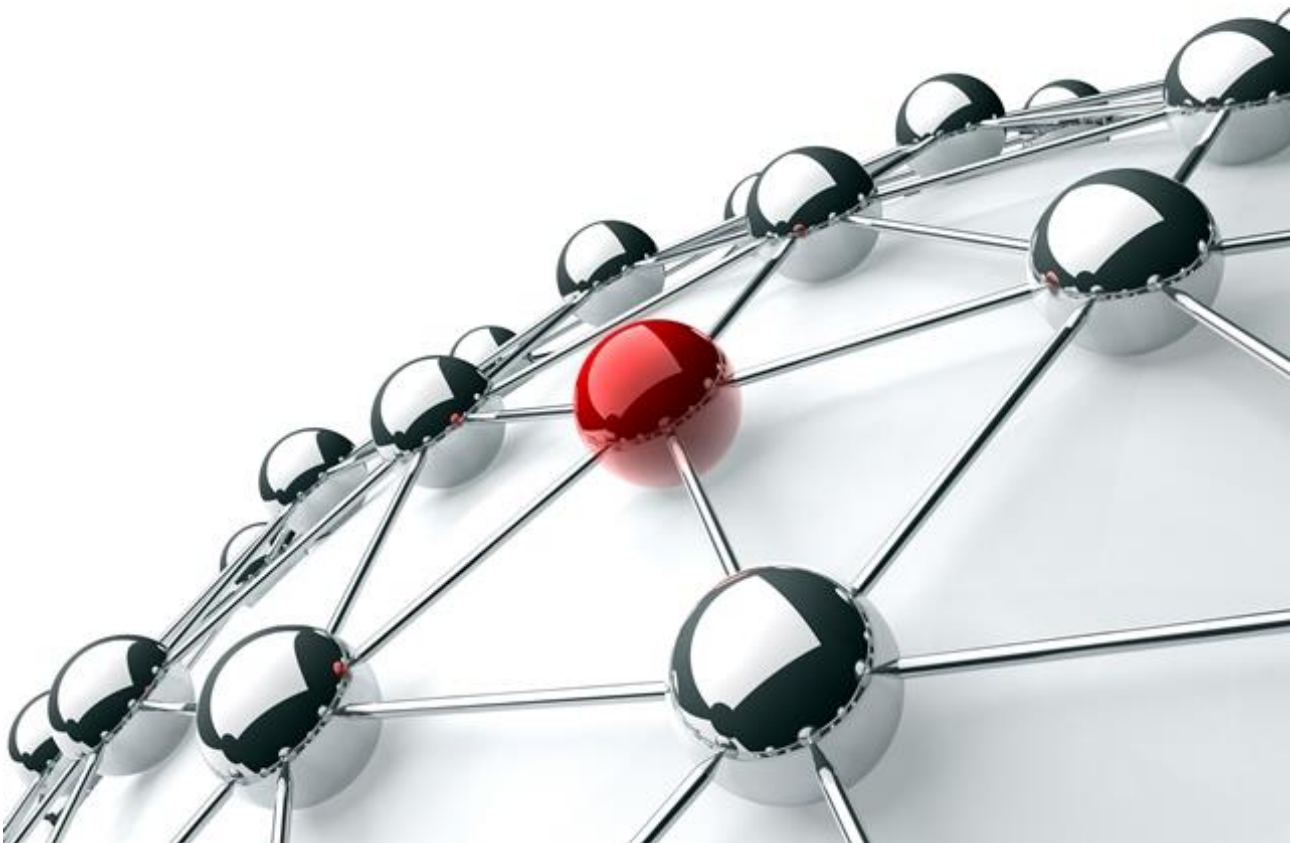
Penteo
Analista TIC

Universo Penteo

Proveedores de Servicios de Ciberseguridad

Departamento de Análisis Penteo | Junio del 2017

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



Índice de contenidos

Introducción

La ciberseguridad ha pasado, de ser una cuestión restringida a los especialistas en la materia, a estar en la mesa de los comités de dirección como elemento clave para salvaguardar el negocio. El 57% de las organizaciones se considera medianamente vulnerable a ciberataques sobre sus activos de información y un 14% considera que su grado de exposición es alto[1].

