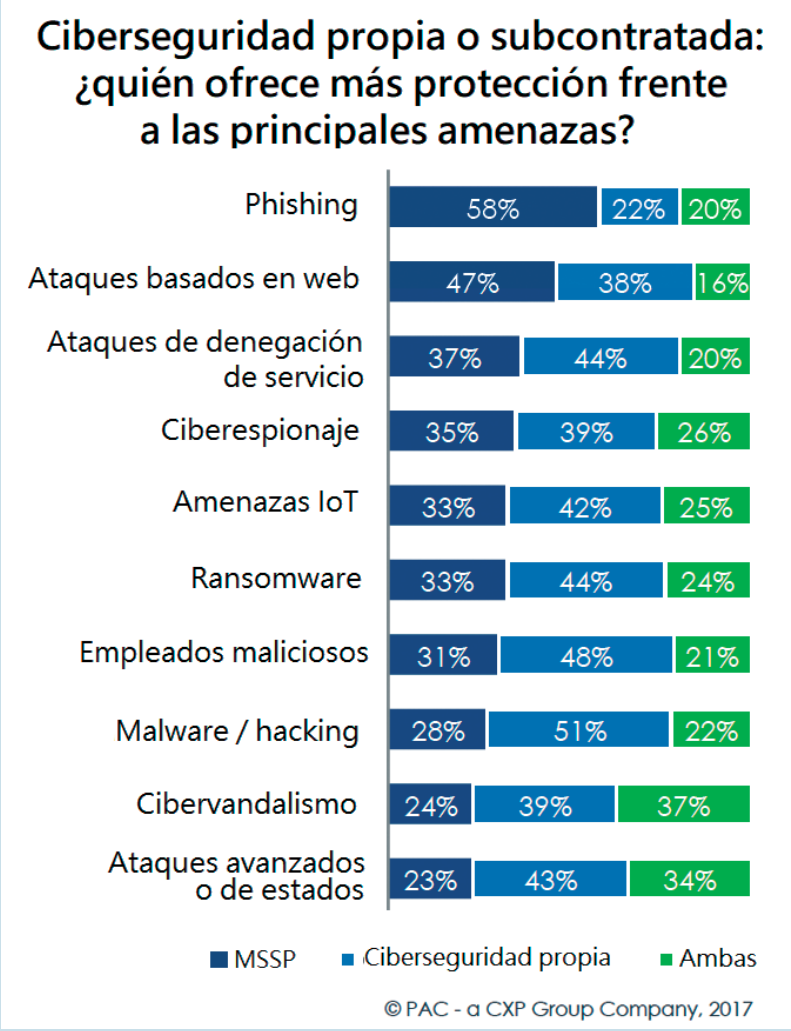
2.-Protección desde la nube. Casi dos tercios de las pequeñas y medianas empresas ya utilizan un promedio de tres soluciones en la nube; por eso, no es de extrañar que la seguridad basada en el *cloud* sea una de las opciones de más rápido crecimiento. Este modelo permite, desde una consola en la empresa, acceder a todo tipo de servicios y tener visibilidad de la red y las posibles amenazas, y gestionarlas a través de herramientas de automatización y de controles manuales. Entre sus grandes ventajas está su reducido coste de contratación e implementación, su facilidad de manejo y las opciones de licencia flexible.

Por ejemplo, "ofrecer la seguridad de ICS como un servicio en la nube tiene el potencial de mejorar la escalabilidad y flexibilidad de las implementaciones al tiempo que se extiende la seguridad a operadores más pequeños que carecen de los recursos para administrar instalaciones complejas", dice **Patrick Daly,** analista de **451 Research**. "Además, la capacidad de compartir instantáneamente la inteligencia sobre amenazas de un sitio de cliente con el resto de clientes debería ayudar a reducir el tiempo necesario para detectar y responder a incidentes de seguridad".

3.-Confiar en la seguridad gestionada. Y, por último, lo que más mercado está ganando: apostar por los MSSP, lo que supone dejar que un tercero o varios se encarguen, bajo nuestra supervisión, de la ciberseguridad de la compañía. Los motivos para apostar por ello son, desde la experiencia, la variedad de perfiles y capacidades, hasta la facilidad para disponer de todo tipo de tecnología y también datos que permitan generar inteligencia y anticiparse a las amenazas.

La razón es que el panorama de ciberamenazas están cambiando tan rápido que sólo el 32% de las empresas son capaces de hacerlas frente de forma efectiva, según un estudio de **NTT** Security. De ahí el auge los MSSP, que actualmente representa un mercado muy segmentado con proveedores centrados en empresas, según su tamaño y complejidad, otros en tipo de sector (finanzas, salud, industrial, *retail*, etc) y, también, muchos que apuestan por la especialización en infraestructuras industriales o el Internet de las Cosas (IoT).

Además, contratar servicios como la monitorización 24x7 permite hacer frente a ataques dirigidos, que suelen producirse fuera del horario normal de actividad de la empresa, según las estadísticas, para pasar lo más desapercibidos posibles. Para ello, los MSSP disponen de Centros de Operaciones de Seguridad (SOC), a través de los que ofrecen información y datos de herramienta SIEM (gestión de información y eventos de seguridad) en tiempo real.

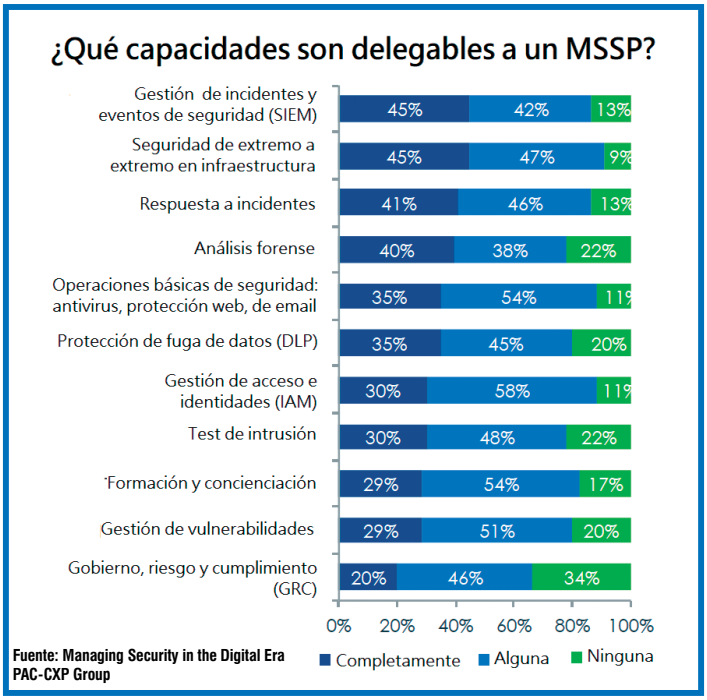


2 ¿Qué papel juegan los servicios de seguridad gestionada?

No todo es brillo en el mercado de los proveedores de servicios de seguridad gestionada. Según el estudio 'Gestión de la seguridad en la era digital', de la consultora **Pierre Audoin Consultants (PAC)** para la firma **Computacenter**, un 31% de las compañías también se están planteando recuperar partes de la gestión de la ciberseguridad subcontratada. De cualquier forma, destaca su auge por la flexibilidad y experiencia que aportan este tipo de empresas de servicios. Más del 70% de sus clientes se muestra satisfecho con su gestión y, de hecho, el 66% de las compañías europeas cuenta con algún MSSP en su ciberprotección, destaca el informe, que también resalta que un 24% tiene previsto invertir en ellos como forma de hacer frente a las principales amenazas y gestionar el cumplimiento de todo tipo de normativas, sobre todo del Reglamento General de Protección de Datos (RGPD).

"Las empresas están bajo más presión que nunca para hacer frente a las ciberamenazas y saben que el uso inteligente de un proveedor de servicios de seguridad gestionada puede ser decisivo", comenta el Director de Servicios de Seguridad de Computacenter, **Jan Müller**, que recuerda que los datos de la encuesta también constatan que aún "muchas compañías son reacias a confiar completamente en un MSSP, apostando por un enfoque mixto que permita combinar su propia experiencia y gestión con el uso de un MSSP con el que acometer una estrategia sensata".

Lo curioso, según este estudio, es que dentro de cada empresa existen diferentes visiones sobre el papel de los MSSP. Mientras que los Consejos de Administración esperan de ellos, sobre todo, un ahorro de costes, los equipos de seguridad buscan cubrir 'huecos'



Fuente: Managing Security in the Digital Era PAC-CXP Group

Los MSSP triunfan también en la F1

F1 y súperdeportivos. Quizá la F1 suene muy alejada de la ciberseguridad pero es un buen ejemplo de la vitalidad de los MSSP. Uno de sus referentes mundiales, **SecureWorks,** ha firmado un contrato con el **Grupo McLaren** para asegurar sus datos sin importar donde estén, así como hacer frente a amenazas en tiempo real. Un aspecto crítico, ya que entre otras situaciones, McLaren dispone del simulador más avanzado del 'Gran Circo' donde un piloto disputa las carreras de forma virtual en su sede de Woking (Reino Unido) durante los Grandes Premios para ayudar a tomar las mejores estrategias en paradas, neumáticos, telemetría, etc. Además, estos datos son usados por la compañía para el desarrollo de sus deportivos de calle, incluyendo sus futuros modelos. "Esta alianza nos ha permitido externalizar la mayoría de los recursos de la seguridad cibernética; nuestro equipo interno es capaz de enfocar su tiempo y recursos en los proyectos que llevan beneficios directos a McLaren", ha explicado el CISO de la marca, **Jonathan Neale**.

que con la tecnología y personal propios no pueden gestionar de forma eficaz.

