Penteo
Analista TIC

Marketing Report

Universo Penteo

Proveedores de Servicios de Ciberseguridad

ACKCENT

Departamento de Análisis Penteo | Diciembre del 2018

info@penteo.com 902 154 550 www.penteo.com @penteoanalyst Penteo ICT Analyst | Penteo Business and IT Executives

La ciberseguridad se ha convertido en una de las prácticas prioritarias para la mayoría de las organizaciones, debido a la transformación digital que se está llevando a cabo en empresas tanto privadas como públicas, y que asegura una correcta evolución en el sector previniendo ataques de carácter malicioso que puedan poner en riesgo sus activos de información. El presupuesto destinado a soluciones y herramientas de prevención que mitiguen los riesgos asociados a la seguridad ya no es percibido como un gasto por la dirección general, sino como una inversión en el negocio.

Índice de contenidos

Introducción

La ciberseguridad ha pasado de ser una cuestión restringida a los perfiles técnicos y expertos en la materia, a estar en la mesa de los comités de dirección como elemento clave a la hora de proteger los activos de información de las organizaciones. El 40% se consideran medianamente vulnerables a ciberataques y un 17% considera que su grado de exposición es alto. [(1)]

La práctica de la ciberseguridad abarca varios ámbitos, y algunos de los más comunes son los relacionados con la seguridad gestionada (SOCs), seguridad de contenidos (detección de *ransomware* y cualquier otro tipo de ataque de código malicioso) y control de accesos, que aparecen implantados en más del 90% de las empresas. Por otro lado, existe aún desconocimiento acerca de ámbitos más emergentes en ciberseguridad, como sistemas para la prevención de la fuga de datos (Herramientas de DLP) o la aplicación de Planes Directores de Seguridad (PDS) y la formación del empleado mediante campañas de concienciación de ataques de ingeniería social o también conocidas como campañas *anti-phishing*. [(1)]

Sin duda, los tiempos en los que las inversiones en ciberseguridad tenían dificultades para ser aprobadas por las direcciones generales empiezan a ser parte del pasado. El compromiso de la Dirección y el mayor peso del CISO en la organización comienzan a ser factores relevantes para que el sector de la ciberseguridad pueda crecer y tener mayor recorrido en las organizaciones, sobre todo, tras los últimos ciberataques perpetrados contra organizaciones internacionales y de reconocido prestigio, así como la aparición de brechas de seguridad en algunos de sus sistemas.

En los últimos meses, y debido a las consecuencias jurídicas que ha provocado, ha tenido mucha repercusión la fuga de información y apropiación indebida de datos personales de millones de usuarios de Facebook. Además de éste, se han perpetrado distintos tipos de ciberataques a lo largo del año que han ocasionado que las organizaciones estén cada vez más concienciadas acerca de la seguridad informática. Algunos de los ataques más sonados los detallamos en este informe.

[(1)] Ver informe Penteo: Market Trends 2018 – Tendencias de Ciberseguridad en España

Ciberataques en 2018

Tras el ciberataque WannaCry perpetrado en 2017 contra grandes organizaciones europeas, la repercusión de los ataques informáticos o las brechas de seguridad informáticas han seguido teniendo una alta repercusión mediática, ya que la concienciación de los profesionales de la mayoría de las compañías ha aumentado durante los últimos meses y el desconocimiento de la práctica de la ciberseguridad ya no es tan alto, consiguiendo que tanto usuarios, clientes finales o empleados conozcan este sector de la informática. Por todo esto, muchos medios, y no solo los más especializados, se han hecho eco de los ataques más mediáticos que se han producido a lo largo de este año, y que sin llegar a tener la repercusión que tuvieron los ataques tipo *ransomware WannaCry y NotPetya*, se han dado a conocer en el mundo profesional. Los más destacados han sido:

- Filtraciones de datos de más de 50 millones de usuarios estadounidenses de Facebook, por las que el CEO de la compañía tuvo que declarar ante los tribunales y pedir disculpas por este "gran" descuido. A través de una app de predicción de personalidad en base al perfil del usuario, Facebook se vio envuelta sin prever tal magnitud, en un escándalo de manipulación y robo de datos por parte de investigadores afines a una consultora que más tarde proporcionaría toda esa información a uno de los partidos políticos del país, para su posterior interpretación y predicción de intención de voto. En España este tipo de falla de seguridad se podría asemejar a la que sufrió Movistar hace unos meses, en la que una brecha de seguridad en su web comprometió durante unas horas datos confidenciales y personales de sus clientes, aunque el número de estos no llegó al centenar.
- En marzo de este mismo año se produjo el mayor ataque de denegación de servicio (DDoS) de la historia. Lo sufrió la página web de código abierto GitHub, y a pesar de la gran cantidad de tráfico que impactó contra la plataforma, 1,35 Tbps (terabits por segundo), los responsables consiguieron mitigar el ataque en 9 minutos. Éste consistió en aprovecharse de más de 100.00 servidores que replicaron la IP de la web y que enviaban la solicitud de datos que ponía en un compromiso la disponibilidad de la web, produciendo la caída de esta durante ese período de tiempo. En nuestro país, este tipo de ataques es sufrido muy a menudo por organismos públicos, como fue el caso del Banco de España durante este verano, y que provocó la caída de la web, perpetrado en este caso por el grupo de hackers Anonymous Catalonia desde servidores externos.
- En agosto, una falsa campaña de correos de phishing detectada por el INCIBE informó de un caso de dirigido hacia usuarios y cuentas de Paypal. En este tipo de correos se adjuntaba una factura y supuesta compra del cliente con el fin de llevar a cabo una suplantación de identidad y así conseguir acometer pagos con la cuenta suplantada. El parecido en los correos venía dado por el uso de una estructura muy parecida mediante logo y facturas, pero el dominio de las cuentas de correo desde donde se enviaban era lo que delataba que todo era una campaña defraudadora. Además, en los correos aparecía un enlace con la solicitud de credenciales y datos bancarios, por lo que acceder a esta URL podía comprometer al cliente a ser víctima del ataque.
- No sólamente organizaciones y compañías en las que predomina el uso de software se han visto afectadas, también compañías fabricantes de hardware, en este caso Intel y AMD, debido a la aparición de fallos de seguridad y vulnerabilidades en sus chips. Dos ataques que aprovechaban estos fallos de diseño, Meltdown y Spectre, afectaron a millones de estos dispositivos, habilitando el acceso a los hackers para la introducción de malware y el robo de claves de seguridad de los sistemas en los que se encontrasen instalados.
- Tampoco nos podemos olvidar este año del *ransomware*, ya que la administración pública de Atlanta (EE. UU) ha sido una de las últimas víctimas de este tipo de ciberataque, en el que una gran cantidad de programas de software se vieron afectados, sobre todo los usados por la policía y los tribunales de justicia, y por el que se los cibercriminales exigían un rescate de 51.000 dólares en modo de pago bitcoin para la recuperación de la información secuestrada.