Aunque el concepto de ciberseguridad abarca varios ámbitos, los más comunes son los relacionados con seguridad perimetral, de contenidos (detección de intrusiones/software malicioso) y control de accesos, que aparecen implantados en casi el 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 información o la protección de entornos móviles, donde un 17% de los CIOs reconoce un conocimiento bajo[1].

La perspectiva de evolución presupuestaria para la ciberseguridad estará marcada por un crecimiento del 150% de la inversión neta en el 2017 respecto al año 2016 [2]. 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. Nadie duda hoy de que no puede hablarse de un negocio sostenible si no está convenientemente salvaguardado de las amenazas inherentes a una realidad marcada por la hiperconectividad (expresión de su transformación digital), la ya industrialización de la ciberdelincuencia y, en general, de toda clase de actividades ilícitas sobre los activos de información.

Sin ir más lejos, el pasado 12 de mayo se vivió un viernes negro a nivel mundial en lo que a ciberseguridad se refiere. El más que conocido ya malware de tipo ramsomware que afectó a miles de compañías de todo el mundo ha dado mucho que hablar y, sobre todo, ha despertado en todas las organizaciones interés por la gran importancia que tiene la ciberseguridad en ESTE mundo cada vez más digital.

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

[2] Ver informe Penteo: Strategic Report - IT Spending 2017.

Análisis del ataque WannaCry

Hemos tenido la oportunidad de hablar directamente con los proveedores que han sido posicionados en el Universo y conocer de primera mano cómo vivieron el ataque y cómo ha reaccionado el mercado español tras este suceso. Estas son las principales conclusiones recogidas:

- El ciberataque ha supuesto efectos positivos para la ciberseguridad. Por un lado, aquellas organizaciones que no se han sido afectadas han visto el valor de contar con un partner de ciberseguridad en el que apoyarse en estas situaciones. Por otro lado, las que sí han sido afectadas se han dado cuenta de la necesidad de invertir más en proyectos relacionados en materias de ciberseguridad.
- En general, el ciberataque ha conseguido concienciar a los directivos de la importancia de la ciberseguridad. Todos los proveedores coinciden en que sus clientes han mostrado mayor interés y previsión en ampliar el presupuesto y alcance en sus servicios de ciberseguridad.
- El rol del CISO también ha ganado en importancia. En aquellas organizaciones que no contaban con este rol se plantean adoptarlo. Y, en aquellas en las que ya se disponía de su figura, se le ha involucrado a nivel de comité de dirección en las últimas semanas.
- Hay determinados sectores, como el industrial, que disponen de infraestructuras críticas, y en los que las actualizaciones de los sistemas no son tan triviales y están continuamente expuestos a las vulnerabilidades identificadas en los sistemas operativos.
- WannaCry ha tenido una repercusión muy notable, porque ha afectado a usuarios finales en muchos países, y los medios de comunicación se han hecho eco rápidamente del ataque. No obstante, existen ataques continuos día a día, mucho más dañinos que WannaCry, y de los que los medios no se hacen eco. Pero que resultan más peligrosos y generan más pérdidas a las empresas.
- Una empresa nunca estará 100% segura, ya que ha habido ataques en el pasado, sigue habiendo a día de hoy, y se seguirán produciendo en un futuro. Por ello, es muy importante adoptar medidas de gestión de crisis y protocolos de actuación para cuando sucedan estos ciberataques, así como tener siempre copias de seguridad de los principales activos y datos, tanto a nivel de compañía como a nivel de usuario.
- Se pueden considerar diferentes formas preventivas, pero tal vez las más importante de todas ellas seas, para estos casos: (1) aplicar los parches de seguridad que hay disponibles, (2) emplear las últimas firmas de los antivirus y (3) disponer de copias de seguridad perfectamente actualizadas que permitan la continuidad en el negocio.
- Telefónica fue la primera compañía en España en comunicar que su red y sistemas habían sido infectados y por ello los medios se hicieron rápidamente eco y aparecieron en todas las portadas. No obstante, se ha demostrado con posterioridad que también ha sido una de las compañías que más han ayudado a acotar y minimizar el impacto que ha tenido el ataque tanto a nivel nacional, según comenta INCIBE en nota de prensa, como a nivel internacional según comenta el Centro Europeo de Ciberdelincuencia en una entrevista realizada a Europol. No obstante, y referidos concretamente al posicionamiento en este Universo, el ciberataque no afecta a Telefónica en su posición en el mercado de la ciberseguridad en España, ni a sus capacidades ni prestaciones para prestar los servicios a sus clientes.
- WannaCry ha puesto sobre la mesa que la prevención sea uno de los factores más importantes en la definición de una estrategia de ciberseguridad en las compañías.

