IDG
RESEARCH SERVICES

INFORME

SEGURIDAD CLOUD

Telefónica | EMPRESAS

Resumen Ejecutivo

En este informe se realiza un análisis del mercado de la seguridad en la mediana y gran empresa española (empresas de más de 500 empleados), haciendo foco en cloud.

El mercado de la seguridad está experimentando una fase expansiva, impulsada por el desarrollo de los negocios digitales, que va a continuar durante los próximos años. No obstante, este crecimiento no es uniforme. Por ello, en este informe se ha realizado una segmentación, que permite priorizar los grupos con mayor oportunidad, para permitir un enfoque comercial diferenciado.

Para realizar la segmentación, el criterio utilizado ha sido el de la inversión en seguridad respecto al presupuesto de TI. Este criterio ha permitido crear cuatro segmentos, en los que sus empresas comparten un conjunto de características homogéneas.

El promedio de inversión en el conjunto de las grandes y medianas empresas españolas es del 5.7% de su presupuesto de TI. Los segmentos de más interés son los dos que invierten por encima de este promedio, que se describen a continuación:

- Seguridad proactiva: Invierten más del 10% del presupuesto de TI en seguridad. En estas empresas (15% del total) la seguridad forma parte de la estrategia digital de la empresa: es un pilar de la confianza de los clientes, y entra en las iniciativas desde el principio. Muchas de ellas tienen un CISO independiente que está evolucionando hacia una mayor integración con el negocio y cuya interlocución mira cada vez más hacia la dirección. Este segmento permite mensajes más sofisticados y las áreas de crecimiento se encuentran en la innovación, en la creación de nuevos servicios y su protección.

- Seguridad expansiva: Invierten entre el 7 y el 10% de su presupuesto de TI en seguridad. En estas empresas (24% del total) la inversión en seguridad crece más rápido que la de TI. Esto se debe a su dinámica de digitalización, así como al impacto de la regulación. No obstante, la seguridad está todavía fuertemente ligada al área de tecnología (de hecho, el responsable de seguridad reporta al CIO), y no se entiende como un elemento integrado en la actividad de la empresa. En estas organizaciones es recomendable entender las prioridades de negocio, y vincularlas con las soluciones de seguridad, ayudando a su responsable a extender su ámbito de influencia.

Los segmentos que invierten por debajo de la media son de menor interés, dado que dan menor prioridad a la seguridad: su enfoque es más táctico y reactivo, y son más sensibles al coste. Necesitan un esfuerzo de educación a medio plazo que no puede realizar una empresa en solitario, sino que atañe a la industria de seguridad en su conjunto.

En el caso de cloud, para entender la demanda entran en juego dos variables: la madurez en seguridad, así como la madurez en cloud. Sin embargo, estas no están acompasadas. Mientras que el mercado está adoptando cloud mayoritariamente, la seguridad solo es una prioridad para una de cada cuatro empresas. Esto indica que hay un recorrido de crecimiento para los proveedores, aunque requiere un trabajo de concienciación.

Esto se refleja con claridad en un nutrido grupo de empresas (40%), que están avanzadas en sus migraciones a cloud, pero inmaduras en su seguridad. Esto significa que están asumiendo riesgos, y por tanto es de interés posicionarse en ellas, dado que en algún momento esos riesgos dispararán la necesidad de invertir en seguridad.

Los nuevos desarrollos representan el área más compleja para comercializar la seguridad, dado que además de su madurez entra en juego la adopción de metodologías ágiles. Una oportunidad a destacar aquí es la de las empresas que realizan sus desarrollos de una forma más tradicional, sin utilizar cloud, pero incorporando la seguridad desde el principio (25%). En estas empresas, el esfuerzo de los responsables de seguridad ha dado sus frutos, lo que facilita la conversación sobre la seguridad. El reto está en evolucionar hacia la agilidad sin disrupciones.

Por otro lado, gran parte de las empresas que realizan nuevos desarrollos en cloud, lo han hecho lanzando nuevas metodologías como DevOps, y no han tenido en cuenta la seguridad para incorporarla en los ciclos de desarrollo. Para el responsable de seguridad esto representa volver al punto de partida y, por ello, tienen por delante un recorrido de maduración.

En resumen, el posicionamiento de la seguridad en cloud varía según la situación: en el caso de migraciones de cargas de negocio se producirá un despegue súbito de la seguridad cuando se den las condiciones, mientras que en los nuevos desarrollos las oportunidades van a presentarse de forma gradual.

Finalmente, el estudio ha explorado cuáles son los actores de referencia en la seguridad cloud. El resultado indica que la preferencia de las empresas es una combinación de ellos: una gran mayoría (75%) se apoya en su equipo interno en primer lugar; después, un 59% mira hacia su proveedor de servicios en cloud. El fabricante de seguridad se toma como referencia en un 14% de los casos, y el operador de telecomunicaciones en un 9%. Estos datos invitan a evaluar las estrategias de alianzas entre los distintos actores.