1. Definición del Universo de Ciberseguridad 2018

Contexto

Por **ciberseguridad** entendemos la práctica que engloba las disciplinas y herramientas destinadas a salvaguardar la seguridad informática tanto de organizaciones como de usuarios particulares, así como las políticas, medidas de seguridad, análisis de riesgos y categorización de amenazas que se desarrollan para la protección de activos de información (aplicaciones, plataformas, infraestructuras, información), expuestos habitualmente al acceso no autorizado y a los ataques de agentes externos.

Los servicios asociados se materializan en una oferta de implantación y administración continua relacionada en todo momento con la formación y concienciación del empleado, el cumplimiento legal y normativo, la gestión de identidades, seguridad en aplicaciones, redes e infraestructuras; la seguridad de datos ya sea en los propios sistemas de la organización o en el Cloud; seguridad gestionada mediante centros de vigilancia y operaciones; y la gestión de la respuesta inmediata ante incidentes, así como su posterior recuperación en caso de desastre mediante servicios resilientes de contingencia y continuidad del negocio.

Alcance

Los proveedores de servicios de ciberseguridad son aquellos que proporcionan servicios externalizados de seguridad informática con un enfoque integral y multidisciplinar, abarcando uno o varios de los grandes ámbitos de la seguridad, como son el gobierno, protección, vigilancia y resiliencia de los ciber activos, todo ello desde un punto de vista tanto tecnológico como normativo.

- **Gobierno de la ciberseguridad:**
  - Servicio de oficina técnica de seguridad (plan director de seguridad, definición de políticas y normativas, análisis de riesgos).
  - Cumplimiento legal y certificación normativa; protección de datos (GDPR, SOX); Esquema nacional de Seguridad (ENS); seguridad en infraestructuras críticas (LPIC).
  - Formación y concienciación del empleado (workshops, seminarios, webinars, e-learnings); campañas de concienciación (vídeos, simulación de campañas de phishing).

- **Protección y seguridad de los activos:**
  - Gestión de identidades, control de accesos, gestión de permisos y autorizaciones (privilegios de acceso, autenticación…).
  - Protección de la información, prevención de fuga de información mediante herramientas DLP, cifrado de la información.
  - Seguridad en las aplicaciones, protección contra el malware, desarrollo del ciclo de vida del software (SDLC).
  - Seguridad en redes, segregación y segmentación de redes, seguridad en dispositivos móviles y seguridad en dispositivos IoT.
  - Gestión de activos.
  - Seguridad en el Cloud mediante políticas y normativas definidas, controles de seguridad y la propia seguridad proporcionada por el proveedor (CSP).

- **Vigilancia en las operaciones:**
  - Seguridad gestionada en centros de operaciones (SOCs); monitorización de eventos, accesos y actividades; testing y mejora continua de los procesos de detección de eventos.
  - Hacking ético; escaneo, identificación, análisis y priorización de vulnerabilidades; aplicación de parches de actualización; pruebas de "pentesting"; diagnósticos forenses.
  - Protección de la marca mediante prevención del fraude y de suplantación de identidad.

- **Servicios de resiliencia**:
  - Respuesta y aprendizaje ante incidentes; gestión de crisis; cyber wargaming; notificación de incidentes ante las autoridades.
  - Contingencia y continuidad del negocio; recuperación ante desastres.
  - Ciberseguridad en tecnologías emergentes (técnicas de ciberseguridad mediante IA, técnicas de seguridad en dispositivos IoT).
  - Mejora continua mediante incorporación de lecciones aprendidas, la actualización de estrategias de recuperación y la reducción en la probabilidad de futuros incidentes.

Tipos de proveedores

A continuación, se presenta el posicionamiento en el mercado de los proveedores que conforman el panorama de ciberseguridad en España clasificados por las siguientes categorías:

- **Estrella:** dispone de unas capacidades y prestaciones consolidadas, una propuesta de valor que da cobertura en todos los servicios analizados, presencia en todas las geografías, y una penetración amplia y variada en el mercado nacional.
- **Consolidado:** es un referente en el mercado y es capaz de dar un servicio completo end-to-end en la solución. Su propuesta de valor es sólida y aspira a convertirse en estrella.
- **Desafiante:** tiene experiencia en la tecnología y da servicios de calidad en los ámbitos analizados. Aspira a tener más presencia en el mercado para evolucionar a un proveedor consolidado.
- **Emergente:** ha iniciado su camino en la tecnología posicionándose entre los principales proveedores del mercado nacional, disponiendo de un gran potencial de crecimiento.