Definición del Universo

Definición del mercado

Por **ciberseguridad** entendemos el conjunto de disciplinas contenidas en la seguridad informática que se dedican al análisis de riesgos y amenazas, y a la protección de activos de información habitualmente expuestos a su acceso o publicación en Internet.

Los servicios asociados se materializan en una oferta de implantación y administración continua asociada a la gestión de identidades y acceso a recursos, seguridad de aplicaciones, seguridad de datos, seguridad de dispositivo final, seguridad de redes, seguridad en cloud, gestión y análisis del riesgo, cumplimiento legal y normativo, y gobierno de la seguridad.

Así mismo, los **proveedores de servicios de ciberseguridad** se definen como aquellos que proporcionan servicios externalizados de seguridad informática con un enfoque integral y multidisciplinar de la seguridad corporativa, abarcando uno o varios de los grandes ámbitos listados anteriormente, tanto desde el punto de vista tecnológico como normativo:

- Tecnológico y servicios asociados:
  - Servicios gestionados de ciberseguridad, implantación de productos de ciberseguridad, arquitectura y consultoría técnica: perimetral, SIEM (Security information and event management), IDS/IPS (Intrusion Detection / Prevention System), gestión de identidades, prevención de fuga de información, firma electrónica, seguridad en el cloud y SecaaS (Security as a Service), seguridad en torno al dispositivo móvil, etc.
  - Servicio de SOC (Security Operation Center)
  - Prevención, detección y gestión de las amenazas de ciberseguridad: Red Team, hacking ético, desarrollo seguro de aplicaciones, análisis de malware y forénsic digital, prevención y detección del fraude, etc.
  - Servicios de protección de marca.
  - Servicios de formación.

- Cumplimiento legal y normativo (auditoría, adecuación y cumplimiento):
  - LOPD/RLOPD.
  - ENS (Esquema Nacional de Seguridad).
  - Gestión de Continuidad de Negocio, ISO27001 (Sistema de gestión de la seguridad de la información) e ISO27002 (Planes Directores de Seguridad).
  - LSSICE (Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico).
  - PCI-DSS (Payment Card Industry Data Security Standard).
  - COBIT 5 (Control Objectives for Information and related Technology), etc.

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 en relación 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 o por verse sometidas a alguna normativa que exija auditoría y cumplimiento, por poner algunos ejemplos.

Criterios de evaluación

Para efectuar la evaluación[3] se ha analizado el posicionamiento relativo de los actores seleccionados en función de dos dimensiones, caracterizadas de acuerdo a 10 factores formados por 33 indicadores, que se desglosan en más de 105 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.

[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.

- **Capacidad**: Valorar los medios, recursos y alcance necesarios de los que dispone el proveedor para cubrir las necesidades, así como su visión estratégica en relación con este tipo de servicios.
  - **Solidez y viabilidad**: Trayectoria en el mercado de la ciberseguridad, peso de la línea de negocio de ciberseguridad dentro de la compañía, equipo involucrado y estrategia de gestión del talento en relación con el servicio.
  - **Capacidades de entrega de los servicios**: Presencia en España y resto del mundo. Centros de excelencia o de soporte especializados y número de empleados dedicados.
  - **Penetración en el mercado**: Trayectoria y presencia actual en el mercado de servicios de ciberseguridad, cartera de clientes de la solución y servicios, calidad de referencias y segmentación de la cartera de clientes. Identificación del proveedor con la línea de ciberseguridad (Top of Mind).
  - **Go to market**: Visión y propuesta de valor de la compañía en relación con la ciberseguridad. Claridad de la oferta y portafolio comercial. Facilidades de adquisición y contratación.
  - **Estrategia**: Inversión en innovación. Roadmap de solución / servicio previsto. Sectorización o soluciones verticales. Estrategia de alianzas.