Por eso, cada vez más compañías apuestan por un MSSP para aspectos concretos de su ciberseguridad optando por un enfoque mixto (*pick and mix*, se denomina en inglés) entre lo interno y lo externalizado. Ello lleva a buscar proveedores flexibles y rápidos en el despliegue de sus soluciones y su gestión aprovechando la nube y el software como servicio (SaaS) para hacer frente a las amenazas más convencionales como el *ransomware*, la suplantación (*phishing*) y el software malicioso, apostando por los MSSP con mayor madurez para ayudar a hacer frente a los ataques dirigidos de estados y grupos de espionaje industrial.

Automatización para lo habitual

La automatización de tareas es uno de los grandes alicientes de este tipo de servicios. Por ejemplo, a través de plataformas como IBM QRadar y similares, se puede hacer frente a los incidentes más comunes sin personas, contar con los datos más importantes para investigarlos y reducir los tiempos de recuperación y respuesta. De hecho, en ellas ya se usa de forma masiva la inteligencia artificial.

Eligiendo al mejor proveedor de seguridad

Para garantizarse siempre unos 'básicos' en cualquier proveedor, los expertos recomiendan tener en cuenta, antes de contar con un MSSP, asegurarse de que sus equipos tienen las certificaciones de seguridad más conocidas (CISSP, GSEC, CEH, CCSP, CCNA, CISM, etc.), ya que aun no siendo garantía total de su calidad sí permiten asegurarse unos mínimos conocimientos y experiencia, sobre todo, en el equipo de analistas, evitando que se ponga excesivo énfasis en la tecnología y automatización, que no permiten hacer frente a las amenazas de mayor riesgo.

Ciberataques contra MSSPs:
el cibercrimen ya sabe que son la llave a cientos de empresas

Convertirse en el corazón de un ataque a la cadena de suministro es una mala experiencia para cualquier organización, pero lo es más para aquellos que, precisamente, ofrecen servicios de ciberseguridad gestionada. El acceso directo y sin restricciones a las redes de sus clientes son las principales razones por las cuales los MSSP se están convirtiendo en uno de los grandes objetivos del cibercrimen.

Frente a su seguridad los atacantes saben que, de tener éxito, tendrán acceso en cascada a los datos e información de otras muchas empresas o a generar problemas en las operativas de negocio. Y, por supuesto, para la víctima supone una pérdida de credibilidad y reputacional, cuyas consecuencias están en consonancia con la gravedad del ataque (baste recordar el recientísimo caso de una de nuestras primeras energéticas).

Tal es la amenaza que la **Agencia de Ciberseguridad y Seguridad de las Infraestructuras** (**CISA**) estadounidense emitió en octubre pasado una 'Alerta Técnica' sobre el aumento en la actividad cibernética maliciosa (especialmente, de actores chinos) a través de APTs contra proveedores de servicios, incluidos MSSP. En ella, advertía que muchos de los ciberataques se valen de credenciales comprometidas (nombres de usuario y contraseñas).

Ransomware contra MSSP

Lamentablemente, las filtraciones de ciberseguridad que afectan a la cadena de suministro son muy numerosas. Un reciente estudio de **Ponemon Institute** indica que, en 2018, el 59% de las empresas experimentaron una violación de datos causada por uno de sus proveedores o socios. El *ransomware* es considerado, junto al riesgo de accesos no autorizados, uno de los principales riesgos de ataque contra los MSSP.

Uno de los ejemplos más recientes lo encontramos a principios de este mismo año, cuando un error en un *plugin* de ConnectWise provocó que un MSSP se infectara con el *ransomware* GandCrab, afectando a 80 clientes. Como detalla **Reddit**, los atacantes habían utilizado el propio software de gestión y monitorización remotas (RMM) del MSSP para implementar el *ransomware*. Se cifraron de 1.500 a 2.000 puntos finales, incluidos servidores, y esta compañía se enfrentó a un rescate de 2,3 millones de euros.

Otro ataque que deja clara la dimensión de las ciberamenazas en los MSSP ocurrió en junio. **Reuters** informó que un grupo de piratas informáticos que trabajaban para el Ministerio de Seguridad del Estado chino accedieron ilegalmente hasta en ocho grandes proveedores de servicios de tecnología para robar secretos comerciales, obtener información confidencial y posteriormente atacar a sus respectivos clientes. El ataque, denominado 'Operation Softcell', afectó a compañías que proporcionan servicios de seguridad gestionada, como IBM, Fujitsu, HP, DXC Technology y NTT.

Ya pasó en 2017 con WannaCry

Dada la circunstancia, la decisión de desconexión que tomó Telefónica tras padecer el alboroto causado por el mediático WannaCry evitó que muchos de sus clientes se infectaran con el *ransomware* que se transmitía como un virus 'tipo gusano'. Con todo, aunque el ataque no iba dirigido expresamente contra MSSP, sí demostró los riesgos de atacar con éxito a grandes proveedores de servicios TIC con no todos los deberes hechos. De hecho, en función de su tamaño y clientes, hay expertos que consideran que los MSSP podrían ser considerados infraestructura crítica, según los servicios de cibereguridad que presten a organizaciones operadoras de IC.

3 Qué vacíos de la gestión de la ciberseguridad cubren hoy los MSSPs

Según un estudio de **VMware** y **Forbes Insights** en la actualidad sólo uno de cada cuatro directivos confía en la estrategia actual de ciberseguridad de su organización. De hecho, este informe destaca sonrojantemente que, en España, el 69% de los directivos y responsables de TI cree que las soluciones de seguridad con las que trabajan sus empresas están desactualizadas, aunque más de la mitad (51%) afirma que ha adquirido soluciones de ciberseguridad durante el último año para abordar los potenciales problemas en este ámbito.

¿Su apuesta a corto plazo? El 20% de los encuestados planea invertir más en la detección e identificación de ataques, y cerca de un tercio (31%) afirma contar con más de 26 soluciones de seguridad instaladas en sus organizaciones, una situación en la que también están interviniendo los MSSP para hacerlo todo más fácil y rápido de gestionar, sumado a la reducción de costes que supone, ya que sólo cuatro de cada diez responsables de seguridad de la información cuentan con un presupuesto lo suficientemente grande como para asegurar las infraestructuras de manera eficiente e interna, por lo que subcontratar servicios es una de las opciones más demandadas.

I. Necesidad de lo manual

Sí, en un mundo donde la automatización y la robotización están permitiendo implementar servicios de forma escalable, los analistas y la gestión personal de incidentes y su análisis continúa siendo crítica. Y las empresas se ven limitadas por no disponer ni del número ni de la experiencia necesaria para ello, algo de lo que los MSSP sí disponen. Y ofrecen.

II. Cubrir más superficie de ataque

Redes sociales, servicios en la nube, decenas de aplicaciones en todo tipo de dispositivos (incluso usados en casa, como es el caso de la tendencia BYOD), las nuevas redes 5G y el Internet de las Cosas (IoT), etc. El perímetro tecnológico de las empresas está completamente difuminado. A ello se suman la mayor complejidad de la red. Y para protegerla ya no basta con soluciones internas: exige contar con especialistas en cada disciplina.

III. Costes ajustados

Licencias, actualizaciones, personal… El presupuesto para ciberseguridad siempre se queda corto en gran parte de las entidades. Para paliar esta carencia, los MSSP ofrecen soluciones de seguridad asequibles, confiables y eficaces.

IV.
Evitar el estrés

Los expertos en protección digital no dan abasto, según un reciente informe de **Symantec**, que ha contado con la opinión de más de 3.000 CISO de Francia, Alemania y Reino Unido. En él han confesado que "están hartos del estrés y los días de trabajo interminables", por lo que un 64% se ha planteado dejar su trabajo actual y un 63% el sector, una circunstancia que los servicios de un MSSP pueden ayudar a atenuar en lo relativo a las tareas más trabajosas y de menos valor para la gestión pura del negocio de la empresa que recaían en la órbita competencial del CISO.

V.
Seguridad en la nube

Actualmente, se calcula que el 90% de las empresas ya trabajan en el entorno de la nube. Y quién no lo ha hecho lo hará en breve. Ello está dando pie a un nuevo nicho de seguridad con nuevos perfiles, como el de ingenieros de confiabilidad de sitios (SRE). Y también nuevas estructuras de organización que obligan a los equipos del SOC y los SRE a trabajar juntos. Ofrecer seguridad en todas las aplicaciones que hay en ella se ha convertido en uno de los grandes retos de los departamentos de ciberprotección que, además, se enfrentan, en ocasiones, a datos e información no catalogados que se "suben" a la nube fuera de su control.

VI.
Sistemas sin actualizar

Más de la mitad de los dispositivos que usan las pymes tienen sistemas operativos obsoletos, según destaca **Alert Logic**, que encontró que el 66% de ellos tienen sistemas operativos de Microsoft vencidos o próximos a expirar, un aspecto en el que para un proveedor de servicios de seguridad gestionada puede ser vital al llevar, por ejemplo, la implementación de actualizaciones de seguridad de forma automatizada para estar al día. "Los perímetros están desapareciendo y la visibilidad y el control basados en el punto final son críticos".

VII.
Complejidad excesiva

Decía **Albert Einstein** que "si buscas resultados distintos, no hagas siempre lo mismo". La ciberseguridad actual conlleva muchas rutinas y muchas empresas no disponen del presupuesto necesario para automatizarlas, sobre todo si se cuenta con decenas de soluciones que, en muchos casos, no se 'entienden' entre sí.

Hablando de dinero: ¿Suponen los MSSP un verdadero ahorro en costes?