Criterios de inclusión

Los proveedores deben ofrecer servicios gestionados de ciberseguridad que abarquen la mayor parte de necesidades corporativas en este ámbito identificadas en el siguiente listado:

1 | Presencia y capacidad en España para ofrecer los servicios:

- Oficinas en, al menos, Barcelona o Madrid.
- Disponer de un mínimo de 5 clientes activos.

2 | Cobertura mínima relativa a los servicios ofrecidos:

- Implantación y gestión de soluciones.
- Servicios continuos de soporte y mantenimiento.
- Cumplimiento legal y/o normativo.
- Asesoría tecnológica y organizativa relacionada con la ciberseguridad.
- Gestión de incidentes de ciberseguridad.

3 | Mecanismos de contratación:

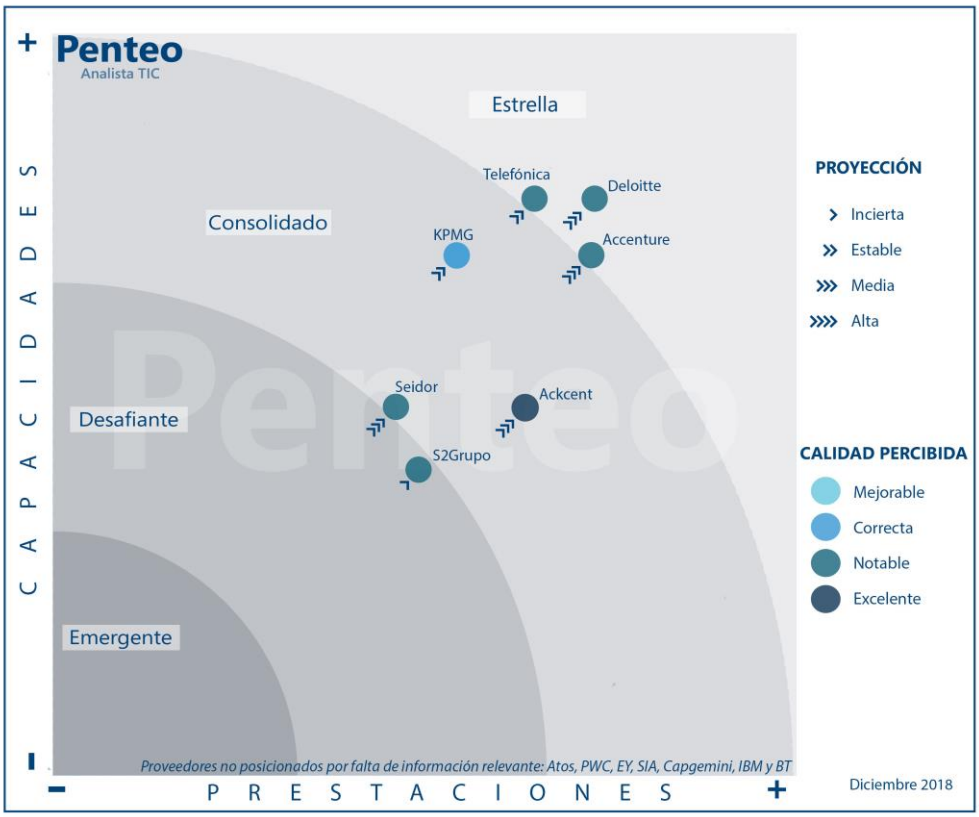
- Gestión y adecuación del contrato a las necesidades de cliente.
- Facturación consolidada de los distintos servicios.

Segmento de clientes

Se incluyen en este universo proveedores de soluciones y servicios para compañías de todos los sectores de actividad y volumen de facturación. En general, las organizaciones cliente que apuestan por servicios gestionados de la ciberseguridad se enmarcan en el segmento corporativo de gran empresa, normalmente más proclives a adoptar servicios totalmente gestionados asociados a grandes volúmenes de activos (infraestructuras, aplicaciones, datos, etc.) que les reduzcan la operación continua de servicios que no son el foco de su negocio.

Dicho esto, las pequeñas y medianas empresas, que normalmente tienen más limitaciones de recursos, también son proclives a utilizar servicios de ciberseguridad, ya sea para instalar y gestionar algún elemento de seguridad perimetral, para evitar ataques de código malicioso mediante la implantación de antivirus o por verse sometidas a alguna normativa que exija auditoría y cumplimiento, por poner algunos ejemplos.

2. Mapa del Universo



Dimensiones evaluadas en el marco de análisis:

Para efectuar la evaluación[3] se ha analizado el posicionamiento relativo de los actores seleccionados en función de dos dimensiones, caracterizadas de acuerdo a 9 factores formados por 33 indicadores, que se desglosan en más de 120 preguntas respondidas por los proveedores. Esto se ha combinado con 15 entrevistas personales, realizadas a sus clientes, y una encuesta respondida por CIOs, responsables de servicios tecnológicos y CISOs de más de 100 empresas españolas o multinacionales con operaciones de tecnología presentes en España.

A. Las **CAPACIDADES** evalúan:

- **Solidez en la línea de servicio:** a nivel nacional e internacional, en antigüedad de la compañía, volumen de ingresos, número de clientes y peso de la línea de negocio.
- **Capacidad del delivery:** centros de delivery, excelencia de los centros, distribución de perfiles, capilaridad del delivery por TIER, geografías y sector.
- **Equipo:** número de FTEs, estructura piramidal, formación del equipo, gestión del talento e índice de rotación.
- **Go To Market:** propuesta de valor, organización comercial, gestión comercial y aproximación al cliente.