- **Prestaciones**: Valorar el nivel de cobertura y alcance de los servicios de ciberseguridad ofrecidos y, de forma relevante, la satisfacción de los clientes que los están utilizando.
  - **Cobertura**: Tipos de servicios ofrecidos, como SOC, cumplimiento legal y normativo, seguridad gestionada y proyectos tecnológicos asociados, prevención, detección y gestión de las amenazas de seguridad, protección de marca, formación en seguridad y productos propios.
  - **Alcance del delivery**: Teniendo en cuenta los ámbitos que componen el espectro de su servicio (cobertura), para cada uno de ellos valorar el tipo y la profundidad con la que se abordan.
  - **Experiencia**: Referencias por sector, alcance técnico, modelo de entrega, servicios adicionales contratados, nivel de transformación realizado y gestión de terceros proveedores.
  - **Calidad del delivery**: Procedimientos y metodologías, prácticas preconfiguradas y certificadas. Satisfacción de las empresas cliente en relación con el conocimiento y expertise técnico y sectorial del proveedor.
  - **Tipología del delivery**: Referencias por sector, en función de alcance técnico y complejidad del delivery.

Mapa del Universo

Estrellas

Proveedores generalistas sólidos destacados. Estos actores cuentan con ventaja en solidez, presencia y una alta capacidad de prestación de servicios, sin olvidar sus inversiones continuas en innovación, adquisición de otras compañías, acuerdos con terceros proveedores de tecnología y penetración en el mercado nacional. Son líderes de mercado.

Soles

Proveedores generalistas sólidos. De igual modo, cuentan con la ventaja de la solidez, presencia y una alta capacidad de prestación de servicios, sin olvidar sus inversiones continuas en innovación, adquisición de otras compañías, acuerdos con terceros proveedores de tecnología y penetración en el mercado nacional. No son líderes en el mercado.

Planetas

Proveedores generalistas emergentes. Actores que tienen importantes capacidades como proveedores generalistas, pero unos servicios menos desarrollados. Están menos presentes en el mercado, ya que han comenzado la línea de negocio recientemente.

Satélites

Proveedores especialistas sólidos. Estos actores tienen importantes prestaciones al ser especialistas en el ámbito analizado, y cuentan con una trayectoria contrastada en la prestación de estos servicios.

Cometas

Proveedores especialistas emergentes. Actores que tienen importantes prestaciones al ser especialistas en el ámbito analizado, pero cuentan con una trayectoria más reciente en la prestación de estos servicios.

Posicionamiento de los diversos actores

Accenture es uno de los proveedores con mayor antigüedad en el mercado de ciberseguridad, y dispone de un elevado número de recursos y capacidades para cubrir las necesidades de sus clientes. Su penetración en el mercado es alta, y mediante la reciente adquisición de compañías está apostando por aspectos más innovadores en el ámbito de ciberseguridad.

Ackcent es una compañía especialista en ciberseguridad. Dispone de personal con un alto expertise a nivel técnico, sus clientes muestran una alta satisfacción por sus servicios, y en tan solo 3 años ha experimentado un importante crecimiento en su cartera y nivel de ingresos. Es un proveedor nuevo, aunque consolidado, al recoger la experiencia de Capside, que ha conseguido hacerse un hueco entre los más generalistas.

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 referencias en las que ya presta estos servicios. Disponen de una suite de productos propios bastante amplia y tienen en roadmap varias líneas de trabajo en aspectos más innovadores.

Capgemini comenzó a ofrecer servicios de ciberseguridad en el 2015 y ya ha ganado varias referencias de notable relevancia, con lo que ha conseguido hacerse un hueco en el mercado. Dispone de buenas capacidades y prestaciones, pero su aspecto diferencial es la alta calidad con la que acomete sus proyectos. Está realizando una importante apuesta en esta línea y prueba de ello es su alto crecimiento experimentado en estos 2 años.