Apostar por los MSSP supone ahorros de espacio, personal, tecnología y, también, disponer de servicios 'a demanda' y a 'a la carta' muy complicados de mantener, internamente para grandes, medianas y pequeñas empresas.

De todos modos, no existen informes independientes de peso sobre este campo y cada MSSP de referencia ofrece sus comparativas. Por ejemplo, **BAE Systems EMSS** considera, en su estudio 'Impacto económico total de los servicios gestionados de seguridad', realizado por **Forrester**, que externalizar la protección cibernética evita, por ejemplo en la gestión de vulnerabilidades, la contratación de 16 profesionales, con un ahorro anual de casi 640.000 euros. Además, su capacidad para identificar amenazas que pasan desapercibidas para muchas empresas es de 500 veces más al año, incluyendo la detección de cuatro brechas de seguridad que ponen en riesgo los datos.

Según se desprende de uno de los clientes de BAE, del sector financiero, en un solo año, consiguió un ahorro de costes por sanciones por incumplimiento que rondan los 830.000 euros al año, 270.000 en tiempo de remediación de incidentes, así como 184.000 euros en gestión de operaciones de ciberseguridad, evitando dedicar analistas a los incidentes más comunes, con una resolución en torno a las 48 horas, para centrarse en los que más riesgo supone. Esto representa para los CISO no estar involucrados en los incidentes de menor prioridad, delegando su gestión y repuesta al MSSP.

Además, el estudio de BAE también destaca una mayor calidad de la información de 'inteligencia de amenazas' para anticiparse a los nuevos tipos de ataques o los más complejos de detectar, así como disponer de conocimientos, paso a paso, para implementar las mejores medidas proactivas, "lo que dio pie a un entorno más seguro para la empresa", destacan los expertos de BAE.

En total, la empresa analizada por Forrester cuantificó sus beneficios anuales por su ciberseguridad con un MSSP en 4,3 millones de euros a tres años, frente a una inversión en él de 1,9 millones, con un ROI de un 125%. Además, el CISO de la compañía también destacó que había ganado visibilidad y comprensión sobre las posibles amenazas, pudiendo responder a ellas de manera más eficaz y precisa "reduciendo el apetito al riesgo, consciente de que las amenazas más frecuentes están siendo correctamente gestionadas por nuestro MSSP". Ello supone para el CISO un 'tiempo extra' que ronda el 15% para centrarse en otras áreas.

Inversión sin retorno cierto

Eso sí, en un estudio de Kaspersky también se destaca que este mercado aún no está tan maduro como para tener métricas fiables que evidencien el retorno exacto de inversión (ROI) de lo gastado en un MSSP. De cualquier forma, "el 62% de las grandes empresas y el 59% de las pequeñas y medianas consideran que seguirán invirtiendo en este tipo de servicios independientemente de su rendimiento", destaca la compañía en uno de sus informes.

Por ello, el uso de una sola plataforma integrada, a través de un MSSP, puede mejorar su eficiencia y reducir el trabajo que supone. Se requieren nuevos enfoques para reducir el esfuerzo que comporta gestionar tanta tecnología y tan diferente.

VIII. Necesidad de más inteligencia

Para anticiparse a las amenazas es imprescindible contar con el mayor número de datos. Pero estos no se pueden analizar y gestionar sin técnicas y tecnologías de IA y aprendizaje automático, herramientas y capacidades que están ofreciendo, al máximo nivel, los MSSP que están presentes de forma global, con datos de todo tipo de clientes y tecnologías escalables, "que permiten que los expertos de las empresas se centren en las tareas más importantes y gratificantes y reducen la presión sobre la necesidad de contratar más profesionales", destaca en un artículo el CTO y Vicepresidente de Tecnología de Symantec para EMEA, **Darren Thomson**.

IX. Cumplimiento normativo

A la seguridad tradicional se suma, desde 2018, la de protección del dato personal, con la entrada en vigor plena del reglamento europeo (RGPD). Empresas como **British Airways** ya han sido multadas con 205 millones de euros por una fuga de datos que afectó a 500.000 clientes o la cadena de hoteles **Marriott** con 111 millones de sanción por no haber protegido la información personal de más de 390 millones de clientes. De hecho, **IBM** calcula que cada fuga de datos personales tiene un coste medio para las medianas y grandes empresas de 3,3 millones de euros.

Por eso, el 29% del presupuesto de ciberseguridad de las empresas se dedica a tareas relacionadas con el cumplimiento normativo –donde suele encuadrarse el ámbito de la privacidad y los datos personales–, según el informe 'The Cyberthreat in Europe", de **Black Hat.**

Una solución para hacerle frente es recurrir a los MSSP, que utilizan de forma intensiva y realista la IA, la detección automatizada y la caza proactiva de amenazas cibernéticas, "soluciones poderosas que las empresas deben aprovechar para tener mejor oportunidad de cumplir con los nuevos requisitos establecidos por el RGPD y la Directiva NIS".

Inteligencia Artificial, SOAR y MDR, las tecnologías que lo cambiarán todo

Más de la mitad (56%) de los directivos, a nivel mundial, piensan que sus analistas de ciberseguridad se ven desbordados por el inmenso volumen de unidades de información que deben vigilar para detectar y prevenir intrusiones; una cifra que en España asciende hasta el 63%, según un estudio de **Capgemini** sobre el papel crítico que va a jugar la inteligencia artificial para hacer frente a la nueva generación de amenazas de ciberseguridad de las empresas.

De hecho, una clara mayoría de empresas (69%) cree que no va a tener capacidad para responder a los ciberataques sin el uso de la IA (muy similar en España, con un 71%), y el 61% afirma que necesita la IA para identificar las amenazas críticas (un 66% en España).

Además, un 27% de los preguntados en un estudio de **ESG** también destacó estas técnicas y tecnologías para acelerar la respuesta a incidentes. Esto significa mejorar las operaciones, priorizar los incidentes correctos e incluso automatizar las tareas de remediación. Y un 24% para ayudar a su organización a identificar y comunicar el riesgo a la empresa (para clasificar montañas de vulnerabilidades de software, errores de configuración e inteligencia de amenazas para aislar situaciones de alto riesgo que requieren atención inmediata).

De hecho, según un estudio, de julio pasado, de **Palo Alto,** el 26% de los encuestados en EMEA prefieren que su ciberprotección sea gestionada por un sistema IA en vez de por humanos, llegando al caso de Italia donde el 38% destacó su confianza en ella.

Herramientas SOAR: automatizando la respuesta a incidentes

Entre las claves para contar con un buen proveedor de servicios de seguridad gestionados destaca su capacidad para contar con métricas fiables de los datos que recibe y analiza. Ello le permite, de manera exponencial, reducir el tiempo medio de detección (MTTD) y de respuesta (MTTR), el número de incidentes resueltos en cada turno, etc. Por eso, contar con herramientas adecuadas y personal que sepa sacarles partido es vital según los expertos.

Y en este aspecto destaca un 'nuevo' concepto, el de las tecnologías de orquestación de seguridad y respuesta automatizada (SOAR), que permiten automatizar respuestas a incidentes, uno de los grandes avances en la última década en los MSSP y en las compañías con un alto grado de madurez en ciberseguridad, que cuentan con SOC propios.

Así, las soluciones SOAR ofrecen alertas de sistemas TI, OT, SIEM, correo-e, CRM, escritorio, sistemas UEBA (comportamiento de usuarios), control y acceso, puntos finales… y actúan en ellas de forma automática, reduciendo el riesgo sin necesidad de analistas, aunque este tiene conocimiento de ello a través de un panel de control centralizado, al igual que los clientes. De hecho, este tipo de soluciones han ganado mercado rápidamente por lo que suponen de mejora de escalabilidad, productivas y experiencia del cliente.

Gestión de detección y respuesta

Además, los MSSP están apostando por construir un ecosistema de tecnologías y expertos que les permita ofrecer servicios de búsqueda de amenazas persistentes avanzadas (*APT Threat Hunting capability)*. Es lo que la consultora Gartner ha denominado como 'Servicios de gestión de detección y respuesta (MDR, por sus siglas en inglés), creando una categoría de empresas enfocadas a detectar amenazas que suelen pasar desapercibidas y suelen entrar en la red de las compañías. Es la última línea de defensa. De hecho, la consultora Gartner prevé que el 15% de las empresas cuenten con servicios MDR para 2020, frente al poco más de un 1% actual.

Obligados a automatizarlo todo ante la falta de personal

'CERRADO' POR FALTA DE EXPERTOS

Tan crítico es carecer de las medidas de seguridad mínimas, como no disponer del personal que las aplique. "Imagine que va a una ciudad y encuentra las casas y las tiendas vacías: pues esa es la imagen más fidedigna de lo que está sucediendo con el talento en el mundo de la ciberseguridad en toda Europa", explica en un artículo el ya citado CTO y Vicepresidente de Tecnología de Symantec para EMEA, Darren Thomson. "La falta de talento en materia de seguridad es un gran riesgo para las empresas a medida que dan el salto a entornos como la nube o manejan grandes cantidades de datos para comprender mejor a sus clientes".

De acuerdo con el Informe del Estado de Ciberseguridad de 2019 de **Isaca,** el 69% de las organizaciones desvela que sus equipos de seguridad no cuentan con suficiente personal, mientras que el 58% tiene puestos sin cubrir. De hecho, el 32% confesó que tardó en cubrir ciertas vacantes, de media, más de seis meses, perdiendo seguridad en las competencias que necesitaban cubrir.