[3] Adicionalmente, la calidad de la información proporcionada por los proveedores también es un factor indirecto de influencia en la valoración. Aun así, ésta se ha realizado con la mejor información disponible, complementada por fuentes secundarias tales como entrevistas a clientes, encuestas, datos recopilados fruto de procesos de selección realizados por Penteo, u otros.

B. Las **PRESTACIONES** evalúan los servicios de ciberseguridad ofrecidos y, de forma relevante, la satisfacción de los clientes que los están utilizando:

- **Cobertura del servicio**: disponibilidad en el portafolio y número de FTEs dedicados.
- **Alcance del servicio:** descripción de cada uno de los servicios del portafolio.
- **Herramientas y metodologías:** metodologías de análisis de riesgos, herramientas GRC, soluciones tecnológicas provistas (DLPs, sistemas de detección de malware, etc), sistemas de monitorización de eventos, etc.
- **Buenas prácticas:** aplicación de las mejores técnicas de ciberseguridad en cada uno de los ámbitos analizados: gobierno, protección, vigilancia y resiliencia.
- **Capilaridad del mercado:** Top Of Mind, principales competidores, distribución de clientes por ámbitos, por TIER, por geografías y por sectores.

C. La **PROYECCIÓN** evalúa por un lado la evolución pasada y previsión futura en volumen de negocio, clientes, empleados y, por otro lado, las estrategias de innovación en el producto, servicio y crecimiento de la compañía y línea de negocio.

D. La **CALIDAD** evalúa la satisfacción de los clientes en el proceso comercial, en el delivery del servicio, en la cobertura de expectativas y en la compañía.

Posicionamiento de los diferentes actores

- **ACCENTURE,** uno de los proveedores que más tiempo lleva en el sector, presenta un portafolio de servicios que abarca todos los ámbitos, destinando un elevado número de recursos a cada uno de ellos. Con una estrategia muy planificada, tiene una alta presencia en el mercado, a la vez que la adquisición de pequeñas compañías especializadas en la materia le permite posicionarse como una de las compañías más innovadoras del mercado.

- **ACKCENT,** compañía altamente especializada en ciberseguridad, gracias al alto conocimiento técnico de su personal. Sus clientes muestran un alto grado de satisfacción con los servicios provistos, y en estos últimos años ha incrementado tanto su cartera de clientes como su nivel de ingresos. Aunque joven, este proveedor ha ido ganando notoriedad progresivamente en el sector, lo que ha supuesto su consolidación dentro del Top of Mind de proveedores de servicios de ciberseguridad.

- **DELOITTE,** dispone de un portfolio de servicios completo y adaptado, profesionales certificados en todas las áreas, así como relaciones estratégicas con proveedores de soluciones líderes del mercado. Ofrece conocimiento, preparación y respuesta en materia de ciberseguridad de alta calidad. Sus centros de excelencia y operaciones en Madrid y Barcelona, con equipos técnicos altamente cualificados, le permite cubrir con garantías todo el portafolio de sus servicios.

- **KPMG,** tiene el área de transformación de la seguridad que ofrece servicios de formación y concienciación, gestión de identidades y arquitecturas de seguridad en base al despliegue de una oficina adaptada a sus clientes. Destacan sus servicios de asesoramiento estratégico en el cumplimiento de normativa de ciberseguridad. También provee servicios más técnicos de ciberdefensa y respuesta a incidentes.

- **S2 GRUPO,** dispone de un portafolio de servicios especializados en 4 ámbitos diferenciados: seguridad en los sistemas de información, monitorización y control de accesos, gestión de la seguridad en tiempo real y explotación de plataformas tecnológicas. Destacan sus servicios de implantación de SGSI y asesoramiento en el cumplimiento de las normativas del sector. Dispone de soluciones y productos propios especializados.

- **SEIDOR,** dispone de una estrategia definida en materia de ciberseguridad y presenta un crecimiento constante en esta línea de negocio. Abarca un amplio y diverso número de clientes en diferentes sectores, y estos valoran positivamente su flexibilidad a la hora de poder personalizar sus servicios en base a las necesidades del negocio del propio cliente.

- **TELEFÓNICA,** uno de los líderes del mercado tanto en prestaciones como en capacidades. Dispone de una elevada experiencia en el sector, una imagen de marca muy consolidada en materia de ciberseguridad y un portafolio muy completo. Al ser una multinacional, dedica un alto número de recursos a los servicios que provee.

Actores no posicionados por falta de información relevante

- **ATOS,** tiene capacidades end-to-end y uno de los portfolios más completo y maduro en servicios de ciberseguridad. Además, cuenta con bastante experiencia y soluciones propias en el despliegue de este tipo de servicios. También disponen de productos y soluciones de ciberseguridad adaptados a las tecnologías emergentes.

- **BT,** multinacional con mayor presencia a nivel global que local. Dispone de servicios más especializados en la seguridad gestionada, entre los que destacan la protección frente a ataques de denegación de servicio, seguridad en el Cloud y la supervisión monitorizada de eventos de seguridad. También realiza evaluaciones del grado de madurez de seguridad de las compañías mediante revisiones y análisis de riesgos.

- **Capgemini,** uno de los proveedores que menos tiempo lleva en el mercado, pero que se ha hecho un hueco gracias a las referencias de sus clientes. Destacan sus servicios de adecuación y preparación para el cumplimiento de GDPR en materia de ciberseguridad. Ha experimentado un alto crecimiento, debido a que también cubre servicios de otros ámbitos como los de seguridad gestionada a través de su centro SOC y equipos CERT, y de protección mediante servicios de control de accesos y gestión de identidades.

