

Penteco Cybersecurity Report 2025

Overview Universo integradores
de servicios de Ciberseguridad

Enero 2025

PENTEO

Índice

1.	<u>Alcance del Universo</u>	3
2.	<u>En 1 minuto..</u>	4
3.	<u>Mapa del Universo</u>	6
4.	<u>Vendor Profile</u>	7
5.	<u>Sobre el Universo Penteo</u>	12

Alcance del Universo

Penteo define a los proveedores de servicios de Ciberseguridad como aquellos que son capaces de proporcionar servicios externalizados de ciberseguridad 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 activos, todo ello desde un punto de vista tanto tecnológico como normativo.

Ámbitos analizados como proveedores de servicios de Ciberseguridad:

_ Gobierno y Estrategia de la Ciberseguridad.

- Assessments y estrategia de Ciberseguridad. Hoja de ruta.
- Servicio de oficina técnica 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).

_ Protección y seguridad de los activos.

- Gestión de identidades, control de accesos, gestión de permisos y autorizaciones (privilegios de acceso, autenticación...).
- Gestión de activos: protección de los recursos físicos y digitales que componen el ecosistema de las empresas mediante controles y monitorización.
- Protección de la información, prevención de fuga de información mediante herramientas DLP, cifrado de la información. Seguridad en aplicaciones y Redes. Seguridad en Cloud. Ciberseguridad OT. Ciberseguridad sobre tecnologías emergentes.

_ 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.
- Protección de la marca mediante prevención del fraude y de suplantación de identidad.

_ Servicios de resiliencia

- Contingencia y continuidad de negocio.
- Respuesta y aprendizaje ante incidentes. Ciberseguridad en tecnologías emergentes.
- Uso de Inteligencia artificial para la evaluación de riesgos, amenazas y otras propuestas que fortalezcan la seguridad de las empresas

Propiedad Penteo.

Esta publicación no puede ser reproducida o distribuida.

En 1 minuto...

La ciberseguridad continúa consolidándose como una prioridad estratégica en las organizaciones, pasando de ser una preocupación técnica a un pilar fundamental para la protección de activos digitales y la continuidad del negocio.

Evolución de la madurez y el conocimiento:

Mayor sofisticación: Los CIOs y CISOs demuestran un conocimiento cada vez más profundo de conceptos avanzados como Zero Trust, SASE, Cybersecurity Mesh y seguridad en entornos multi-cloud.

Enfoque proactivo: Se observa una transición hacia una postura de seguridad proactiva, anticipando amenazas y adoptando medidas preventivas.

Integración con el negocio: La ciberseguridad se integra cada vez más en los procesos de negocio, impulsando una cultura de seguridad a todos los niveles de la organización. La aparición de normativas como NIS2 obliga a los Comités de Dirección a estar formados y concienciados en materia de ciberseguridad.

Inversión y presupuestos:

Aumento sostenido: La inversión en ciberseguridad sigue creciendo a un ritmo acelerado, con un enfoque en soluciones tecnológicas avanzadas y servicios gestionados.

Justificación de la inversión: Las empresas buscan cada vez más justificar la inversión en ciberseguridad demostrando un retorno tangible en términos de reducción de riesgos y mejora de la reputación.

Priorización de la nube: La nube sigue siendo una plataforma estratégica para la implementación de soluciones de seguridad, impulsada por la agilidad y escalabilidad que ofrece.

Tendencias emergentes:

Seguridad en la nube: La seguridad en entornos multi-cloud y híbridos se convierte en una prioridad, con un enfoque en la protección de datos en tránsito y en reposo.

IA y aprendizaje automático: La inteligencia artificial se utiliza para detectar amenazas de manera más eficiente, automatizar procesos de seguridad y mejorar la respuesta a incidentes.

Ciberseguridad de dispositivos IoT: Con el crecimiento exponencial de dispositivos IoT, la seguridad de estos dispositivos se convierte en un desafío crítico.

Privacidad de los datos: Las regulaciones de privacidad de datos, como el RGPD, continúan impulsando la adopción de medidas de protección de datos más robustas.

Ataques dirigidos y ransomware: Los ataques, cada vez más dirigidos, y el ransomware siguen siendo una amenaza significativa, lo que exige una mayor vigilancia y preparación.

Barreras y desafíos:

Brecha de talento: La escasez de profesionales de ciberseguridad altamente cualificados sigue siendo un desafío importante.

Complejidad del entorno: La creciente complejidad de los entornos tecnológicos y la rápida evolución de las amenazas dificultan la gestión de la seguridad.