CONTENIDO

1. Introducción 6
2. Presupuestos de seguridad 8
3. Cuatro segmentos en función del presupuesto 10
  3.1 Segmento proactivo 12
    3.1.1 Criterios para identificación 13
  3.2 Segmento expansivo 14
    3.2.1 Criterios para identificación 15
  3.3 Segmento reactivo 16
    3.3.1 Criterios para identificación 17
  3.4 Segmento Infra-invierten 18
    3.4.1. Criterios para identificación 19
4. Prioridades 20
5. Seguridad de cloud pública 23
  5.1 Ciclo de seguridad en cloud 25
  5.2 Perfil de seguridad y adopción cloud 26
    5.2.1 Migración a cloud y perfiles de seguridad 27
      5.2.1.1 Segmento arriesgado: mover hacia el seguro 28
      5.2.1.2 Segmento seguro: optimizar la inversión en seguridad 29
      5.2.1.3 Segmento inmaduro: concienciar de la “security-first” cuando se muevan a cloud 29
      5.2.1.4 Segmento conservador: Aproximación caso a caso 30
    5.2.2 Desarrollos en cloud y perfiles de seguridad 30
      5.2.2.1 Segmento conservador: Concienciar de cómo cloud permite habilitar DevOps y DevSecOps 32
      5.2.2.2 Segmento seguro: Crecer con el cliente – expandir las oportunidades de innovación segura 32
      5.2.2.3 Segmento arriesgado: Introducir la seguridad en los desarrollos, desde el principio del proyecto 33
      5.2.2.4 Inmaduro: Educar al cliente 33
6. Percepción de proveedores 34
  6.1 Percepción sobre Telefónica y Akamai 36
7. Recomendaciones de IDG Research 38
  7.1 Recomendaciones generales 38
  7.2 Recomendaciones por segmento 39
  7.3 Recomendaciones sobre la protección de cloud 41
Anexo 1. Demografía de la muestra 42
Anexo 2. Decisión sobre el presupuesto 43
Anexo 3. Propensión hacia la externalización 44

1. Introducción

El mercado de seguridad se encuentra en una etapa expansiva impulsada por el desarrollo de los negocios digitales. Durante los próximos años va a seguir experimentando un crecimiento en línea con la transformación digital de las organizaciones.

No obstante, este crecimiento no es uniforme. Hay un conjunto de empresas que conciben la seguridad como un pilar del negocio digital, sobre el que descansa la confianza de clientes y empleados. Son estas empresas quienes están liderando la inversión y sirven de referencia para el resto del mercado. En ellas, el puesto del responsable de seguridad está evolucionando hacia una mayor integración con el negocio y una interlocución que mira cada vez más hacia la dirección.

Sin embargo, el grueso del mercado dista de estar en esta situación. Lo más habitual es que el área de seguridad sea un área especializada dentro del departamento de TI, pero con escasa relación con las unidades de negocio. Esto lleva a que sus inversiones se produzcan bajo un enfoque táctico y pragmático, y que se perciban como un freno a las iniciativas de negocio.

Desde el punto de vista de proveedor, las diferencias en el enfoque digital de los negocios y en la importancia que dan a la seguridad se traducen en perfiles distintos de empresa, que requieren aproximaciones diferentes. Con este fin, en este informe se realiza una segmentación, identificando grupos con características homogéneas, que permiten un enfoque comercial consistente, así como priorizar aquellas empresas en las que existe una mayor oportunidad.

El estudio analiza de forma específica la seguridad en cloud. Actualmente, no se encuentra entre las principales prioridades del grueso del mercado; muchas están adoptando cloud sin una estrategia de seguridad. Esto representa una oportunidad para que los proveedores se posicionen: el mercado de seguridad en cloud está destinado a despegar, y puede que lo haga de forma brusca si tiene lugar algún ataque o incidencia a escala.

Finalmente, se ha estudiado la seguridad en los desarrollos en cloud. Este es uno de los aspectos que recibe menos atención en las empresas, dado que tiende a priorizarse la agilidad.

El estudio pone de manifiesto que la seguridad en cloud requiere un cambio de paradigma por parte de las empresas. Esto también afecta a la forma en que se comercializan las soluciones, en particular cuando se trata de los segmentos más avanzados. Los responsables de seguridad necesitan que sus proveedores les liberen tiempo y recursos para dedicarlo a la estrategia. También necesitan que los proveedores hablen su lenguaje, entiendan sus prioridades (ej. resiliencia de las operaciones), y hayan analizado la cadena de impactos hasta llegar al riesgo de negocio. Los proveedores que hagan el esfuerzo estarán por delante de la competencia.

2. Presupuestos de seguridad

El presupuesto de seguridad es un indicador del grado de madurez de la organización en relación con la seguridad. Aunque la eficacia de esta inversión viene determinada por el hecho de que exista una estrategia bien definida y alineada con el negocio, la proporción sobre el gasto TI refleja la importancia de la seguridad en la organización.

Las cifras que se utilizan en este estudio son las del presupuesto que maneja el responsable de seguridad. Se trata de una aproximación a la inversión global en la empresa, pues existen aspectos de la seguridad que son financiados por otras áreas. Por ejemplo, este es el caso de las unidades de negocio que adquieren tecnología o realizan desarrollos con cargo a sus propios fondos.