- **Grupo SIA**, es una compañía de origen español con presencia en Madrid, Barcelona y La Coruña, con un portafolio de servicios que incluyen diseño e implantación de infraestructuras de seguridad en la red, gestión de identidad y accesos, firma electrónica y custodia de documentos. Desde su centro de excelencia SIA-CEC, con servicio 24 x 7 y ANS, ofrecen inteligencia, monitorización, prevención, análisis de código malicioso, forencic y gestión de incidentes. También ofrecen servicios de gobierno y cumplimiento de las normativas.

- **EY,** dispone de programas de ciberseguridad, especialmente orientados a entidades financieras, con servicios de assesment, evaluación de vulnerabilidades o implantación de oficinas técnicas de seguridad, así como servicios de prevención, detección y respuesta ante incidentes, gestión de identidades y accesos, protección y privacidad de datos y resiliencia.

- **IBM,** multinacional que ofrece servicios end-to-end en infraestructuras de una forma integrada, automatizada y completamente gestionada para la prevención de riesgos. Destacan servicios técnicos que provee su equipo IBM X-Force, como los de respuesta ante incidentes o el análisis de amenazas detectadas. También ofrece servicios de cumplimiento como los relacionados con la protección de datos y las normativas asociadas.

- **PwC,** ofrece servicios de estrategia y negocio de la ciberseguridad, de continuidad y resiliencia, auditoría y cumplimiento normativo, y servicios más técnicos como el despliegue de arquitecturas seguras de red en

entornos IT, OT y servicios de SOC y CERT. Destacan sus servicios de asesoramiento legal en los que ofrecen planes estratégicos para la protección y privacidad de la información.

3. Puntos clave del mercado

Como comentábamos, el mercado de la ciberseguridad ha pasado de ser una cuestión restringida a especialistas en la práctica a estar encima de la mesa de los comités de dirección como elemento clave y estratégico en los procesos de negocio de las organizaciones. Aun así, la concienciación al respecto en la mayoría de las empresas y el presupuesto que las organizaciones destinan a esta materia tanto en las líneas estratégicas como en las más tecnológicas son aún mejorables.

En cuanto a las soluciones más adoptadas por las organizaciones, destacan las de seguridad de contenidos para la detección y prevención del malware, así como las de gestión de identidades y el control de accesos. Está previsto que avance la implantación de soluciones para la prevención de fuga de datos (DLPs), debido a la repercusión mediática que han tenido algunos de robo de información que se han dado en diversas organizaciones. Además, los Comités de Dirección priman por encima de otros aspectos el cumplimiento de las regulaciones que impactan en la actividad del sector. Por tanto, la estrategia a seguir en cuanto a cumplimiento normativo es evidente, lo que lleva a que el ámbito de gobierno de ciberseguridad sea una de las prioridades de las organizaciones. Por otro lado, los servicios de seguridad gestionada provistos con la intención dar una respuesta temprana a cualquier tipo de incidente o ataque externo, se encuentran también muy presentes en las inversiones que aprueba la alta dirección.

Caracterización de la demanda

- La mayoría de los CIOs de las organizaciones asocian la ciberseguridad a la salvaguarda de los contenidos y activos de información, lo que implica que los conceptos relacionados con las medidas de seguridad más extendidas entre las organizaciones sean las que protegen ante ataques de código maliciosos (*ransomware,* spam, gusanos informáticos, troyanos …).
- Las empresas españolas ignoran en gran medida el peligro de los nuevos ciberataques que se están originando en los últimos tiempos, como las filtraciones y fugas de datos, teniendo por tanto una percepción errónea por la cual creen no estar expuestas ante este tipo de vulnerabilidades y brechas de seguridad.
- Los clientes se ven cada vez más obligados a asegurar el cumplimiento de los nuevos marcos regulatorios que aplican a la compañía en materia de ciberseguridad, así como por formar y concienciar tanto a los empleados como a la alta dirección mediante campañas de simulación de *phishing*.
- Los beneficios que la mayoría de los clientes esperan obtener tras la implantación de soluciones y herramientas de ciberseguridad son la prevención del fraude tanto interno como externo, la protección de la marca y la mejora en el cumplimiento de las regulaciones.
- La decisión sobre la adopción de soluciones de ciberseguridad se encuentra en manos de la dirección de Ciberseguridad (CISO), aunque sigue promovida por la dirección TIC (CIO), debido a la evolución del rol TI en las compañías hacia perfiles más especializados en determinadas prácticas del negocio.
- La ciberseguridad es percibida cada vez más como una inversión rentable, aunque el coste de adopción de las medidas asociadas aún supone una barrera a la hora de aumentar la inversión en la materia.
- Las empresas se aproximan a la ciberseguridad en la medida en que su grado de vulnerabilidad aumenta o se ven expuestas a ciberataques inesperados, lo que implica que tomen medidas correspondientes para salvaguardar los activos de información de la compañía y que este tipo de ataques tengan el menor impacto posible en la continuidad del negocio.