DXC nace de la fusión entre HPE y CSC finalizada en marzo del 2017, que les ha aportado claras sinergias en sus capacidades para prestar servicios en ciberseguridad. Es capaz de ofrecer servicios end-to-end y el grado de satisfacción de sus clientes es elevado. Tienen capacidades contrastadas para dar soporte a sus clientes a nivel estratégico en ciberseguridad.

Seidor dispone de una estrategia de ciberseguridad clara y presenta una buena trayectoria con un crecimiento constante en esta línea de negocio. Dispone de un gran número de clientes en el ámbito nacional con un amplio abanico en todos los segmentos. Además, sus clientes valoran su grado de personalización y capacidad para adaptarse a las necesidades de su negocio.

Telefónica se sitúa como líder destacado en prestaciones y capacidades. Tiene un portfolio muy completo, maduro y evolucionado, así como la capacidad para ofrecer servicios end-to-end. También un gran volumen de negocio en el mercado nacional, y dispone de un elevado número de empleados dedicados a ciberseguridad, además de una dilatada experiencia en esta línea de negocio.

Puntos clave del mercado

Como comentábamos, este mercado ha pasado de ser una cuestión restringida a especialistas en la materia para estar ahora 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 el seno de las empresas, en las líneas de estrategia, organización o relevancia de los roles que deben gestionarla y supervisarla, tiene aún camino por recorrer.

En cuanto a los servicios más adquiridos actualmente por la empresa española, destacan aquellos relacionados con la seguridad del perímetro de las redes y la intrusión mediante contenidos maliciosos. Tal y como se pudo ver recientemente tras el ciberataque del pasado 12 de mayo, es un mercado que aún tiene un largo camino por recorrer para poder estar realmente blindados a problemáticas de esta índole, y debemos ser conscientes de que nunca se podrá estar 100% protegido ante estos ataques. La autopercepción de las empresas es que son vulnerables, tal y como veremos a continuación al caracterizar la demanda. Esta percepción se confirma con la prioridad que muestran en inversión en ámbitos relacionados con servicios gestionados de ciberseguridad, como respuesta a la creciente complejidad tecnológica y a la necesidad de ofrecer respuestas tempranas a incidentes en medio de la diversidad de sistemas y plataformas objetivo de ataques.

Caracterización de la demanda

Uno de los principales retos que deben encarar las empresas es el desconocimiento, en muchos casos, de las infraestructuras y topologías de red de las que se dispone. Y, particularmente, de los puntos de conexión con el exterior, ya sea mediante puertas de red o mediante la gran diversidad de dispositivos que se ponen en manos de los usuarios. La gestión de los activos se ha convertido en el caballo de batalla, por tanto, como parte de una política coherente de seguridad. Además de ser extraordinariamente relevante para asegurar el compliance relacionado con los servicios tecnológicos y, en esa línea, asegurar no solamente la protección de los mismos, sino facilitar su visibilidad dentro de un mapa gráfico de la seguridad.

La mayoría de las organizaciones se considera medianamente vulnerable a ciberataques sobre sus activos de información claves y un 14% considera que su grado de exposición es alto. Esta percepción no ha variado, en esencia, con respecto a la que hemos venido recogiendo entre los CIOs españoles en los últimos años, a pesar de la evolución que ha seguido la tecnología.

De hecho, un 60% de estos CIOs teme sufrir en los próximos doce meses un incidente relevante sobre sus sistemas de información. Y un 55% reconoce que sus organizaciones no están bien preparadas para responder a las amenazas actuales sobre los dispositivos móviles en manos de sus empleados. Y es que, la práctica totalidad de los directivos IT o responsables de ciberseguridad, reconocen que sus empresas, en realidad, no estarían preparadas en caso de recibir ataques enfocados y altamente especializados como seguramente y, desafortunadamente, haya podido comprobarse hace escasas semanas.