Resistencia al cambio: La transformación digital y la adopción de nuevas tecnologías pueden encontrar resistencia en algunas organizaciones.

Factores clave de éxito:

Liderazgo y compromiso: El apoyo de la alta dirección es fundamental para el éxito de cualquier iniciativa de ciberseguridad.

Cultura de seguridad: Fomentar una cultura de seguridad en toda la organización es clave para prevenir incidentes. Desde los comités de Dirección hasta los programadores que deben imbuir la seguridad en sus diseños.

Colaboración entre equipos: La colaboración entre los equipos de TI, seguridad y negocio es esencial para una gestión efectiva de la ciberseguridad.

Partners estratégicos: La elección de partners de ciberseguridad confiables y experimentados es crucial para complementar las capacidades internas.

El futuro de la ciberseguridad:

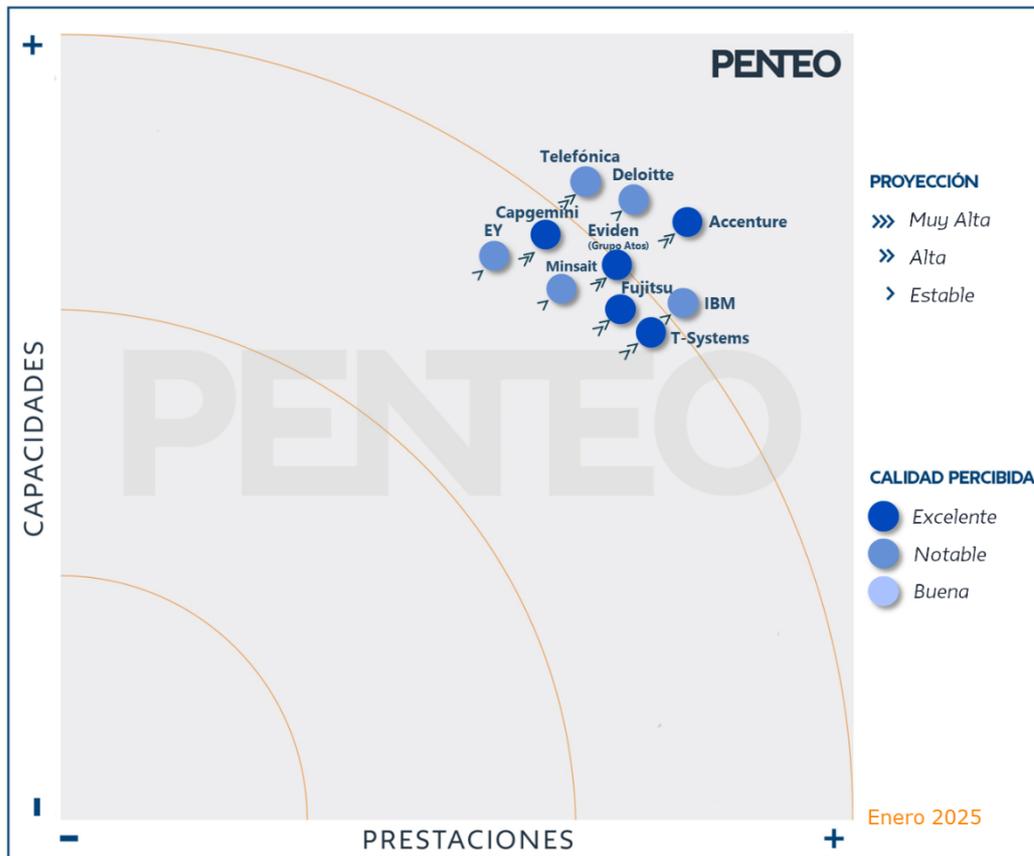
Ciberseguridad como servicio: Se espera un crecimiento significativo en la adopción de servicios de seguridad gestionados, como los SOCs y SOAR.

Automatización y orquestación: La automatización de procesos de seguridad y la orquestación de herramientas permitirán una respuesta más rápida y eficiente a las amenazas.

Seguridad basada en identidad: La identidad digital se convertirá en el perímetro de seguridad, con un enfoque en la autenticación multifactor y la gestión de identidades y accesos.

Los 10 principales actores posicionados por Penteo y por orden alfabético en el Universo de Ciberseguridad 2024 son: Accenture, Capgemini, Deloitte, Eviden (Grupo Atos), EY, Fujitsu, IBM, Minsait, T-Systems y Telefónica.