Por eso, se considera que los MSSP ganarán mercado por esta situación de desequilibrio: para 2021 se calcula que habrá 3,5 millones de empleos en ciberseguridad sin poderse cubrir por falta de candidatos, según la consultora **Cybersecurity Ventures**. De hecho, la demanda de este tipo de profesionales crecerá a un ritmo del 36,5% hasta 2022, según **US News** y **WorldReport**, una situación que pueden paliar, al menos de momento, los MSSP.

Por ejemplo, cuando la empresa **Codere** apostó por el vSOC de la empresa Aiuken "entre los indicadores que priorizamos fue la experiencia de las personas que gestionan los servicios, ya que, cuando existe la posibilidad de ataques masivos, es fundamental que se cuente con expertos que ya los han vivido y tienen experiencia en gestión de crisis", destacó **Luis Miguel Brejano,** de Codere, en la última edición de **Securmática**. Prestamos "un servicio que permite tener la máxima seguridad sin comprar nada, ya que para tenerlo sólo hace falta pagar una cuota: Aiuken estudia cuáles son los activos más críticos de una organización y se despliega lo que realmente se necesita. Ello nos permite ofrecer un servicio gestionado, pagando por lo que realmente se consume, con facilidad para aprovisionar nuevas necesidades, de forma escalable y flexible en el despliegue", añadió el Director Comercial de **Aiuken**, **Luis Miguel Muñoz**,con la ventaja de "que se puede reducir o ampliar según las necesidades puntuales del cliente".

Niveles de servicios (SLA): cómo deben ser y cómo evitar errores que se pagan

Como en tantos otros contratos de externalización y concernidos, en el mercado de MSSP también son claves los llamados 'Acuerdos de Nivel de Servicio' (SLA). Se trata de los contratos, legalmente vinculantes, que describen exactamente lo que hará y no hará por sus clientes, donde quedan materializados los servicios que se prestan, en qué condiciones, a qué precios y qué hacer ante incumplimientos.

Por eso, en ellos se plasma el alcance, coberturas y forma en la que se prestan los servicios de ciberseguridad. También se incluyen qué capacidades propias se integran con las subcontratadas y se marcan los protocolos para ofrecer resultados concretos según las necesidades del momento, entre ellas el tiempo de resolución de problemas.

En este contexto, ¿qué recomiendan los expertos para que los SLA sean eficaces y permitan mejorar la seguridad en el día a día?:

1. **Establecer objetivos razonables y alcanzables.** A través de una redacción clara, sencilla y detallada, evitando la interpretación. Sobre todo en lo más crítico: cómo encarará el MSSP, de forma coordinada, la respuesta a un incidente, en qué plazo de tiempo y cómo evitará que vuelva a producirse. Por eso, en función de las amenazas y riesgos, es bueno que este tipo de documentos sean actualizables.
2. **Ser transparentes y realistas.** Los SLA son acuerdos contractuales y, por ello, también deben ser claros en los servicios que se prestan y qué relación se establece con el cliente.
3. **Exigir personal formado.** Es importante que el MSSP tenga el personal capaz de cumplir lo que se promete en el SLA, en tiempo y procesos. Así, cada perfil debe tener claro qué servicios debe proporcionar, cómo relacionarse con el cliente, qué hacer antes de una crisis, etc.
4. **Tener métricas medibles y de riesgo.** Los expertos aconsejan incluir en ellos cláusulas que garanticen unos resultados para los que se ha contratado al MSSP, así como penalizaciones en caso de no cumplirlas.

No obstante, en algunos tramos de mercado, son los propios grandes clientes los que definen qué servicios demandan, en qué condiciones, a qué precio, por cuánto tiempo y a qué precio máximo, detalle este último que en algunos llamamientos al mercado algunos MSSPs concurrentes deciden mejorar, a veces rozando la falta de rentabilidad o asumiéndola por considerar más ventajoso ganar un cliente.

4

La gestión de identidades y la necesidad de ofrecer seguridad en 5G e IoT marcarán su crecimiento

'MSSPs Business': quiénes son la referencia y cuáles son las compañías españolas que pugnan por serlo

El 25% del mercado de ciberseguridad español ya se encuadra dentro de la categoría de 'gestionada'. Se trata de uno de los negocios que, según Gartner y Forrester, más crecimiento tendrá en los próximos años con la llegada del 5G y el IoT. En él los grandes referentes de la ciberprotección clásica se enfrentarán a las compañías de telecomunicaciones, frente a las que apostarán por la especialización. Nadie quiere perder el tren de un sector que, para 2028, puede mover hasta 90.000 millones de euros.

El ramo de los MSSP muestra gran vitalidad y gozará de mejor salud según pasen los años. En 2018, su crecimiento en el entorno global fue del 6,7%, según **Gartner**, alcanzando los 9.500 millones de euros; pero analistas como **Allied Market Research** prevén que llegue a un 16,6% para 2022, generando más de 36.000 millones de euros, unas cifras muy por encima de las del mercado completo de ciberseguridad, cuyo crecimiento medio rondará el 10,2% anual, durante los próximos cinco años, según **Markets and Markets**. Hay incluso analistas, como **Persistence Market Research,** que consideran que este mercado crecerá un 18% suponiendo un negocio de hasta 90.000 millones en 2028.

Lo de siempre sigue dando más negocio

Actualmente, los servicios más demandados son los de gestión de la seguridad (3.300 millones de euros) y de las amenazas (1.800 millones), los de administración de puntos finales y los de protección de los datos (1.700 millones). También destacan los servicios de seguridad de aplicaciones (1.600 millones) y los de gestión de identidades y accesos (1.100 millones), uno de los que más crecerá, según el estudio de **Nelson Hall** para **DXC Technology.**

Esta demanda dibuja un panorama en el que existe una gran diversidad de ofertas. Un ejemplo lo encontramos en el 'Cuadrante Mágico' de Gartner para proveedores de servicios seguridad gestionada, con las 14 compañías que considera más significativas. Entre ellas están desde organizaciones de alcance mundial, como **IBM, Fujitsu** y **Atos**, hasta *pure players* de ciberseguridad como **Symantec, Secureworks** y **Trustwave**, además de empresas de telecomunicaciones como **AT&T, NTT** y **Verizon**, y consultoras como **Capgemini**. Curiosamente, este año no están en él algunos de los referentes de ediciones anteriores, como **BT, DXC Technology, HCL Technology** y **Orange,** aunque Gartner no da motivo concreto de su exclusión.

A la demanda tradicional de este tipo de servicios, se está sumando la necesidad de proteger nuevos entornos como la nube, el 5G, el IoT y la industria 4.0. Todo ello bajo la presión de cumplir con todo tipo de normativas (de privacidad, de pago seguro, de

infraestructuras críticas, etc) para no pagar multas millonarias. Algo a lo que se suma una dificultad añadida: el déficit preocupante que ya existe de expertos en ciberseguridad y que los analistas consideran que se incrementará en los próximos años.

Por ello, el sector está incrementando la sofisticación de sus servicios y esto hace que, en algunos casos, también integren en su portafolio a otros especialistas de seguridad, ya sea comprando MSSPs o mediante acuerdos de colaboración con *partners* con capacidades de integración, consultoría, reventa y alcance geográfico allí donde no se está presente.

Un buen ejemplo lo encontramos en Telefónica que, para ofrecer su amplio abanico de servicios de ciberseguridad, ha realizado una gran inversión en habilidades y tecnologías. Entre otros socios de la operadora, Gartner destaca a **Devo, Blueliv, 4iQ** y **CounterCraft**. Además, también integra las tecnologías de fabricantes tradicionales del sector como **F5, Radware** y **Arbor Networks** y de **Palo Alto Networks** y **Panda Security** para el análisis, detección y respuesta a amenazas. También es significativa la reciente fusión entre **S21sec** y **Nextel**, a instancias del emporio portugués Sonae, que dió pie en 2018 a la mayor empresa dedicada exclusivamente a servicios

Los operadores de telecomunicaciones quieren convertirse en la referencia

La competencia de las operadoras es uno de los puntos de inflexión que está experimentando el sector de los MSSP, un mercado que conocen bien, ya que fueron casi pioneras en él a través de una oferta de servicios administrados alrededor de las 'cajas' que vendían a aquellos clientes que no querían gestionarlas ellos mismos. De hecho, Telefónica cuenta con SOC en España desde hace más de 15 años.

Los cambios disruptivos que están teniendo lugar en sus negocios en los últimos años derivados, especialmente, de la 'explosión' de la demanda de datos, les ha llevado a diversificar su portafolio hacia el desarrollo de soluciones y servicios especializados alrededor de la nube, el IoT, la IA, el *big data* y la ciberseguridad, entre otros.

EJEMPLOS DE INGRESOS EN SEGURIDAD DE TRES DE LAS GRANDES TELCOS

País	Operador	Ingresos anuales Seguridad
Reino Unido	BT	€ 553m
España	Telefónica	€ 430m
Singapur	Singtel	€ 347m

Fuente: HardenStance 'New Managed Security Opportunities for Telcos' Julio 2018 (extraido de los últimos informes de ingresos)

Precisamente, en ciberprotección las 'telcos' compiten con ofertas atractivas, y presentan una gran competencia para muchos MSSP que, por capilaridad y recursos, no pueden luchar contra grandes compañías como **Telefónica, Orange, BT, NTT Security, AT&T** y **Verizon**, entre otras. Además, para muchos expertos, podría ser el principal factor de 'comoditización' del sector, dada su agresiva política de precios y escalabilidad.