Además, existe una dispersión de los presupuestos en función del tamaño de la empresa y del sector de actividad en el que operan. Esta persiste incluso en el caso de empresas similares. Por tanto, es difícil establecer comparativas individuales. Otros factores para considerar en la variabilidad observada en los presupuestos son:

- Presupuesto descentralizado: Un modelo completamente centralizado, como el que funciona para la organización de TI, puede no ser extrapolable al ámbito de la seguridad. Esta debe buscar un equilibrio entre el alineamiento con las necesidades de cada unidad de negocio y un enfoque consistente en toda la organización.

- Presupuesto oculto, no visible para el responsable de seguridad: Muchos departamentos compran embebida la seguridad en algunas soluciones sin involucrar al departamento responsable de la misma. Además, algunas actividades pueden estar fuera del ámbito del departamento de seguridad. Por ejemplo, la formación de los empleados.

- Costes recurrentes: La velocidad de cambio en el terreno de la seguridad hace que el gasto sea difícil de predecir, y todavía más de cuantificar. En particular, resulta difícil estimar el volumen de gastos recurrentes.

Otros aspectos que impactan en la dispersión de los presupuestos están relacionados con la estrategia de la empresa y su posiciona-miento en el mercado:

- Grado de digitalización: Las necesidades de seguridad están estrechamente vinculadas a la transformación digital de la empresa. A medida que se adoptan nuevas tecnologías digitales, se amplía la superficie de ataque y las necesidades de seguridad aumentan.

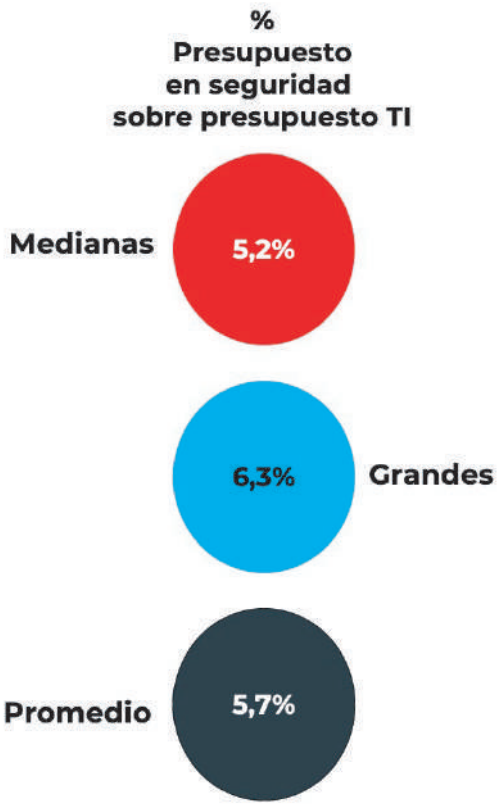
- Estrategia de negocio: En muchas empresas la seguridad sigue estando aislada de la estrategia de negocio y, por tanto, se invierte de forma reactiva. Por el contrario, en las empresas más avanzadas digitalmente, la seguridad forma parte de la estrategia empresarial y se vinculan los recursos con el riesgo de negocio.

Finalmente, hay una correlación entre inversión en seguridad e impacto en la empresa hasta que se alcanza un umbral. Una vez cubiertas ciertas necesidades básicas, un mayor presupuesto no se traduce necesariamente en una mejor protección. Los responsables de seguridad necesitan visibilidad sobre el valor real que proporciona cada producto en el que invierten; esto pasa por saber si se está utilizando de manera efectiva y si se obtienen los resultados esperados.

No obstante, los datos de inversión en seguridad son suficientemente representativos para agrupar a las empresas en diferentes segmentos con características homogéneas. Estos segmentos se presentan más adelante en el estudio.

El siguiente gráfico muestra el presupuesto promedio destinado a seguridad por parte de las empresas con más de 500 empleados. La inversión representa una proporción del 5,7% respecto al presupuesto en TI.

Gráfico 1. Presupuesto en seguridad promedio y tamaño de empresa



Fuente: IDG Research, 2019

3. Cuatro segmentos en función del presupuesto

A partir del presupuesto en seguridad pueden establecerse cuatro segmentos de empresas con un conjunto de características propias, relacionadas con su madurez en la seguridad. Aquellas con mayor grado de madurez tienen un enfoque de dentro a fuera; parten de la estrategia de negocio para decidir el riesgo que quieren asumir. Sin embargo, las menos maduras tienen un enfoque de fuera a dentro; parten de las amenazas y vulnerabilidades para asignar sus recursos.

Las diferencias de enfoque se traducen en diferencias de porcentaje de la inversión en seguridad sobre el presupuesto total de TI. De este modo, el análisis presupuestario permite distinguir entre empresas proactivas, empresas en fase expansiva, empresas reactivas y aquellas que infra-invierten.

- Empresas proactivas. Este segmento de empresas invierte más del 10% de su presupuesto de TI en seguridad. Son el segmento de empresas con mayor grado de madurez y entienden **la seguridad como un habilitador del negocio digital.** Este grupo es minoritario: solo abarca un 15% de las empresas de más de 500 empleados.

- Empresas expansivas. Este segmento de empresas invierte entre un 7% y un 10% de su presupuesto de TI en seguridad. Son el segmento de empresas en el que **los presupuestos tanto en TI como en seguridad están aumentando.** Un 24% de las empresas de más de 500 empleados pertenecen a este grupo.