Caracterización de los proveedores

El sector de la seguridad tecnológica en España se encuentra en la actualidad muy atomizado y polarizado entre los grandes jugadores internacionales (fabricantes de hardware y software, firmas de servicios profesionales con áreas dedicadas a la gestión de riesgos tecnológicos, operadoras, outsourcers TIC), con presencia en nuestro país, y compañías con carácter local y relativamente escaso despliegue a nivel nacional. En términos generales, y enunciándolos de manera somera, este sector se caracterizaría por:

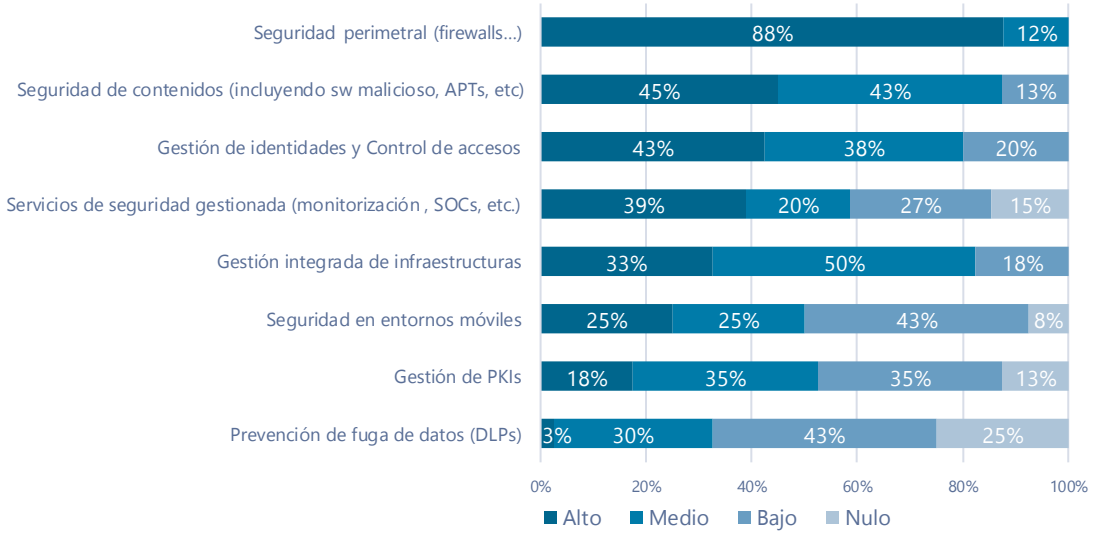
- Compañías específicamente dedicadas a la venta de productos y servicios relacionados con la seguridad tecnológica (software, hardware específico y/o servicios), con portfolios bien diversificados, bien específicamente orientados a alguno de los tres ámbitos.

- Fabricantes de hardware y software especializados en plataformas tecnológicas para el equipamiento de redes y comunicaciones, que incorporan en sus portfolios dispositivos appliance de seguridad.
- Firmas tecnológicas y de consultoría con divisiones dedicadas a la prestación de servicios de asesoría, auditoría, integración de soluciones o servicios gestionados, o bien outsourcers de gestión de infraestructuras.
- Operadores de telecomunicaciones que han desarrollados sus portfolios hacia las prestaciones avanzadas de red, y que ofrecen servicios evolucionados de SOC (Security Operations Center).
- Firmas de nicho en el ámbito de los servicios de asesoramiento y auditoria de seguridad (hacking ético, tests de penetración), con capacidades puntuales de implantación de ciertas herramientas.
- Firmas de nicho en ámbitos específicos (hardware/electrónica) relacionados con la seguridad física.
- Distribuidores de hardware y software, incluido equipamiento de seguridad

Caracterización de los servicios

Realizando barómetros en nuestras investigaciones respecto del grado de implantación actual de diversas tipologías de soluciones y servicios en el ámbito de la ciberseguridad, obteníamos los resultados de la siguiente figura:

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 nuestros datos de mercado, los elementos de seguridad perimetral y de contenidos (detección de intrusiones/software malicioso) aparecen implantados en mayor o menor grado en el 90% de los casos. Ninguna de las organizaciones consultadas señala no disponer de algún elemento relacionado con la seguridad perimetral en sus infraestructuras.

Por otro lado, las organizaciones consideran importante gestionar la complejidad en la administración de los diferentes entornos de seguridad en un escenario de datacenter y multifabricante, que es lo que da a entender el hecho de que en más del 80% de los casos se disponga de soluciones de gestión integrada de infraestructuras.