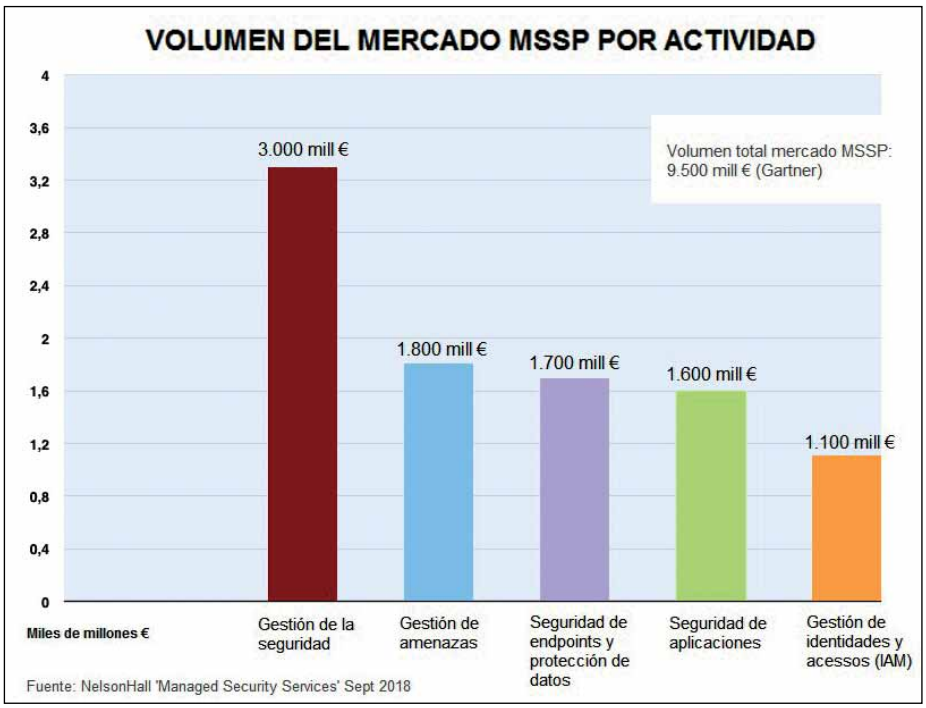
En la actualidad, los servicios de ciberseguridad gestionados ya representan entre un 25% y un 50% de los ingresos totales de ciberseguridad de la mayoría de las grandes empresas de telecomunicaciones, según el informe 'New Managed Security Opportunities for Telcos' de **Nokia** y **Symantec**. El documento posiciona, por ejemplo, a BT con unos ingresos de 553 millones de euros al año en ciberseguridad y a Telefónica con 430. Además, el volumen de Orange en este campo ascendió a 600 millones de euros anuales tras la compra de SecureLink.

Uno de los movimientos más importantes en este mercado se produjo en abril de 2018, cuando **Etisalat, Singtel, SoftBank** y **Telefónica** firmaron un acuerdo para crear la primera Alianza Global de Seguridad entre operadoras de telecomunicaciones, con el fin de ofrecer a las empresas una amplia cartera de servicios de ciberseguridad. A este grupo se sumó en marzo **AT&T** y juntas congregan una red de 28 SOCs y más de 6.000 expertos en ciberseguridad, en más de 60 países de todo el mundo. Además, las compañías de telecomunicaciones tienen la oportunidad de explotar una ventaja "natural" que emerge en la seguridad empresarial: la virtualización de funciones de red (NFV) y el 5G en particular.

Eso sí, hasta la fecha, solo un reducido grupo de operadoras se ha comprometido a prestar servicios de ciberseguridad gestionada a nivel mundial, quizá porque las más pequeñas no quieren hacer frente a un mayor riesgo financiero y también pecan de falta de experiencia y familiaridad con los modelos operativos de seguridad gestionada. Porque ya no se trata solo de administrar el cortafuegos o SIEM de un cliente en sus instalaciones, sino de ofrecer también servicios de análisis, protección, detección y remediación (en su mayoría desde un SOC o red de SOCs) en entornos de TI, 24 horas al día, los 365 días del año.

de ciberseguridad en España y uno de los referentes europeos en este campo.

No son casos aislados. Grandes gigantes como IBM están creciendo a través de programas de canal MSSP en los que ya cuentan con más de 100 empresas, entre ellas la española **Sothis**, que fue considerada por el gigante azul como el mejor *partner* de ciberseguridad de 2019 en nuestro país, y que ha construido su centro de operaciones de ciberseguridad, ERIS-CERT, con la tecnología QRadar. Nadie quiere quedarse atrás en la carrera por ofrecer todo tipo de servicios gestionados a las empresas que, por costes y flexibilidad, renuncian a tenerlos propios.



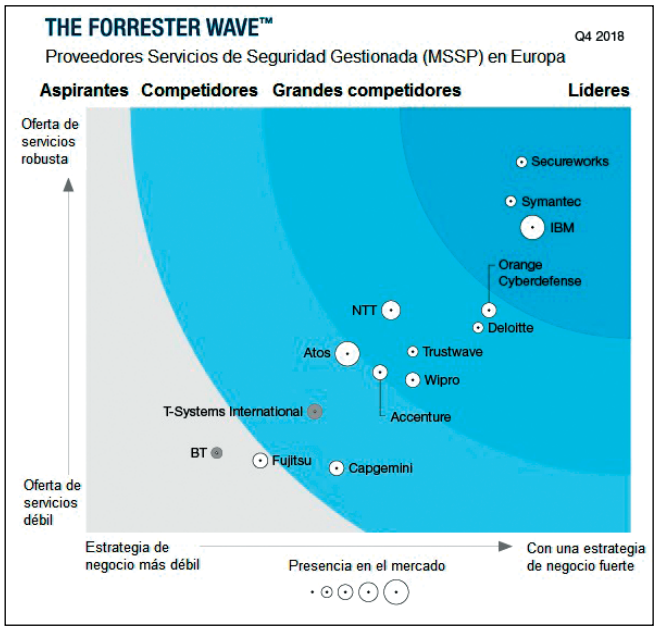
América, la referencia; Asia, el futuro

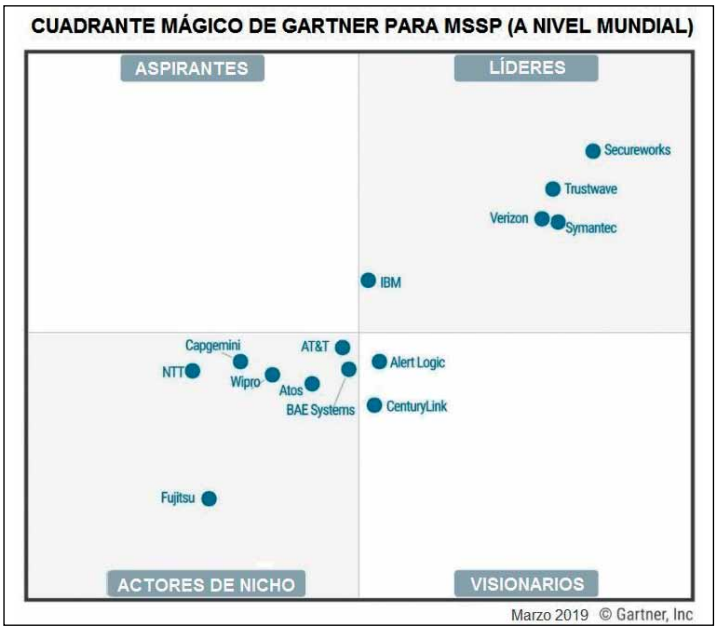
Por zonas geográficas, el gran mercado de MSSP está en América del Norte, sobre todo en servicios de SOC, una vasta zona donde compañías como IBM Security, Symantec, Secureworks, Verizon, BT y Trustwave gozan de una buena posición, ya que el 60% de sus ingresos en este negocio proceden de EE.UU. Sin embargo, Asia, Pacífico y Medio Oriente se está convirtiendo en el área de mayor crecimiento por el incremento de las ciberamenazas y la inversión que se está acometiendo para hacerlas frente.

El Viejo Continente, por su parte, muestra signos de un mercado desarrollado y en crecimiento por la mayor conciencia empresarial en ciberseguridad. Sin embargo, los buenos datos del sector de MSSP no se deben sólo a factores externos. Las compañías europeas exigen socios que, como bien resume Gartner "aporten tres claves: confianza, idiomas y cercanía". Ello lleva a los proveedores europeos a ofrecer servicios personalizados, según los requisitos de cada país, con soporte en lenguas locales y una decidida apuesta por mantener la soberanía de los datos en la UE, aspectos determinantes que, según Gartner y Forrester, marcan la diferencia con la oferta de mercado en América del Norte o Asía/Pacífico.

Europa, un mercado complejo

Y es que la variedad cultural, idiomática y normativa de Europa obliga a "los MSSP a personalizar al máximo sus servicios para ayudar a los clientes a obtener valor,





MSSPs

CENTROS DE OPERACIONES (SOC) DE

CAPGEMINI

GMV

ENTELGY INNOTEC

GRUPO ICA

ONESEQ

INGENIA

LOGICALIS

TELEFÓNICA

S21SEC

MSSPs

ALGUNOS PROVEEDORES ESPECIALIZADOS

AIUKEN

S2 GRUPO

T-SYSTEMS

NUNSYS

MNEMO

ACKCENT

DAVINCI

SECURA

SOTHIS

CIPHER

independientemente de cuál sea su grado de madurez", afirman los expertos de Forrester. Además, "para poder cumplir con los numerosos requisitos normativos locales, el mercado europeo apuesta por proveedores con equipos y capacidades basados en la UE. Con ello, intentan "minimizar las transferencias extracomunitarias de datos y reducir las posibles interrupciones de los servicios", añade la consultora.