- Empresas reactivas. Este segmento de empresas invierte por debajo de la media, entre un 3% y un 6% de su presupuesto de TI en seguridad. No existe un alineamiento entre los riesgos de negocio y la seguridad. **La inversión en seguridad se realiza de forma táctica, como respuesta a amenazas.** A este grupo pertenecen un 31% de las empresas de más de 500 empleados.

- Empresas que infra-invierten. Este segmento de empresas invierte menos de un 3% de su presupuesto de TI en seguridad. Son empresas con un escaso grado de digitalización y la tecnología no es una prioridad para el negocio sino más bien un servicio. **La seguridad se percibe como un gasto que hay que limitar.** Este grupo es todavía significativo y a él pertenecen el 30% de las empresas de más de 500 empleados.

Gráfico 2. Segmentación de empresas según presupuesto

Segmento	% Seguridad sobre gasto TI	Descripción	Promedio empresas
	Proactivo >10%	La seguridad como un habilitador del negocio digital	15% Empresas
	Expansivo 7%-10%	Los presupuestos tanto en TI como en seguridad están aumentando	24% Empresas
	Reactivo 3%-6%	No existe un alineamiento entre los riesgos de negocio y la seguridad	31% Empresas
	Infra-invierten <3%	Escaso grado de digitalización: la tecnología no es una prioridad	30% Empresas

Fuente: IDG Research, 2019

3.1 Segmento proactivo

Este segmento agrupa a las empresas en las que una parte importante de su actividad es digital; la seguridad se entiende como un componente intrínseco de su estrategia de negocio. Este grupo de empresas no necesita un esfuerzo de concienciación por parte del proveedor. Se trata de organizaciones que aceptan un mensaje más sofisticado, orientado a futuro y no sólo a cubrir sus necesidades actuales.

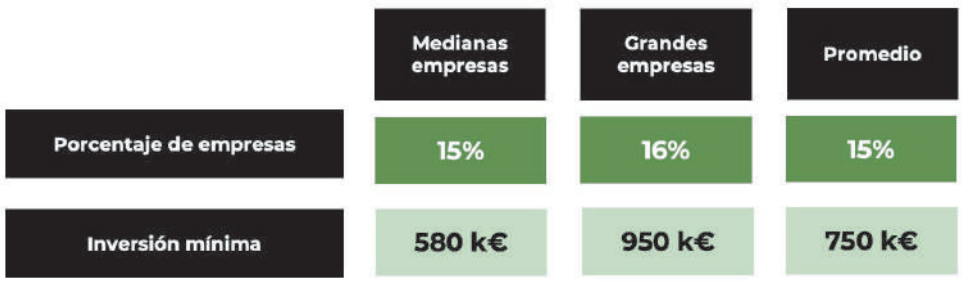
La inversión en seguridad representa más de un 10% de su presupuesto TI, muy por encima de la media que se sitúa en el 5,7%. Es un grupo minoritario, aproximadamente el 15%. La inversión en términos absolutos muestra un umbral mínimo presupuestario de 750 k€, pero es significativamente mayor en las grandes empresas -950 k€- que en las medianas- 580 k€-.

A este segmento pertenecen tanto grandes como medianas empresas. Su proporción de inversión en seguridad es similar. Las características que definen este grupo son:

- Grandes empresas: Un 16% de las empresas de más de mil empleados pertenecen a este grupo. Los sectores mayoritarios son principalmente el sector público y el financiero.

- Medianas empresas: Un 15% de las empresas entran en este segmento. Abarca a empresas de diferentes sectores, y su inversión en seguridad depende más del grado de madurez de su transformación digital que de la actividad que realizan.

Gráfico 3. Empresas proactivas



Fuente: IDG Research, 2019

3.1.1 Criterios para identificación

- Liderazgo: Cuentan con la figura de un CISO, frecuentemente independiente del área de tecnología, lo que le permite mayor libertad de acción. Además, refleja un entendimiento del riesgo de la seguridad como un riesgo de negocio.

- Decisión: La seguridad entra en el comité de dirección y el CEO participa en la toma de decisiones como parte de la estrategia de negocio. Desde la dirección se impulsan distintas iniciativas y políticas que afectan a la empresa en su conjunto.

- Recursos: El departamento de seguridad cuenta con suficientes recursos, que le permiten crear y retener capacidades propias para ejecutar sus iniciativas. El hecho de que el CISO no reporte al CIO le permite negociar presupuestos sobre una base más amplia (comité frente al presupuesto del CIO). Se evita la externalización de sus actividades al considerarse críticas para el negocio.

- Áreas de prioridad: Las áreas con mayor prioridad varían en función del tamaño de empresa. Las más destacadas son accesos e identidades (grandes empresas) y cumplimiento normativo (medianas).

3.2 Segmento expansivo

Este segmento está en proceso de adquirir un enfoque proactivo. Engloba las empresas que están extendiendo su digitalización, y que perciben la necesidad de proteger sus activos digitales. No obstante, todavía la seguridad esta fuertemente ligada al área de tecnología, y no se entiende como un elemento integrado con el negocio. Por ello, se trata de una fase de transición, lo que se refleja en una dinámica de crecimiento de los presupuestos de seguridad más rápido que los del conjunto de la TI.