Esto es congruente con el hecho de que la complejidad de las arquitecturas tecnológicas diversas es una de las principales barreras a la hora de tratar de adoptar una postura holística y eficiente en la gestión de la seguridad. La elevada difusión de los servicios de seguridad gestionada entre las empresas viene a ser una respuesta, vía externalización, a la gestión de esta complejidad teniendo en cuenta la necesidad de una respuesta temprana a ataques con orígenes y objetivos diversos.

En el ámbito de la salvaguardia de entornos móviles, la situación es bastante diferente. Si bien este apartado es el que más evolución y crecimiento está registrando, el 43% de las empresas han realizado implantaciones solamente puntuales de este tipo de soluciones (habitualmente, centradas en porcentajes pequeños de sus parques de dispositivos móviles, o bien de forma no integrada con el resto de elementos de seguridad).

Por otra parte, la implantación de sistemas para la prevención de la fuga de información (DLP) sigue siendo puntual, sobre todo centrada en el endpoint y restringida, únicamente, en la mayoría de los casos, a puestos de trabajo y medios de almacenamiento considerados a priori de alta sensibilidad. No se puede hablar en absoluto, por tanto, de un uso generalizado de este tipo de soluciones.

Finalmente, con respecto al modelo de implantación de las soluciones de ciberseguridad, hay que destacar que sigue avanzando el modelo cloud como base para la provisión de ciertos servicios, tal como sucede con cualquier ámbito de las TIC. Respecto de las soluciones de seguridad, hay que destacar que los modelos de pago por uso / suscripción de sistemas de protección no es reciente, pero lo es, relativamente, la implantación de sistemas de seguridad en la nube (por ejemplo, brokers de seguridad de infraestructuras cloud o firewalls de nueva generación basados en cloud).

Siguientes pasos

Cabe esperar que los nuevos roles relacionados con la digitalización (CDOs, CISOs, COOS, etc.) contribuyan a dotar de más contenido y organización para asegurar la protección de activos y procesos. Las organizaciones no pueden permitirse continuar con responsables de seguridad enterrados en áreas técnicas del departamento de sistemas, sin ninguna visibilidad, exponiendo ámbitos del negocio a peligros provenientes del exterior.

La evolución de la organización de la seguridad (con especial atención a la existencia de marcos de referencia únicos, adheridos a las mejores prácticas del mercado) va a determinar la capacidad de las organizaciones para protegerse de las amenazas actuales y, sobre todo, de las que están en ciernes.

Vendor Profile: Ackcent

Company Profile

- Fundación: 2014 (como Ackcent).
- Fecha de inicio de prestación de servicios en España: 2001 (como Capside).
- Oficinas en España: Barcelona y Madrid.
- Empleados: 95, de los cuales 87 en España.
- Propiedad (principales accionistas): Directivos Ackcent (60%), Capside (40%).
- Ingresos último año fiscal:
  - España: 5,9 M €
  - Global: 8,25 M €
- 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 seguridad gestionada en ciberseguridad.
- Descripción de la compañía: Empresa especializada en servicios de ciberseguridad para la protección de activos digitales críticos estableciendo relaciones de partnership con sus clientes para el soporte y acompañamiento en la gestión de la seguridad de la información, con el objetivo de controlar y mitigar riesgos, vulnerabilidades y amenazas, y así lograr una mayor resiliencia.

Service Profile

- Inicio de prestación de servicios en ciberseguridad en España: 2001 (como Capside).
- Plantilla dedicada a servicios de ciberseguridad en España: 35 empleados.
- SOC: 10 FTEs con más de 50 clientes.
- Principal cobertura de servicios de ciberseguridad: SOC, servicios de compliance, asesoría técnico-legal, servicios de ciberseguridad para dispositivos móviles, servicios de seguridad gestionada: Firewall, Proxy, WAF, RASP, AV, email security gateway, DDos, SIEM, IPS, IDS, CASB, así como servicios de seguridad en el cloud y SecaaS, arquitectura y consultoría técnica y gestión de amenazas.
- 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: Capside, Microsoft, AWS, Checkmarx, Cylance, KnowBe4, Proofpoint.
- Segmentación de la cartera de clientes de servicios de ciberseguridad:
  - Pequeña empresa (< 100 M €/año): 6%
  - Mediana empresa (100 – 500 M €/año): 57%
  - Gran empresa (500 – 1.000 M €/año): 35%
  - Corporación (>1.000M €/año): 2%