Diferencias entre Gartner y Forrester

Ambas consultoras identifican a **Secureworks, Symantec** e **IBM** como los MSSP de referencia mundial y, también, en Europa. La gran diferencia entre sus cuadrantes es que Forrester sí incluye a las grandes consultoras como **Deloitte**, **Accenture** y **Capgemini** entre los grandes protagonistas del mercado europeo.

El desarrollo de servicios de asesoría en ciberseguridad y la gestión a a través de los equipos del Centro de Operaciones de Ciberseguridad, de la forma más 'a medida' posible son algunas de las razones que están ayudando a que las grandes consultoras ganen mercado en Europa, unidas las estrategias de acuerdos con fabricantes e, incluso, la compra de otras compañías para ampliar portafolio.

El negocio de los MSSP ya supone el 25% del mercado español

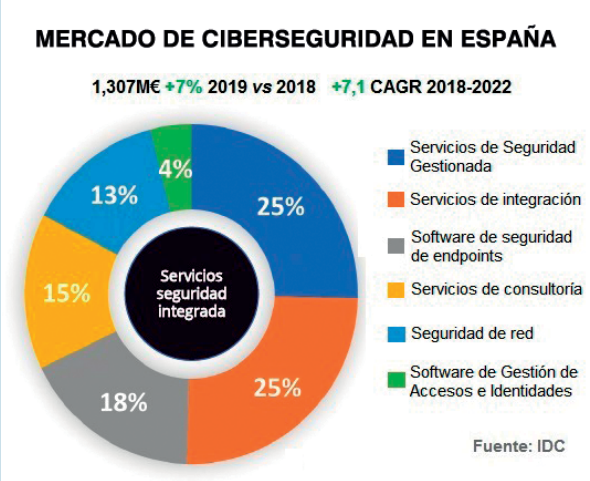
En nuestro país,el mercado de los servicios gestionados es uno de los más prolíficos, representando en la actualidad el 25% del sector de la ciberseguridad nacional, según cálculos de la filial española de **IDC**, que recientemente se ha sumado a establecer previsiones anuales sobre el mercado corporativo, previsiones que ya viene haciendo SIC desde 2000.

La oferta de estos servicios en España comenzó hace más de veinte años de la mano de una serie de compañías pioneras, como **GMV Soluciones Globales Internet**, **SIA**, **S21Sec** y, posteriormente, **Ecija** y **Telefónica**.

Así, actualmente hay una amplia oferta con proveedores de distinto origen, tamaño, grado de internacionalización y especialización, como operadores de telecomunicaciones (**Telefónica**, **BT** y **T-Systems** –filial de Deutche Telecom–, **Everis** –filial de NTT–), *big four* (**Deloitte**), consultoras/integradores de TIC (**Accenture, Indra-Minsait**, **Capgemini**, **Logicalis**, **Atos**, **DXC Technologies**, **Iecisa**, **Ingenia**, **Nunsys**, **OneseQ**, **MDtel**, **Oesía**, **Thales**, **GFI**), fabricantes e integradores (como **IBM, Fujitsu**, **Symantec**, y donde entran españolas como **Grupo ICA, ITS, Mnemo, Entelgy Innotec System, Necsia**, **Unitronics, Secura**, **Secure&IT**, **DaVinci** y **Sothis,** entre otras), así como algunos específicos como **S21sec**, **S2 Grupo**, **Ackcent** y la reciente **Cipher** (resultante de la antigua Prosegur Ciberseguridad y su compra de la homónima brasileña).

Además, nuestro país empieza a hacerse un hueco entre los proveedores de servicios de ciberseguridad en el mercado europeo. Gartner ha incluido a **Aiuken** (MSSP en nube) y a **Telefónica** en su listado de las diez compañías más 'interesantes' en este campo, dentro de su 'Cuadrante Mágico 2019' para el mercado europeo.

Según la consultora, ambas destacan por ser "proveedores notables". Se trata de la primera vez que Aiuken forma parte de este informe y en él se destaca su flexibilidad, personalización tanto del producto como de la plataforma, y su buena aplicación de tecnología propia para la detección de incidentes de ciberseguridad. Por su parte, de Telefónica resalta un portafolio muy completo, maduro y evolucionado y un equipo con experiencia, especializado en ciberseguridad, a través de sus tres SOCs en Europa (dos en Madrid y uno en Reino Unido).



A efectos generales, se detecta un cierto sobredimensionamiento de la oferta en el mercado español, en parte motivado por la "obligación' que toda compañía de TIC tiene de ofrecer servicios en este campo, y en parte mantenido por la salida natural a los mercados hispanoamericanos. Sucede que la mayoría de prestadores generalistas no vieron el auge de los servicios de ciberseguridad y han engordado la oferta cuando el sector estaba ya muy organizado y contaba con firmas especializadas o con habilidades de ciberseguridad por las que habían apostado hace muchos años.

Estas compañías pioneras (menos de una decena) son, salvo honrosas excepciones, las más experimentadas en la prestación de servicios gestionados, y, en general, en la práctica y la disciplina de la ciberseguridad orientada a los mercados corporativos (Ibex 35 y grandes empresas).

PROVEEDORES TIC EN ESPAÑA CON OFERTA DE MSSP

- ACCENTURE
- ACKCENT
- AIUKEN CYBERSECURITY
- ATOS
- BT
- CAPGEMINI
- CIPHER
- DAVINCI
- DELOITTE
- DXC TECHNOLOGIES
- ENTELGY INNOTEC SECURITY
- EVERIS (NTT)
- FUJITSU
- GFI
- GMV SECURE eSOLUTIONS
- GRUPO ICA
- IBM
- IECISA
- INGENIA
- INDRA-MINSAIT
- ITS
- LOGICALIS
- MDTEL
- MNEMO
- NECSIA
- NUNSYS
- OESÍA
- ONESEQ
- S2 GRUPO
- SECURA
- SECURE&IT
- SOTHIS
- SIA
- S21SEC
- SYMANTEC
- TELEFÓNICA
- THALES
- T-SYSTEMS

5 SOC: luces y sombras del corazón de los MSSPs

Los Centros de Operaciones de Ciberseguridad (SOC) son el corazón de los servicios de seguridad y su punto de referencia. Y, por ende, son la principal herramienta de los MSSPs. A través de los SOC, ya sea en local o en remoto, se puede disponer de una razonable visibilidad de lo que ocurre en el ciberespacio en cada empresa y hacer frente a amenazas.

Desde sus comienzos, a mediados de los años 70, en EE.UU., los SOC han vivido varias revoluciones y la más grande, con la llegada del 5G, está por llegar. Un mundo con miles de millones de dispositivos conectados entre sí, todo tipo de sistemas automatizados y la llamada Industria 4.0 generará la necesidad de más y mejores SOC dedicados para proteger coches, casas, empresas y, por supuesto, ciudades.

Actualmente, se calcula que existen en el mundo unos 285.000 SOC de diferentes tamaños, aunque el 52% de las empresas con más de 10.000 trabajadores tienen uno, según destaca en un estudio **EY**, y hay unos 5.200 dando servicios a pymes.

Un SOC tradicional, usando técnicas de bloqueo, monitorización y gestión de vulnerabilidades, puede mitigar hasta el 90 % de los ataques, según un estudio de **Black Hat**, que destaca que el 10% restante, ataques sofisticados y dirigidos, son la principal preocupación para el 48% de los profesionales de seguridad.

Además, en su informe constata que el 71% de los SOC con una madurez alta (preparados para responder a incidentes), suelen solucionar los incidentes más graves en menos de una semana, gracias al contexto proporcionado por los analistas más especializados, los llamados "cazadores de amenazas" (*Threat Hunting).*

Un mercado millonario

De hecho, el mercado de SOC se prevé que mueva este año cerca de 28.000 millones de euros, según la consultora **Research and Markets**. Y se espera que crezca, de aquí a 2025, a un ritmo de un 11,5% anual, fruto de la mayor demanda de servicios gestionados de ciberseguridad. Para entonces se situará casi en el doble: 54.000 millones.

La razón es sencilla: ya no es posible gestionar el riesgo digital únicamente con recursos propios. Y tecnologías como el IoT o el 5G lo hará más complejo aún y obligarán a medir bien la inversión en este tipo de centros propios por parte de las empresas: se calcula que tiene un coste un 80% mayor que contratar servicios gestionados a través de SOC, según datos de **CI Security.** "Hay muchas alternativas a la creación y dotación de personal de un SOC interno, y las empresas deberían explorarlas, además de los diversos tipos de modelos SOC", destaca el analista principal de Gartner Research, **Siddharth Deshpande.**

A día de hoy, medio centenar de empresas pugnan en el mundo por ofrecer los mejores servicios de SOC. El reto no es defender el perímetro… ahora se trata de anticiparse a las amenazas. Para ello, referentes como Symantec, Microsoft, IBM, BT, Cisco o, en España, Telefónica y Aiuken, cuentan con acuerdos con terceros especializados analizando y compartiendo teras de información que las permitan anticiparse.

En ellos trabajan desde analistas hasta ingenieros de seguridad y gerentes, con una amplia experiencia en TI y redes, generalmente con formación en ingeniería informática, criptografía, ingeniería de re-

1975, se crea el primer SOC

El primer embrión de lo que hoy son los SOC comenzó a funcionar en EE.UU. en 1975, bajo la denominación de 'Centro de Operaciones de Seguridad de la Información' (ISOC). Estaba pensado para monitorizar posibles virus informáticos en los sistemas más críticos del Departamento de Seguridad Nacional (DHS).