Caracterización de los proveedores

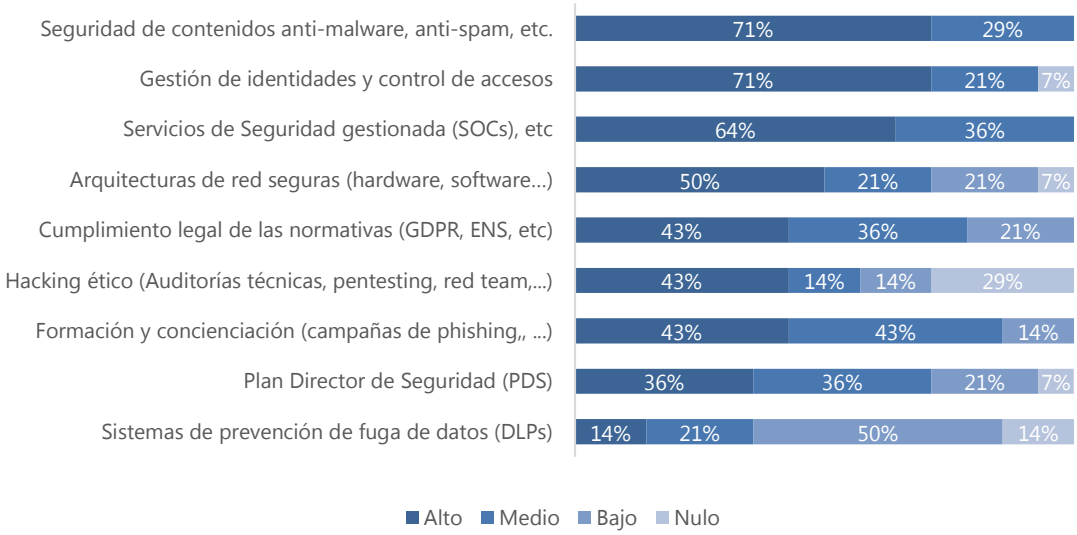
El sector de la seguridad tecnológica en España lo acaparan en la actualidad grandes actores del panorama de la ciberseguridad tanto nacionales como internaciones (fabricantes de hardware y software, firmas de servicios profesionales con áreas dedicadas a la gestión de riesgos tecnológicos, operadoras, outsourcers TIC). En términos generales, el mercado de la ciberseguridad se caracterizaría en forma de:

- Compañías específicamente dedicadas a la venta de productos y servicios relacionados con la seguridad tecnológica (software, hardware específico y/o servicios), con portfolios bien diversificados, cubriendo los cuatro ámbitos analizados.
- Fabricantes de soluciones de hardware y software especializados en plataformas tecnológicas para el equipamiento de redes y comunicaciones, tecnología Cloud e infraestructuras críticas que incorporan en sus portfolios dispositivos de seguridad.
- Firmas tecnológicas y de consultoría con divisiones dedicadas a la prestación de servicios de asesoría y cumplimiento de normativas, auditoría y revisiones de seguridad, integración e implantación de soluciones de protección o servicios gestionados, o bien outsourcers de gestión de infraestructuras.
- Operadores "Telco" que han desarrollado sus portfolios hacia las prestaciones avanzadas de red, y que ofrecen servicios evolucionados de SOC (Security Operations Center) y servicios de seguridad adaptadas a las tecnologías que proveen.
- Firmas de nicho especializadas en el ámbito de los servicios de asesoramiento y auditoría de seguridad (hacking ético, tests de penetración, gestión y priorización de vulnerabilidades), o de seguridad en el Cloud, con capacidades puntuales de implantación de ciertas herramientas.
- Firmas de nicho en ámbitos específicos (hardware/electrónica) relacionados con los controles de seguridad física.
- Distribuidores de hardware y software, incluido equipamiento de seguridad.

Caracterización de los servicios

En base a nuestras investigaciones y consultas al mercado acerca del grado de implantación de soluciones y servicios de ciberseguridad [1], obteníamos los siguientes resultados acorde a las respuestas proporcionadas por CIOs y responsables del área de TI de diversas compañías:

Figura 1. Implantación de soluciones y servicios de ciberseguridad



- ***Alto**: Grado de implantación completa, en modo explotación estable, extensivo al conjunto de sistemas e infraestructuras que son el alcance habitual de la solución.*
- ***Medio**: Grado de implantación parcial (en desarrollo o no sobre el conjunto de sistemas e infraestructuras que son el alcance habitual de la solución).*
- ***Bajo**: Implantación parcial, limitada a un entorno de poco impacto o en proceso de iniciación de proyecto.*

De acuerdo con estos datos, hemos comprobado que debido a los ataques tipo *ransomware* que tanta repercusión mediática tuvieron en 2017, la implantación de herramientas y soluciones que protegen a los activos de información frente a cualquier ataque de código malicioso (virus, gusanos, *ransomware*…), es a día de hoy el servicio que presenta un mayor grado de implantación en la mayoría de las empresas.

Además, para prevenir este tipo de intrusiones no autorizadas, las organizaciones consideran importante gestionar los accesos a sus infraestructuras y aplicaciones estableciendo los controles más avanzados y seguros del mercado, así como la implantación de soluciones IAM (Identity Access Management) que gestionan las identidades de los usuarios autorizados por la organización.

Este hecho da lugar a que las organizaciones quieran tener controlada la seguridad de la compañía mediante servicios de vigilancia y monitorización 24x7, ante posibles eventos anómalos que pudieran producirse, y de este modo dar una respuesta temprana ante incidentes que pudiesen comprometer la actividad de los sistemas de información. Por lo tanto, la contratación de este tipo de servicios de seguridad gestionada a través de centros de operaciones (SOC) también presenta un grado de adopción considerable.

[1] Ver informe Penteo: Market Trends 2018 – Tendencias de Ciberseguridad en España

En el ámbito del gobierno y cumplimiento de las normativas que regulan el sector, el 43% de las compañías aseguran cumplir con todos los estándares y mejores prácticas, y un 36% asegura que cumple con ello, pero no de forma total, por lo que queda clara la importancia que las compañías otorgan a este ámbito. A pesar de ello, la mayoría de las organizaciones aún tienen un largo recorrido por delante a la hora de adaptarse y no verse envueltas en sanciones y problemas legales en caso de ataques o brechas de seguridad que pudiesen comprometer loa activos de la organización, sobre todo datos e información de carácter sensible y, en consecuencia, datos de terceros, que son los más críticos en cuanto a que pueden acarrear sanciones y multas económicas en caso de no cumplir con las normativas que regulan su tratamiento.