Claras fortalezas

- Ackcent es un proveedor con foco en mediana y gran empresa, con capacidad para dar un servicio casi integral y cross en todos los sectores, y respaldado para dar aquellos servicios no cubiertos por su oferta mediante terceros. Además, cuenta con un alto expertise a nivel técnico en servicios de prevención, detección y gestión de amenazas y vulnerabilidades, y capacidad para automatizar informes mediante sus herramientas. Aunque la empresa se fundó en 2014 como Ackcent, su experiencia y grado de madurez son altos, con un equipo consolidado que trabajaba en la empresa matriz (Capside) desde 2001. También tiene

referencias en clientes de rango corporativo, en el sector Banca&Seguros, donde realiza servicios especializados de auditorías de seguridad y S-SDLC.

- El crecimiento de la organización (en volumen de negocio, empleados, etc.) estos últimos años es muy positivo, y ha iniciado además un proceso de expansión internacional el pasado año con una elevada inversión en Reino Unido. Cuentan con un centro de competencia especializado en soluciones de seguridad de Microsoft, además de presencia también en México, donde disponen de otro centro de operaciones propio para potenciar el servicio SOC 24x7. En cuanto a sus herramientas, están invirtiendo en plataformas como VINT (Vulnerability Intelligence) para la automatización e inteligencia en la gestión de alertas de vulnerabilidades críticas, y RISK (Risk Intelligence Security Knowledge), una plataforma SaaS para ofrecer indicadores de riesgo de ciberseguridad de activos digitales críticos. Destaca también su amplio catálogo en formación a todos los niveles, para empleados tanto de perfil técnico como directivo, incluyendo seminarios, workshops y cursos en las oficinas del cliente. Además, coordinan el master de ciberseguridad en la UPC y diversos cursos de formación a directivos en ESADE.
- Sus clientes muestran una alta satisfacción por los servicios ofrecidos, valorando su alta flexibilidad y capacidad para adaptarse a los proyectos. Aprecian muy positivamente a su equipo, no solo a nivel técnico, sino también a nivel personal. Los clientes contactados no piensan en cambiar de proveedor, sino que incluso han renovado los servicios ampliando el alcance y la duración de los contratos.

A evaluar su evolución en…

- En prestaciones tienen experiencia en servicios SOC y en servicios relacionados con la prevención, detección, y gestión de amenazas de seguridad. Además, con muchas y variadas referencias contrastadas. Pero les falta cubrir servicios relacionados con protección de marca y algunos ámbitos de cumplimiento legal y normativo. Tienen mayor experiencia en servicios operativos y continuados, pero menor en aspectos relacionados con consultoría de gobierno y estrategia.
- A pesar de tener un número elevado de clientes en España, no son aún reconocidos por el mercado ni por sus competidores. Han de poner esfuerzo en impulsar su marca y mejorar su branding. Han incorporado al equipo un director de marketing procedente del sector media y habrá que ver su evolución en este aspecto.
- Su posición en el universo es bastante buena, siendo el único proveedor de nicho especializado en seguridad entre los analizados. Pero sus capacidades en volumen de negocio, número y distribución de empleados están, lógicamente, por debajo de la media, si lo comparamos con los proveedores más generalistas. Habrá que ver la evolución de Ackcent, porque pocos proveedores de nicho puros nacionales pueden presumir de dar servicios y tener presencia fuera de España, además en mercados más maduros como el británico.

Valoración Ackcent

Capacidad	Necesita Mejorar	**Correcta**	Positiva	Líder
Prestaciones	Necesita Mejorar	Correcta	**Positiva**	Líder
Proyección	Incierta	Estable	**Prometedora**	Líder
Valoración	★★★☆☆		 Satélite	

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**