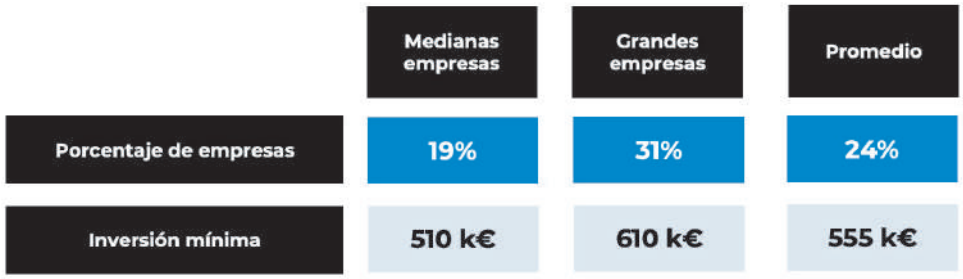
Este segmento invierte en seguridad por encima de la media, entre el 7% y el 10% de su presupuesto TI. Es un grupo de tamaño significativo que alcanza en promedio un 24% del total. La inversión muestra en promedio un umbral presupuestario de 555 k€, siendo ligeramente mayor en las grandes empresas -610 k€- que en las medianas- 510 k€-.

Este segmento está compuesto por empresas de distintos tamaños:

- **Grandes**: Este es el segmento en el que se encuentran un mayor porcentaje de grandes empresas, alcanzando un 31%. Sigue destacando la presencia del sector público, aunque también entran empresas de diferentes sectores que quieren posicionarse como líderes digitales en sus mercados.

- **Medianas:** La proporción de empresas en este segmento supera ligeramente al segmento proactivo y llega al 19%. Existe dispersión sectorial, aunque destacan las empresas de servicios que se han apoyado en los canales digitales tanto hacia el cliente como en sus procesos internos.

Gráfico 4. Empresas expansivas



Fuente: IDG Research, 2019

3.2.1 Criterios para identificación

- Liderazgo: El principal decisor es el CIO, y cuando la empresa cuenta con un CISO, éste frecuentemente le reporta. Esto hace que la seguridad se entienda desde una perspectiva tecnológica, y no se asocie directamente al riesgo de negocio.

- Decisión: El comité de dirección y el CEO participan – en especial en las grandes empresas- en las decisiones de seguridad. La seguridad llega al comité, pero su traducción en términos de negocio y políticas es parcial, afectando únicamente a las áreas más críticas. Es decir, hay recorrido para conseguir que la oportunidad digital se traduzca en mayor inversión en seguridad.

- Recursos: Este segmento depende del presupuesto del departamento de TI para obtener sus recursos. Aunque tiene la capacidad para ejecutar gran parte de las funciones de seguridad internamente, tiene que recurrir a la externalización de algunos aspectos.

- Áreas de prioridad: Las áreas con mayor prioridad, con independencia del tamaño de empresa, son la seguridad de aplicaciones y del dato. Por otro lado, emerge la seguridad de cloud entre las grandes empresas.

3.3 Segmento reactivo

Las empresas de este grupo no son líderes en el negocio digital. Su movimiento hacia lo digital es como respuesta a una dinámica competitiva que les empuja, más que como parte de su estrategia. Son negocios que tienen una actitud de "esperar y ver". Este segmento adopta la seguridad de fuera a dentro; es decir, partiendo de las amenazas externas y con un enfoque eminentemente táctico.

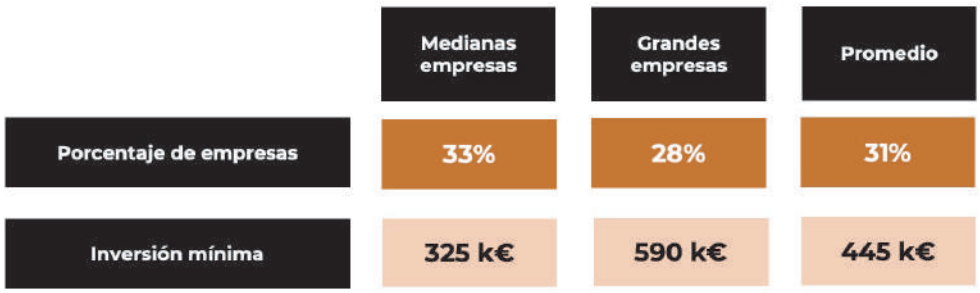
Este segmento de empresas invierte entre el 3% y un 6% de su presupuesto TI en seguridad; es decir, por debajo de la media. Es un grupo de empresas significativo y alcanza en promedio un 31% del total. La inversión en términos absolutos muestra en promedio un umbral mínimo presupuestario de 445 k€, siendo ligeramente mayor en las grandes empresas -590 k€- que en las medianas- 325 k€-.

Este segmento está compuesto por empresas de distintos tamaños, aunque existe una mayor proporción de medianas empresas:

- Grandes: Se trata de un grupo significativo de empresas, que alcanza un 28% del total. Existe dispersión entre sectores. El perfil estratégico es el de seguidora y tienen menor predisposición a innovar. La seguridad no forma parte de la estrategia de negocio.