Mapa del Universo



Dimensiones evaluadas en el marco del análisis:

Para efectuar la evaluación¹, se ha analizado el posicionamiento relativo de los actores seleccionados por Penteo en base a 4 dimensiones: Capacidades, Prestaciones, Proyección y Calidad Percibida, caracterizadas de acuerdo a 10 factores formados por 35 indicadores, que se desglosan en más de 135 preguntas a las que dar respuesta. Más detalladamente:

- Las CAPACIDADES evalúan el volumen de negocio en la línea de servicio, la capacidad del delivery, la estructura y equipo, así como la aproximación al mercado que realiza.
- Las PRESTACIONES evalúan la amplitud y cobertura del porfolio, el alcance de los servicios ofrecidos, las herramientas y metodologías utilizadas, las alianzas y activos, casos de uso, las referencias, etc.
- La PROYECCIÓN evalúa la trayectoria del proveedor en los últimos 3 años combinado con las innovaciones realizadas tanto a nivel de compañía como a nivel de la línea de servicio, el roadmap previsto y la tracción como proveedor de servicios de Ciberseguridad.
- La CALIDAD PERCIBIDA evalúa la satisfacción de sus clientes. Relación valor/precio, proceso comercial, delivery, flexibilidad y adaptación al cliente, etc.

¹ 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.

Vendor Profile



Capgemini

Company Profile

- **Fundación:** 1967
- **Inicio de operaciones en España:** 1975
- **Propiedad:** Capgemini, S.E. (86%), Sogeti, S.A.S. (14%)
- **Ingresos último año fiscal:**
 - España: N.D.
 - Mundo: 22.000 M€
- **Empleados:**
 - España: 11.000 empleados
 - Mundo: 340.000 empleados
- **Oficinas:**
 - España: Oficinas en Madrid, Barcelona y Sevilla y centros de excelencia en Asturias (Langreo), Málaga, Valencia, Murcia y Vigo.
 - Mundo: opera con oficinas en más de 50 países.
- **Principales actividades de negocio:** Con la innovación como eje central, establecen un puente entre el negocio y la tecnología. Su enfoque basado en la innovación permite que sus clientes se beneficien del poder de la tecnología y sus avances. Su portfolio de servicios ofrece una amplia gama de servicios: desde el desarrollo de nuevos negocios, hasta la mejora de su productividad mediante el aprovechamiento de las próximas olas de tecnología. Sus principales servicios: Cloud: aplicando un enfoque cloud-first, ayudan a sus clientes a definir la estrategia cloud más adecuada para su negocio. También les ayudan a gestionar sus entornos híbridos, al tiempo que protegen todos sus datos. Ciberseguridad: su completa cartera de servicios de consultoría, cumplimiento, protección y supervisión está diseñada para proteger las TI tradicionales, así como la nube, el Internet de las cosas y los sistemas digitales. ADM Next: un enfoque único para el desarrollo y mantenimiento de aplicaciones (ADM). Sus servicios son potentes aceleradores del crecimiento, ya que reúnen lo mejor de la tecnología, los procesos y los conocimientos para mejorar la agilidad empresarial frente a la automatización, el big data y otros avances tecnológicos. Digital Core con SAP / SAP HANA. Aprovecha esta plataforma para combinar la tecnología, los procesos y los modelos operativos con el fin de acelerar la innovación, protegiendo al mismo tiempo las aplicaciones SAP esenciales para el negocio. Industria inteligente: impulsada por los datos, su oferta acelera y asegura la convergencia de los mundos físico y digital de sus clientes. Su experiencia abarca desde el PLM (gestión del ciclo de vida del producto) hasta las fábricas 4.0. AI & Analytics: proporcionar a sus clientes soluciones y servicios de IA para desarrollar su excelencia operativa, crecimiento, rendimiento e innovación mediante un enfoque ético y responsable de la IA. Customer Experience: Ayudan a sus clientes a reforzar las relaciones con sus propios clientes, mediante un análisis riguroso y tecnologías de vanguardia que les permitan comprender mejor sus tendencias, intuiciones y personalidades.
- **Descripción de la compañía:** Capgemini es una de las principales consultoras de servicios de tecnología y transformación digital a nivel mundial. Fundada en 1967, la compañía opera en más de 50 países y cuenta con aproximadamente 340,000 empleados. En 2023, alcanzó ingresos globales de 22,000 millones de euros, consolidándose como un referente en servicios de consultoría, tecnología,