NSOC watch floor circa 1975

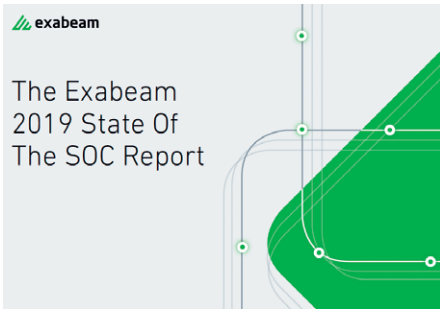
des o ciencias de la computación y certificaciones como CISSP o GIAC, expertos en cuyo trabajo ya están impactando tecnologías como la IA, que les permite "centrarse en las amenazas más complejas y liberarles de las más repetitivas y sencillas". Con ello, se ganará en calidad de los planes de respuesta a incidentes.

Problemas para el SOC

Eso sí, un estudio del Instituto SANS, de 2018, sobre la situación de los Centros de Operaciones de Seguridad, indica que aún queda mucho por hacer, ya que a pesar de su evolución aún se enfrentan a muchos obstáculos, como son: la falta de herramientas eficaces e integradas para inventario de activos y eficaces; la dificultad de proteger a una empresa por la compartimentación entre departamentos y tecnologías; la falta de personal especializado; así como una automatización ineficaz, sobre todo, para correlar eventos, entre otros aspectos. De hecho, por raro que parezca, el informe destaca que "sólo la mitad de los SOC están utilizando métricas", que resultan imprescindibles para gestionarlo de forma correcta y pedir los recursos necesarios para mejorar de forma continua.

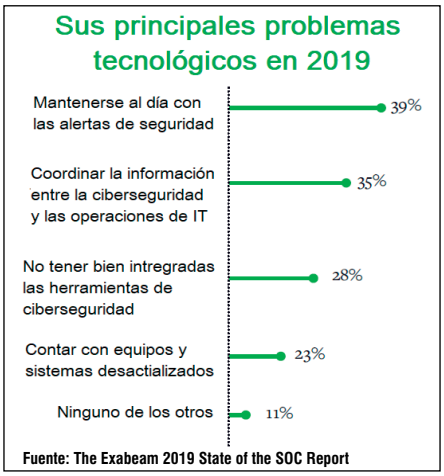
Vida del SOC en 2019

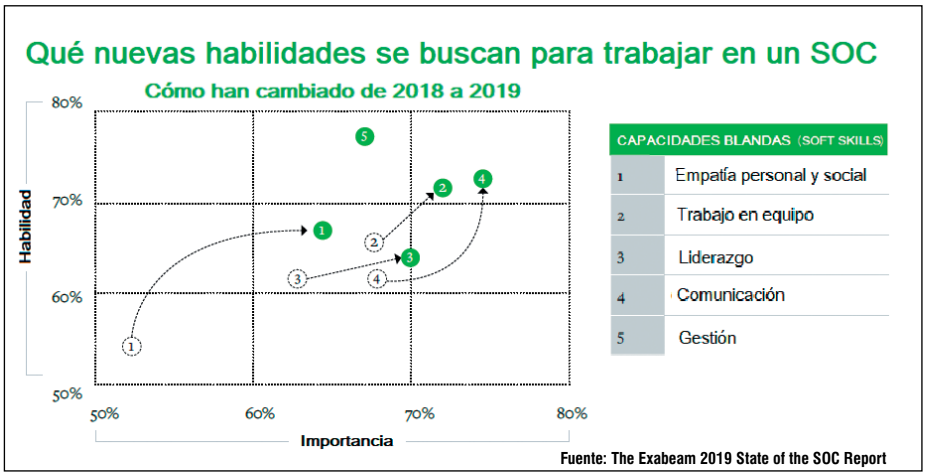
A pesar de sus más de 30 años de vida, los SOC no han hecho más que empezar. Sólo en un año han experimentado grandes cambios, según el estudio de la empresa **Exabeam,** realizado por **Cicero Group,** que analiza su situación en EE.UU. y Reino Unido. Para ello se ha preguntado a 150 responsables de este tipo de instalaciones, así como a CIOs y CISOs.



Grado de satisfacción por servicio

Fuente: The Definition of SOC-cess
SANS 2018 Security Operations Center Survey





En su edición de 2019, identifica los cambios de roles y responsabilidades como uno de los desafíos más apremiantes para los gerentes de estos centros. Esto se plasma en que los máximos ejecutivos apuesten por trabajar en la respuesta a incidentes y la búsqueda de amenazas, dejando a los técnicos las labores menos operativas. Además, gran parte de ellos considera que la gestión del talento y el déficit de profesionales capacitados también es un freno importante: uno de cada tres trabajadores del SOC destacó la falta de personal para hacer bien su trabajo.

Entre los grandes retos actuales, destaca la complejidad para encontrar personal adecuado, al igual que los falsos positivos y la complejidad para generar informes y documentación fácil de interpretar por el cliente. También, el mantenerse al día con las alertas de seguridad generadas de forma automática y analizadas por los expertos del SOC (39%). Entre otras razones, por la incapacidad de las aplicaciones heredadas para registrar eventos de forma eficaz.

Y es que el gran problema continúa siendo tener una visibilidad completa de los eventos que suceden en toda la empresa. Sin ella, los gestores de SOC no son eficientes en la priorización de las alertas de seguridad para centrarse en las realmente críticas. "Hay un dicho que dice que lo que no conoces no puede hacerte daño. Pero esto en seguridad no es así: lo que no se conoce o peor aún, lo que no ves…, va a impactar significativamente en tu negocio", destaca el responsable de Estrategia de Seguridad de Exabeam, **Steve Moore**. "La razón es clara: no se puede proteger lo que no se ve".

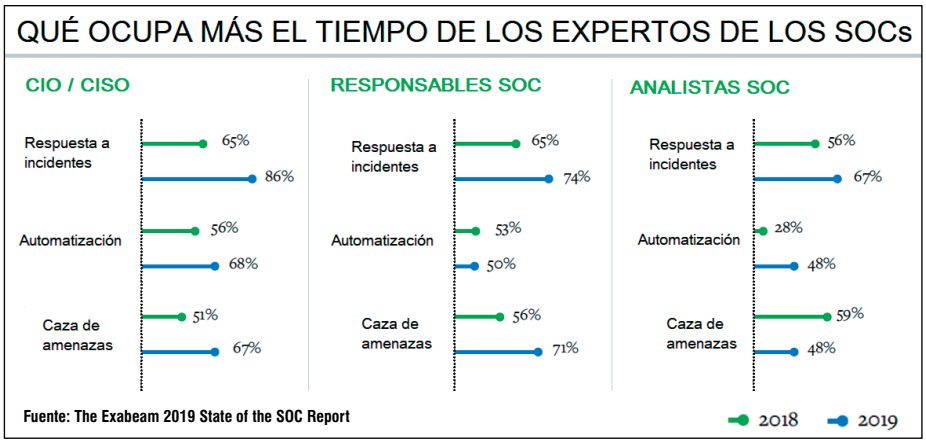
Y es que la visibilidad y poder contextualizar un evento, unido a la automatización, se han convertido en los grandes retos de los actuales SOC para poder ofrecer una defensa proactiva y eficaz frente a adversarios cada "vez más sofisticados".

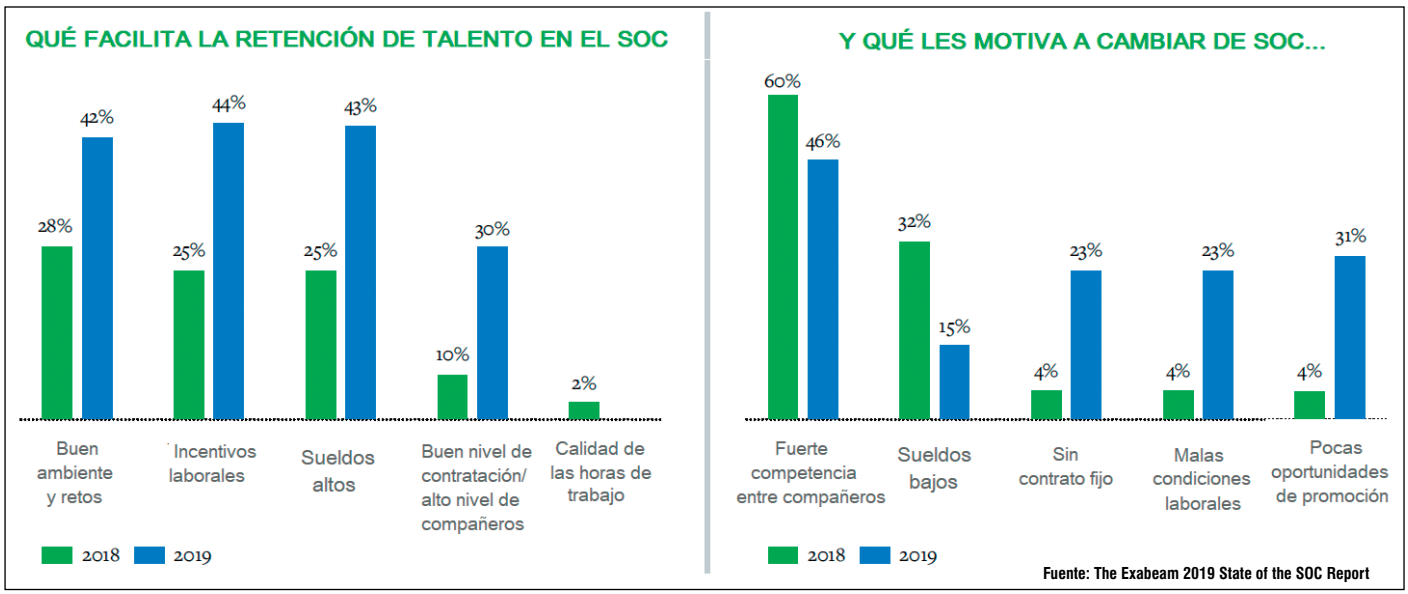
Marcando tendencia

Curiosamente, en los SOC no todo es tecnología. El estudio de Exabeam destaca la "creciente importancia que están cobrando las habilidades personales y sociales, como la comunicación". De hecho, el 65% de los encuestados las destacó como un elemento fundamental para tener éxito en la gestión de los riesgos con los clientes y la propia empresa. También, han crecido en importancia las llamadas 'habilidades duras' como la capacidad de búsqueda de amenazas (*threat hunting)* desde un 7% hasta un 69%, así como de prevención de pérdida de datos (DLP), desde un 8% hasta un 75%.