Por otra parte, los servicios de hacking ético que mejoran las capacidades de las organizaciones para la detección de vulnerabilidades en los sistemas de la compañía, y que dan origen a la instalación de parcheados y actualizaciones en los propios sistemas, aparecen con una proyección alta a la hora de que este tipo de servicios sean contratados por las organizaciones.

Finalmente, cabe resaltar que los servicios de formación y concienciación del empleado son cada vez más demandados y son contratados a través de campañas de simulación de *phishing*. A pesar de que las organizaciones son cada vez más conscientes de los riesgos asociados a la ciberseguridad, la implantación de herramientas que previenen fugas de datos e información, como los DLP (Data Loss Prevention),sigue siendo aún incipiente, no siendo una de las prioridades de la alta dirección a la hora de destinar presupuesto a este tipo de soluciones, a pesar de los últimos casos de filtraciones y fuga de datos que han aparecido en los medios de comunicación a lo largo de estos últimos meses.

Siguientes pasos

Cabe esperar un aumento en la necesidad de disponer de una plantilla más concienciada y especializada en el ámbito de la ciberseguridad, debido al aumento en los presupuestos destinados a la defensa de los activos de información que está llevando a cabo la dirección general de las organizaciones, y que otorga un mayor peso a los roles y cargos de esta área dentro de las compañías. Ya no solo los CISOs y CSOs de las compañías adquieren importancia, sino que los propios empleados de esta área serán muy importantes de cara a asegurar el buen funcionamiento de la organización sin que se vea afectada por ataques no previstos que ponga en riesgo la confidencialidad, integridad y disponibilidad de los sistemas de información.

Debido a la transformación digital del mercado, uno de los principales retos que se le presentan a la ciberseguridad es la adaptación de las nuevas tecnologías como la IA, el IoT o el blockchain. Estas tendencias suponen la aparición de nuevos riesgos y vulnerabilidades asociadas a los dispositivos, softwares y sistemas que aún no tienen desplegadas las medidas de seguridad adecuadas para que las organizaciones no se vean afectadas por cualquier tipo de ciberataque, sobre todo aquellos de tipo *malware* o de denegación de servicio (DDoS), que pueden afectar a la disponibilidad de los dispositivos y sistemas que funcionan gracias a estas tecnologías.

Vendor Profile: Ackcent

Company Profile

- **Fundación**: 2001
- **Inicio de operaciones en España**: 2001
- **Propiedad:** Directivos Ackcent (68%) y directivos Capside (32%).
- **Ingresos último año fiscal**:

  España: 9 M €

  Mundo: 13 M €
- **Empleados:**

  España: ~98

  Mundo: ~ 115
- **Oficinas:**

  España: Barcelona y Madrid.

  Mundo: Londres y México. También han abierto una oficina satélite en San Francisco (USA).
- **Principales actividades de negocio:** servicios de diseño, implementación, operación, gestión y seguridad de sistemas de información en plataformas cloud y on premise, y servicios integrales de consultoría, auditorías, SOC, y ciberseguridad gestionada.
- **Descripción de la compañía:** Empresa especializada y dedicada exclusivamente a la prestación de servicios y soluciones de ciberseguridad. Su misión es ayudar a sus clientes a proteger sus activos digitales críticos. Sus servicios están diseñados para alinear la ciberseguridad y la estrategia de negocio, evaluar y gestionar las vulnerabilidades y los riesgos de los activos digitales, supervisar y administrar los servicios de seguridad en modalidad 24/7 y proteger sistemas y aplicaciones en un entorno cloud.

Service Profile

- **Inicio de prestación de servicios de ciberseguridad en España:** 2001
- **Plantilla dedicada a servicios de ciberseguridad:**

  España: ~42; Mundo: ~54
- **SOC:** Barcelona y México ~12 FTEs.
- **Principal cobertura de servicios de ciberseguridad**: Servicio OTS, servicios de formación y concienciación, protección de datos (DLP, etiquetado de la información), seguridad en las aplicaciones (entre IPS/IDS, S-SDLC), seguridad en redes e infraestructuras (WAFs, DMZ), gestión de activos, seguridad en el Cloud, seguridad gestionada (SOC), hacking ético, ciberinteligencia, respuesta a incidentes (SIEM), aprendizaje ante incidentes y mejora continua.
- **Servicios y soluciones propias:** VINT (Vulnerability Intelligence). Sistema inteligente en la gestión de vulnerabilidades de seguridad, que permite la automatización y alerta proactiva de riesgo asociado a vulnerabilidades visibles desde Internet.
- **Partners y alianzas principales:** Checkmarx, CISCO, Cylance, Darktrace, Imperva, Intsights, KnowBe4, Palo Alto, Proofpoint, Qualys, Sumo Logic.

- **Segmentación de clientes:** el perfil de cliente de Ackcent está muy diversificado, aunque predomina el de mediana empresa (volumen de facturación entre 100 y 500 M€), situado en Barcelona y Madrid, y del sector de Banca y Seguros, también presta muchos de sus servicios en los sectores de Retail, Industria y Servicios.