- Medianas: Es un grupo mayoritario, con una cuota del 33% entre la mediana empresa. Existe dispersión de sectores. Su foco es conseguir el máximo retorno de inversión dado que tienen una clara limitación de recursos. Por eso cubren las necesidades básicas.

Gráfico 5. Empresas reactivas



Fuente: IDG Research, 2019

3.3.1 Criterios para identificación

- Liderazgo: El principal decisor es el CIO, independientemente del tamaño. Este tiene que conciliar sus necesidades de entrega de los servicios TI con su protección. Las prácticas de gestión del riesgo de ciberseguridad no están compartidas en la organización ni consensuadas con la dirección.

- Toma de decisiones: Distintos departamentos intervienen ocasionalmente en la toma de decisión de seguridad. Esto se debe más al enfoque reactivo de la seguridad (ej. incidencias) que a la existencia de una estrategia consensuada.

- Recursos: Unos menores recursos llevan a estas empresas a una mayor propensión a externalizar aspectos de la seguridad. El objetivo es conseguir un mayor rendimiento con un presupuesto limitado.

- Áreas prioritarias: Las áreas con mayor prioridad son la protección frente a amenazas y la seguridad de infraestructura. Por otro lado, destaca que la protección de la innovación no se encuentra en ningún caso entre sus prioridades.

3.4 Segmento Infra-invierten

Este segmento está formado por las organizaciones más lentas en la adopción de tecnologías digitales. La TI no se percibe como parte integral del negocio y la innovación, sino como un departamento de soporte. Esto hace todavía más difícil conseguir una concienciación sobre la ciberseguridad; al no existir un entendimiento claro de la tecnología, todavía lo hay menos del riesgo en torno a la seguridad y su relación con el negocio.

Este segmento de empresas invierte menos del 3% de su presupuesto TI en seguridad; es decir, muy por debajo de la media. Es un grupo de empresas significativo y alcanza en promedio un 30% del total. La inversión en términos absolutos muestra en promedio un umbral mínimo presupuestario de 340 k€, siendo ligeramente mayor en las grandes empresas -410 k€- que en las medianas- 210 k€-.

La presencia de medianas empresas supera a la de grandes, pero existe una proporción relevante de grandes que infra-invierten.

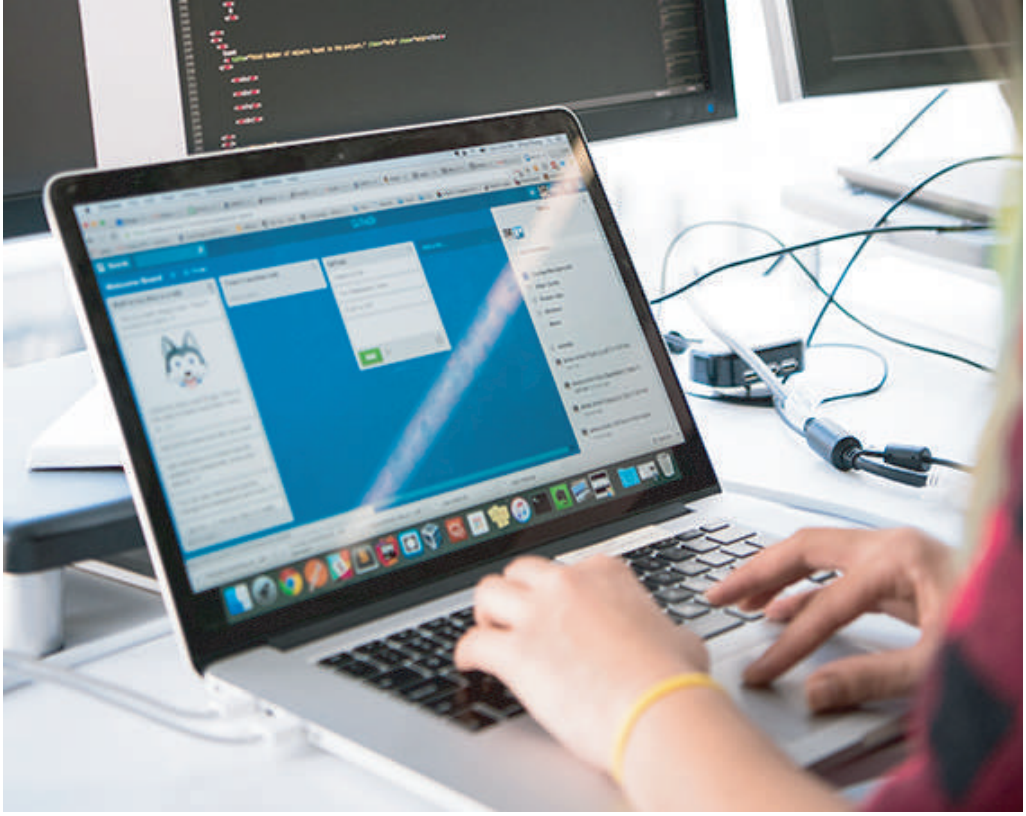
- Grandes: A este segmento pertenece un 25% de las empresas. Es destacable el hecho de que hay más empresas que infra-invierten que proactivas. La distribución sectorial es dispersa, aunque destaca el sector industria. En estas organizaciones no ha tenido lugar una transformación del negocio. Además, la seguridad está supeditada a un incremento en inversión en TI, que también es reducida.