ingeniería y gestión de operaciones. La oferta de Capgemini incluye áreas clave como la nube, la inteligencia artificial, la gestión empresarial, la sostenibilidad y la ciberseguridad. Destaca su enfoque en la innovación y su capacidad para adaptar soluciones tecnológicas avanzadas a sectores como banca, retail, manufactura, salud, telecomunicaciones, energía y aeroespacial. En ciberseguridad, Capgemini proporciona servicios integrales que abarcan la protección de datos, el diseño de arquitecturas seguras y la respuesta a incidentes, ayudando a las empresas a protegerse contra amenazas crecientes. Tiene una fuerte presencia en áreas emergentes como análisis de datos, inteligencia artificial, ciberseguridad, automatización y sostenibilidad empresarial. Su división de ciberseguridad es especialmente destacada, proporcionando soluciones integrales que abarcan desde la evaluación de riesgos hasta la implementación de estrategias de defensa frente a ciberataques. Los servicios incluyen gestión de identidades y accesos, protección de datos críticos, seguridad en la nube, respuesta a incidentes y análisis forense digital, ayudando a las empresas a garantizar la continuidad del negocio y cumplir con normativas de seguridad.

Service Profile

- **Inicio de prestación de servicios de ciberseguridad en España: 2015**
- **Plantilla dedicada a servicios de ciberseguridad:**
 - España: 248;
 - Mundo: > 6,500
- **SOC:** Dispone de un SOC propio en Langreo (Asturias) y otro en Málaga.
- **Principal cobertura de servicios de ciberseguridad:** servicios de análisis y estrategia de ciberseguridad, evaluación de la madurez de los clientes, elaboración y definición de proyectos orientados al cumplimiento legal y normativo, formación a usuarios y concienciación, servicios de gestión de identidades, protección de información, servicios de consultoría en seguridad de aplicaciones y datos, servicios de detección y respuesta a incidentes y ciber inteligencia.
- **Servicios y soluciones propias:** Portal de servicios gestionados para dar una visión de 360º a las operaciones de seguridad gestionada; Identity as a Service bajo modelo OPEX y con tecnologías RSA, Ping Identity y Cyberark; Application Security Testing para detección de vulnerabilidades en código como servicio.
- **Partners y alianzas principales:** Microsoft, Google, Fortinet, Splunk, Veracode, Cyberark, Palo Alto, IBM, Delinea, Watchguard, Claroty y Lookout, entre otras. Recientemente han creado nuevos partnerships con Threema, Zscaler y Crowdstrike
- **Segmentación de clientes:**
 - Pequeña empresa (< 100 M €/año): 0%
 - Mediana empresa (100 - 500 M €/año): 2,5%
 - Gran empresa (500 - 1.000 M €/año): 37,5%
 - Corporación (>1.000M €/año): 61%

Servicios de Ciberseguridad

- **Define:** Servicios que abordan la gama completa de necesidades de ciberseguridad, estrategia, evaluación y despliegue. Incluye servicios de consultoría estratégica y operativa y una amplia gama de servicios de evaluación. Trabajando en estrecha colaboración con sus principales interesados, diseñan una estrategia y una hoja de ruta que se alinea con sus objetivos de negocio. Objetivos: convertir a los clientes en un disruptor digital, automatizar la seguridad, inteligencia artificial, análisis y seguridad en la nube, modernizar prácticas de seguridad actuales, gestión de requisitos de cumplimiento, reducción de coste de aseguramiento.
- **Protect:** Implementación de soluciones que abordan objetivos comerciales al tiempo que protegen los datos, sistemas y usuarios críticos. Sus servicios se adaptan a los requisitos específicos de los clientes, generalmente basados en los resultados los servicios de consultoría y evaluación. Se pueden entregar como una implementación específica para un cliente o como servicios de seguridad gestionados remotos.
- **Defend:** Se pueden entregar como una implementación específica para un cliente o como servicios de seguridad gestionados remotos que podrían incluir, inteligencia de amenazas, detección de incidentes, respuesta a incidentes e informes. Los servicios de monitorización de seguridad cibernética (SOC) podrían incluir el despliegue y la configuración del equipo de seguridad necesario (SIEM, IPS, Sandbox, herramienta de análisis de comportamiento del usuario, plataforma de Big Data, herramientas RPA, herramientas de inteligencia artificial, etc.). Permite obtener una vista completa y precisa de la seguridad, predecir y prevenir ataques y cumplir constantemente los requisitos de cumplimiento.