Servicios en su propuesta de valor

- **Auditorías de seguridad y pentest.** Realizan auditorías especializadas y revisiones de seguridad a la hora de evaluar los riesgos que una organización presenta en cuanto al diseño de sus arquitecturas, las vulnerabilidades en sus sistemas, los accesos no autorizados y las posibles modificaciones de información no autorizadas. También realizan pruebas de penetración para probar la seguridad de la organización mediante ejercicios de intrusión utilizando técnicas avanzadas de hacking ético.
- **Monitorización y gestión de la seguridad 24x7.** Su SOC integra la ciberinteligencia ante amenazas y la monitorización y gestión de alertas 24/7. En sus centros de España y México ofrecen servicios de prevención, monitorización, detección, análisis en tiempo real y respuesta ante incidentes. Sus servicios CERT/CSIRT proveen a sus clientes de las capacidades y competencias necesarias para gestionar incidentes de ciberseguridad.
- **Formación.** Ackcent dispone de un amplio catálogo de cursos, talleres y seminarios, tanto programados como impartidos en eventos especiales de empresa, en los que transmiten su experiencia en ciberseguridad. Estos cursos se imparten a usuarios finales, equipos técnicos y altos directivos. Además, colaboran con universidades como la Politécnica de Catalunya (UPC) en la coordinación de un Máster de ciberseguridad, y en programas de formación en muchas otras universidades y escuelas de negocio, como ESADE.
- **Oficina técnica de seguridad.** Sus servicios OTS ofrecen soporte al cliente en lo relativo a la estrategia y el desarrollo de normativas y políticas de seguridad, hasta su implantación. Facilita también servicios profesionales de consultoría, arquitectura e ingeniería de ciberseguridad en función de las necesidades de cada cliente.

Claras fortalezas

- Ackcent es un uno de los proveedores más especializados en el mercado de la ciberseguridad a nivel nacional e internacional destacando sobre todo en el ámbito de la vigilancia y la seguridad gestionada 24x7, que provee a sus clientes desde sus centros de operaciones en Barcelona y México. En su plan estratégico de expansión geográfica también destaca la apertura de una oficina satélite en San Francisco (EEUU) y el refuerzo de sus servicios en México y Reino Unido. Destaca su experiencia gracias al alto grado de expertise y conocimiento que poseen sus ingenieros y consultores. Están certificados en todas las normativas que aplican a la ciberseguridad tanto en temas de vigilancia, protección y gobierno (CERT, CSIRT, CEH, ISOs, etc), por lo que aseguran la excelencia de los servicios que prestan, especialmente en ámbitos como el Cloud, en los que ofrecen modelos de Security as a Service. Además, en su roadmap para los próximos años se incluye la ampliación del uso de tecnologías de nueva generación, como Inteligencia Artificial, la orquestación y automatización de la ciberseguridad, o los chatbots, para mejorar la seguridad en las organizaciones en las que prestan sus servicios.
- Este proveedor ofrece soluciones y herramientas de seguridad innovadoras como la que incluye en su portafolio de doble factor de autenticación y que desarrolla en colaboración con Duo Security (recientemente adquirido por Cisco), o la solución para proteger el endpoint del ransomware o cualquier otro tipo de amenaza, y que desarrolla en este caso con Cylance. También destacan sus programas de formación y concienciación o sus campañas de phishing, y que las imparten y llevan a cabo sus empleados expertos en la materia.
- Sus clientes muestran una gran satisfacción con el servicio que les proveen, renovando en un porcentaje muy elevado el contrato. Destacan su cercanía y trato personal, así como la flexibilidad a la hora de

adaptarse a necesidades y cambios que puedan surgir durante la prestación de servicios. También valoran el alto grado de conocimiento de sus equipos debido a la especialización en la materia que posee Ackcent.

A evaluar su evolución en…

- Son expertos en servicios de vigilancia 24x7 y monitorización. También están especializados en las soluciones de protección específicas que proveen junto a sus socios tecnológicos. Sin embargo, no cubren al 100% otros ámbitos como los de estrategia de gobierno y cumplimiento, a pesar de que también realizan proyectos de ajuste a normativas que aplican a la ciberseguridad o servicios de contingencia y continuidad, cómo, por ejemplo, planes de recuperación ante desastres (DRaaS), por su propia estrategia de especialización.
- Proveen sus servicios en grandes clientes a nivel nacional en sectores como Banca y Seguros, aunque no son reconocidos por otros competidores que operan a nivel de multinacionales. Han mejorado su branding, sobre todo a base de las buenas opiniones de sus referencias, que les consideran altamente solventes y especializados, pero aún no se asemejan a las grandes compañías de servicios debido al número limitado de empleados en sus equipos, lo que supone que estemos hablando de uno de los mejores proveedores especializados del mercado.
- Su oferta formativa comprende un amplio catálogo de cursos y campañas de concienciación, colaborando además con universidades en cuanto a su impartición. Sin embargo, no destinan muchos FTEs a este servicio, con lo que podrían potenciar aún más su imagen de marca a través de ellos. Ackcent está cada vez más presente en el mercado de la ciberseguridad tanto a nivel nacional como internacional, lo que implica que habrá que estar atentos a su evolución, ya que pocos proveedores especializados tienen una proyección tan destacada debido a su alto grado de conocimiento.

Valoración

Capacidad	Necesita mejorar	Correcta	Positiva	Líder
Prestaciones	Necesita mejorar	Correcta	Positiva	Líder
Proyección	Incierta	Estable	Alta	Muy Alta
Calidad	Mejorable	Correcta	Notable	Excelente

Sobre Penteo

Penteo es el analista TIC independiente que lidera la mayor Comunidad de Conocimiento TIC de España, y ofrece un servicio especialmente diseñado para Directivos con influencia o responsabilidad en las decisiones TIC-Negocio, ayudándoles a garantizar el acierto de sus decisiones, compartiendo conocimiento, asesorándoles y facilitándoles hacer networking. Y para proveedores TI, Penteo aporta información del mercado sobre tendencias y posicionamientos, y proporciona apoyo experto con el que maximizar el éxito en sus estrategias.

Desde hace más de 20 años damos servicio a más de 200 compañías e instituciones de primer nivel del mercado español. Un servicio con el que minimizar riesgo, tiempo y coste, y extraer de las TICS y las Tecnologías Digitales el máximo valor para el negocio.

Penteo
Analista TIC

Tu asesor TIC de **confianza**

que te proporciona el **conocimiento** y el **apoyo experto e independiente**