- Medianas: Este segmento incluye un elevado porcentaje de empresas, un 33%. Aunque existe dispersión de sectores, destaca el de industria. Se trata de sectores con entornos que han estado tradicionalmente aislados de la conectividad (ej. fabricación), o que no están en contacto con el cliente final.

Gráfico 6. Empresas que infra-invierten

	Medianas empresas	Grandes empresas	Promedio
Porcentaje de empresas	33%	25%	30%
Inversión mínima	210 k€	410 k€	340 k€

Fuente: IDG Research, 2019



3.4.1 Criterios para identificación

- Liderazgo: El principal decisor es el CIO, y aunque ocasionalmente exista la figura del CISO, este depende del departamento TI, y tiene escasa visibilidad más allá de esta área.

- Decisiones: El CIO es quien toma las decisiones, y no intervienen otros departamentos. Las motivaciones para invertir en seguridad están impulsadas por las exigencias regulatorias, o por el hecho de haber sufrido una brecha, más que por una visión estratégica. Hay una desconexión con la dirección, que afecta tanto a la seguridad como a la tecnología.

- Recursos: Los recursos propios del área de seguridad son muy limitados, lo que limita su capacidad de ejecución. La seguridad se percibe como un coste, y existe una presión para reducirlo o mantenerlo en los niveles mínimos. Esto hace que sea el grupo con mayor propensión a externalizar buscando la eficiencia. Por ejemplo, es el segmento en el que existe un mayor grado de externalización de la seguridad de los desarrollos.

- Áreas de prioridad: Las áreas son similares para ambos tamaños de empresa, destacando el cumplimiento y la seguridad en red.

4. Prioridades

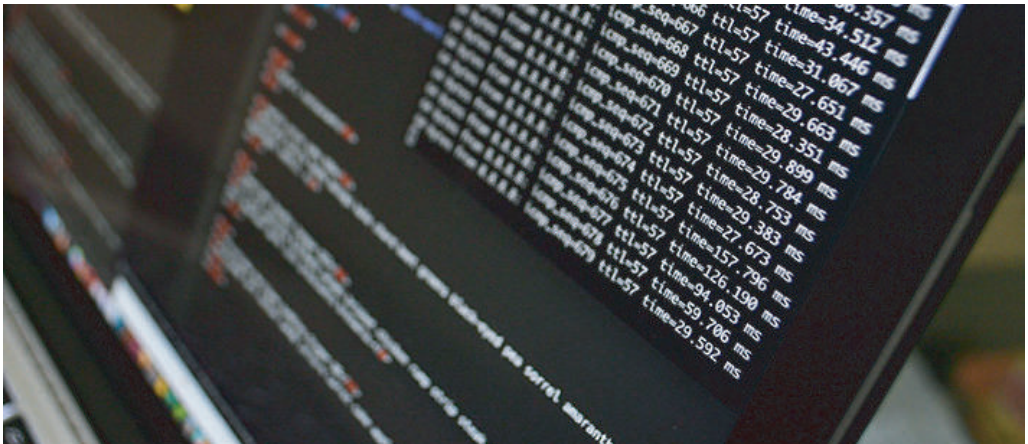
El responsable de seguridad tiene que prestar atención a muchos aspectos con unos recursos limitados. Además, la fragmentación de la oferta se traduce en una proliferación de herramientas ad hoc. En consecuencia, el responsable de seguridad tiene la necesidad de priorizar dónde asigna sus recursos. Para conseguirlo, el mecanismo de partida más eficaz y extendido es un análisis de riesgos.

Las prioridades identificadas en el estudio pueden dividirse en aquellas que son comunes a todas las empresas y aquellas que varían en función del tamaño.

- Prioridades comunes a todos los segmentos: aquellas en las que no existen diferencias significativas según el tamaño de la empresa.

• **Seguridad en el acceso**. Se trata de la prioridad destacada con mayor frecuencia por las empresas (40%). La razón es que tanto empleados como terceros necesitan acceder cada vez a un mayor número de aplicaciones y servicios. Esto conlleva la necesidad de desarrollar un acceso seguro mediante, por ejemplo, una autenticación adecuada. El reto para las empresas es doble. Por un lado, necesitan proteger el acceso a múltiples servicios sin impactar en su experiencia del usuario. Por otro lado, si no existe una política robusta de privilegios puede haber permisos inadecuadamente definidos y abrir brechas de seguridad.

• **Seguridad de aplicaciones**. Para un 35% de las empresas la seguridad de sus aplicaciones es prioritaria. En primer lugar, las empresas están desarrollando un mayor número de aplicaciones, orientadas a la mejora de la experiencia de cliente o la automatización de procesos internos. Por otro lado, las aplicaciones se están volviendo cada vez más complejas – ej. interdependencias, APIs o desarrollos web- que unido a nuevas formas de ataque – ej. bots-, hace que protegerlas sea también más complejo.



Otro factor relevante es que las aplicaciones se encuentran en constante evolución, lo que requiere una dedicación continua de recursos. Por último, aunque se percibe la importancia de la seguridad de las aplicaciones en producción, no se vincula con el proceso de desarrollo.