En cuanto a si este tipo de centros son realmente eficaces, el 71% se muestra satisfecho en EE.UU. por su capacidad para monitorizar y analizar eventos, frente a sólo un 54% en el Reino Unido, unas cifras similares a las del último año. Eso sí, los SOC más pequeños, aquellos con menos de 24 personas, confesaron haber incrementado su eficacia de respuesta a incidentes (en un 79%).

Su talón de Aquiles es la percepción para solventar incidentes de forma automática desde el SOC (54%), un 14% menos que en la anterior edición del estudio. A este problema se suma su dificultad para generar informes y documentación de forma adecuada (33%), los falsos positivos (27%) y las excesivas alertas. Además, se considera problemático dar con personal con experiencia (29%), que es, a ojos del CISO o CIO, garantía de eficacia en un servicio de SOC y que, unido a la carestía de expertos, incrementa aún más el problema de disponer de los recursos humanos necesarios y estables.





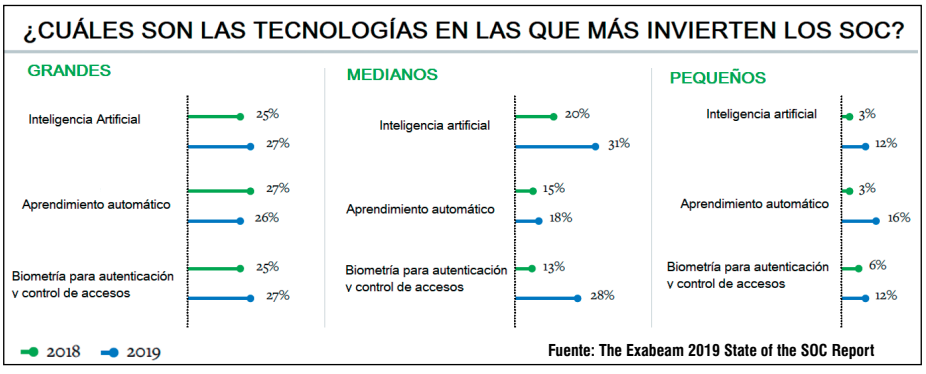
Asimismo, se destaca que mientras los CIO y CISO están más preocupados por la respuesta a incidentes (hasta un 21%) y la automatización (hasta un 12%), las principales inquietudes para los analistas de los SOC son el incremento de la automatización (hasta un 20%) y de las capacidades de respuesta a incidentes (hasta un 11%).

Además, hay una diferencia importante entre los CISO y el personal del SOC respecto a la importancia y eficacia de la respuesta a incidentes, ya que los primeros le dan un peso de un 52% frente a los segundos con un 24% y los incidentes escalados con un 46% por un 33%.

Inversión en nuevas soluciones

Casi el 50% de los SOCs con menos personal destacaron que no cuentan con suficiente presupuesto para mejorar su tecnología; sin embargo, los más grandes confesaron que no basta con gastar en ella, sino que hay que hacerlo de forma constante en lo último y más nuevo (39%).

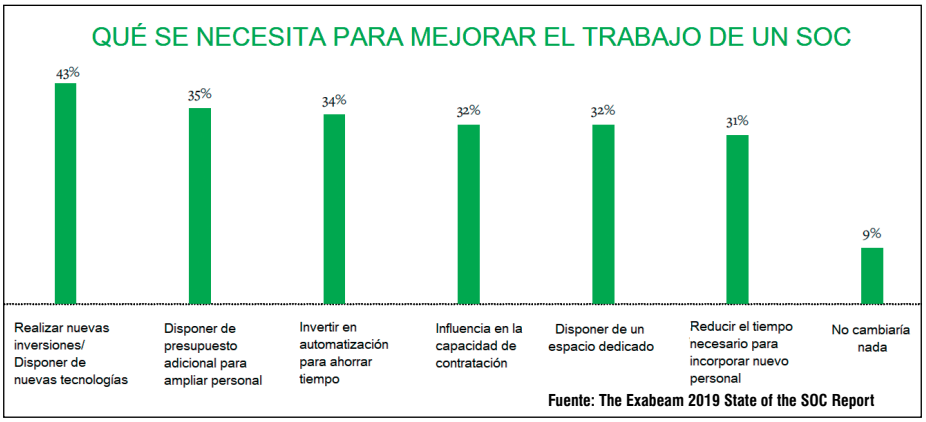
En concreto las mayores inversiones en los centros son en análisis de *big data* (39%), de sistemas para el análisis del comportamiento de usuarios y entidades (UEBA) (22%), así como en inteligencia artificial (23%) y aprendizaje automático (21%). Estas dos últimas son las que más han crecido en el último año, sobre todo en los SOC medianos y pequeños por la automatización de procesos que ofrecen, al igual que la autenticación biométrica y la administración automática de control y gestión de accesos.



Subcontratación

Además, el 50% de los responsables de los SOCs explicó que parte de los servicios que ofrece los subcontrata, sobre todo, los de análisis de *malware*, de amenazas y la inteligencia de amenazas. Por el contrario, se apuesta por la gestión interna en lo que atañe a la monitorización de eventos y su análisis.

Un SOC incluye tanto tecnología de seguridad como la gestión de procesos, de talento de personal especializado (divididos en varias 'líneas' de defensa, según su grado de capacitación y especialización), así como de capacidad para hacer frente a incidentes y responder a ellos, si llegara el caso, de forma ofensiva en caso de que se pongan en riesgo el negocio o sistemas críticos de seguridad nacional.



6

RETOS, ALIANZAS Y ESPECIALIZACIÓN

El futuro de los MSSPs: ¿morirán de éxito?

Vivir en un mundo hiperconectado hará que todo los proveedores de servicios gestionados amplíen su mercado, sobre todo, entre el sector público que, posiblemente, tenga que hacer frente a la seguridad de millones de dispositivos conectados en hospitales, carreteras, ciudades, organismos, aplicaciones… al igual que muchas empresas privadas, como las de automóviles, que tendrán que desplegar todo tipo de sistemas para proteger la conectividad de sus clientes y productos, muchos con datos críticos.

Por eso, los MSSP especializados en campos como el Internet de las Cosas y los entornos industriales (OT) crecerán exponencialmente. Y para ello, también trabajarán de forma confederada entre el sector público y privado y con empresas de todo el mundo para tener una visión precisa del ciberespacio y sus posibles amenazas. El éxito o fracaso de los MSSP dependerá de crear conciencia de marca "con propuestas diferenciadas de sus competidores y asegurando que su oferta cumpla lo que prometen hacer para ser realmente eficaces", según destacan en Digital Defense, que considera que el gran reto será desarrollar soluciones altamente escalables para soportar 'picos de rendimiento', bajo demanda, con aplicaciones multiusuario (*multi tenancy*), ofreciendo servicios a varios clientes a la vez de forma eficiente y con herramientas que eviten la fatiga de los analistas, quitándoles las labores más tediosas, para centrarles en las que realmente puedan sacar partido de sus altas capacidades.

Por supuesto, el incremento de la complejidad entre tecnologías y sistemas exigirá mayores capacidades de

orquestación, plena visibilidad en paneles de control totalmente unificados y una oferta complementaria de servicios, por parte del MSSP, para mejorar la seguridad de los clientes según vayan creciendo o transformándose. Por eso, para los proveedores de servicios de seguridad uno de los grandes retos será contar con fabricantes y socios que les permitan anticiparse a las demandas del mercado, un panorama que vendrá marcado por los servicios de MSSP especializados en IoT, aplicados a gestión de flotas, telemáticas en oficinas y hogares, fábricas 4.0, cibervigilancia, supervisión de conectividad segura en productos conectados, ciudades inteligentes, servicios públicos... Y, sobre todo, por garantizar la identidad digital de personas físicas, personas jurídicas y cosas en todo tipo de servicios.

El vicepresidente de Gartner, **Steve Prentice,** en el simposio anual ITxpo de la firma, en Barcelona, manifestó que "la forma en que viviremos con la tecnología en 2030 estará determinada por cuatro tendencias tecnológicas clave: computación ambiental, dispositivos inteligentes, ciberseguridad y ética, información y análisis". "Y a medida que cada producto, servicio y proceso se digitaliza, la 'nube' del producto puede ser más valiosa que el producto en sí".

Además, recordó que "para la siguiente década, a medida que obtengamos acceso a información casi ilimitada de múltiples fuentes, la ética digital será clave para la gestión de riesgos. Con todo lo que estará conectado y miles de millones de máquinas inteligentes, las oportunidades de hacer algo incorrecto (ignorar la privacidad, favorecer a las máquinas, robar, etc.) estarán constantemente allí". Evitarlo a través de una estrategia de seguridad interna, integrando las capacidades de un MSSP, representará uno de los mercados más boyantes.