Claras Fortalezas

- **Proyección línea negocio y Top of Mind.** Capgemini está experimentando unos altos ratios de crecimiento en cuanto a volumen de facturación, por encima de los objetivos inicialmente marcados. La estrategia planteada hace 4 años les ha permitido avanzar, con un crecimiento superior al 50% respecto al año pasado. Asimismo, continúa reforzando el equipo con perfiles reconocidos en el ámbito de la ciberseguridad en España. Cabe destacar que uno de los focos de la compañía es la fidelidad del talento, apostando por mantener y evolucionar el conocimiento dentro de la firma. Es por ello que cuentan con una de las tasas de rotación más bajas del mercado y de este estudio.
- **Uso de IA y tecnologías avanzadas:** Capgemini aplica inteligencia artificial generativa para identificar y contrarrestar amenazas emergentes como ransomware, phishing y ataques basados en ingeniería social. Este enfoque permite una defensa proactiva y adaptable, optimizando la gestión de riesgos en entornos complejos. Adicionalmente integra innovaciones como análisis de datos en tiempo real y soluciones de automatización para maximizar la eficiencia de la ciberseguridad. Así como tecnologías cuánticas, con las que ayudan a las empresas a resolver problemas empresariales y sociales que antes eran inabordables.
- **Enfoque integral:** Su cartera de servicios abarca desde la protección de infraestructuras críticas hasta la gestión de datos y sistemas en entornos de TI, nube y operaciones tecnológicas (OT). Esto asegura una cobertura completa de las necesidades empresariales, desde el diseño de defensas hasta su implementación (recordemos el gran refuerzo de la compañía en este ámbito tras la exitosa integración con Altran).

A evaluar su evolución en...

- **Experiencia adquirida en proyectos europeos.** El modelo de negocio desarrollado por Capgemini en España les ha llevado a absorber proyectos a nivel europeo en sus centros de Asturias y Málaga, lo que les aporta un conocimiento muy valioso a la hora de ejecutar proyectos a nivel nacional. Adicionalmente, hay muchos equipos que buscan el poder trasladarse de sus países a alguno de estos centros, lo que, sumado al crecimiento en cuanto a facturación y tamaño de clientes, les permite plantearse seguir realizando nuevas contrataciones e incluso llegar a abrir un nuevo centro de excelencia dentro del territorio nacional para cubrir la demanda.
- **Oportunidades en sectores alternativos.** Capgemini tiene una gran oportunidad para posicionarse como líder en el ámbito de la ciberseguridad OT, con capacidades que otro tipo de actores no van a ser capaces de disponer. Su equipo dispone, por ejemplo, de varios certificados representativos en el ámbito de la ciberseguridad industrial. Esto le brinda una oportunidad para consolidar y liderar este tipo de offering en sectores como el aeroespacial, defensa o energía en España. Para poder seguir ganando tracción en esta línea de servicio, parte de su estrategia podría dirigirse a tratar de entrar, a través de proyectos relevantes, en otras verticales que consideren, en las que actualmente se tiene menor presencia o awareness de sus altas capacidades y prestaciones en la línea de ciberseguridad.
- **Mercado.** El mercado de ciberseguridad en España está siendo altamente competitivo, con presencia de grandes compañías muy establecidas en el mercado que están otorgando especial relevancia a la línea de negocio de Ciberseguridad como palanca de crecimiento. La natural evolución esperada tras los 4 años de inversión les ha hecho avanzar en cuanto al cliente objetivo, centrándose y poniendo el foco principalmente en trabajar con empresas del segmento IBEX.

Sobre el Universo Penteo

En el Universo Penteo se posicionan a los principales actores en España de un servicio TI, previa evaluación independiente de Penteo en 4 dimensiones: Capacidades, Prestaciones, Proyección y Calidad. Este análisis es un referente que tiene amplia difusión y llega prácticamente a la totalidad



Sobre Penteo

Penteo es el analista TI independiente que lidera la mayor Comunidad de Conocimiento TI de España, y ofrece un servicio especialmente diseñado para Directivos con influencia o responsabilidad en las decisiones TI-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 10 años, Penteo ha liderado el nivel del mercado de TI y las Tecnologías de la Información.



Desarrollamos informes de primer nivel, y extraer de

Tu asesor TI de confianza que proporciona conocimiento y apoyo experto e independiente

Propiedad Penteo.

Esta publicación no puede ser reproducida. El único informe publicable y distribuible relativo al Universo Penteo es el informe Universe Overview, siempre y cuando se haya contratado el Penteo Market Report con los derechos de reprint asociados correspondientes. La información que contiene este informe se ha obtenido de fuentes consideradas fiables. Penteo no se responsabiliza de posibles errores, omisiones o inexactitudes que pueda contener este informe, así como del uso que pueda hacerse de las recomendaciones u opiniones que contiene.

PENTEO

DIGITAL INNOVATION TECHNOLOGY

+34 902 154 550
info@penteo.com
penteo.com