• **Seguridad del dato.** Un 30% de las empresas consideran la seguridad del dato entre sus prioridades. Entre los motivos destaca el impulso ejercido por la regulación sobre privacidad, que obliga a las empresas a proteger y dar visibilidad sobre el uso y custodia de los datos tanto a clientes como al regulador. A esto hay que añadir que las empresas están construyendo servicios y modelos de negocio innovadores basados en la explotación de los datos. Esto genera nuevos riesgos. Por ejemplo, la inteligencia artificial está abriendo nuevos retos relacionados con el enriquecimiento de los datos y los resultados que se obtienen. Sin embargo, la gestión de la seguridad del dato se produce bajo una fragmentación de la responsabilidad sobre el mismo (el responsable del dato es diferente al responsable de inteligencia artificial o cloud) y resulta difícil abarcar de forma coordinada todo el ciclo; es decir, desde su captura o creación, acceso, operación hasta su borrado.

- Contraste entre segmentos: grupo de prioridades en las que existen diferencias en función del tamaño de empresa.

• **Mayor importancia en grandes empresas**.

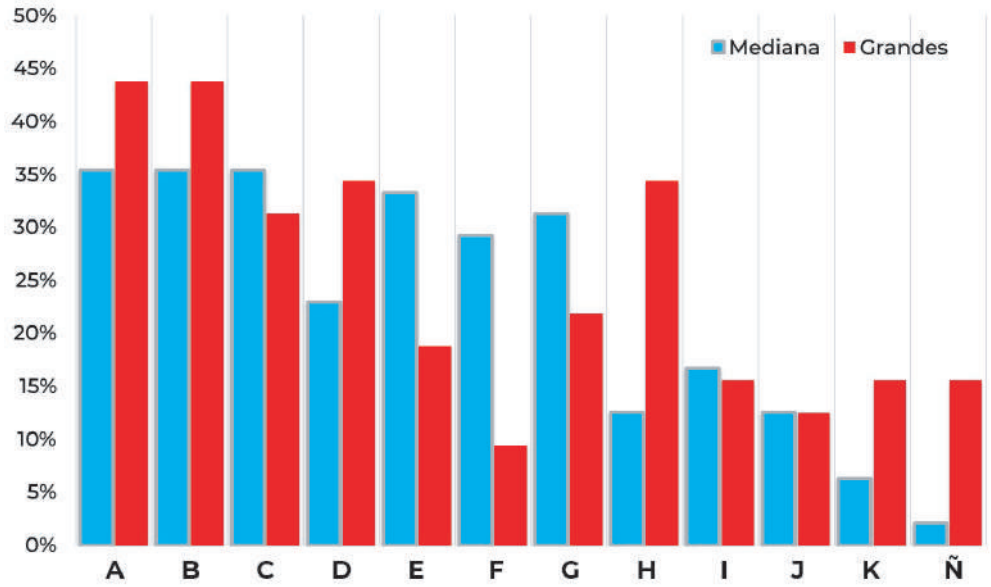
o **Seguridad cloud.** Esta es una prioridad para el 35% de las grandes empresas, mientras que apenas alcanza el 15% de las medianas. La diferencia se debe a que las grandes han comenzado a migrar cargas críticas a cloud (ej. ERP). Además, se trata de un pilar sobre el que se genera la confianza de los clientes y esencial para el negocio. Sin embargo, en las medianas, menos maduras en su uso de cloud, la seguridad todavía no forma parte de sus prioridades.

• **Cumplimiento normativo.** Para un 35% de las grandes empresas es una prioridad, mientras que desciende al 25% en el caso de las medianas. La razón es que las grandes empresas están cambiando gradualmente su mentalidad hacia la regulación, entendiéndola como un marco en el que se va a desarrollar la competencia. Por su parte, las medianas empresas mantienen un enfoque más táctico, buscando el cumplimiento.

• **Mayor prioridad en la mediana empresa**

o **La protección de infraestructura y sistemas.** Mientras que esta es una prioridad para el 30% de las medianas empresas, apenas alcanza el 10% de las grandes. Este ámbito de la seguridad más "tradicional" está fuertemente arraigado entre las medianas empresas, en las grandes, se trata de un aspecto que ha sido abordado.

Gráfico 7. Principales prioridades por tamaño de empresa



A - accesos e identidades **B -** seguridad de aplicaciones **C -** seguridad del dato **D -** cumplimiento regulatorio **E -** seguridad en la red **F -** protección de infraestructuras y sistemas ... **G -** gestión de amenazas y seguridad ... **H -** seguridad de cloud **I -** seguridad de desarollos propios **J -** gestión de la privacidad **K -** seguridad del dispositivo y end points **Ñ -** seguridad de innovación, (ejem. IoT)

Fuente: IDG Research, 2019

5. Seguridad de cloud pública

Los usos de cloud pública están proliferando. En los últimos años las empresas han pasado de utilizarla con un enfoque predominantemente táctico, a adoptar nuevas tecnologías digitales (ej. inteligencia artificial) e incluso migrar cargas críticas.

La situación del mercado puede describirse del siguiente modo:

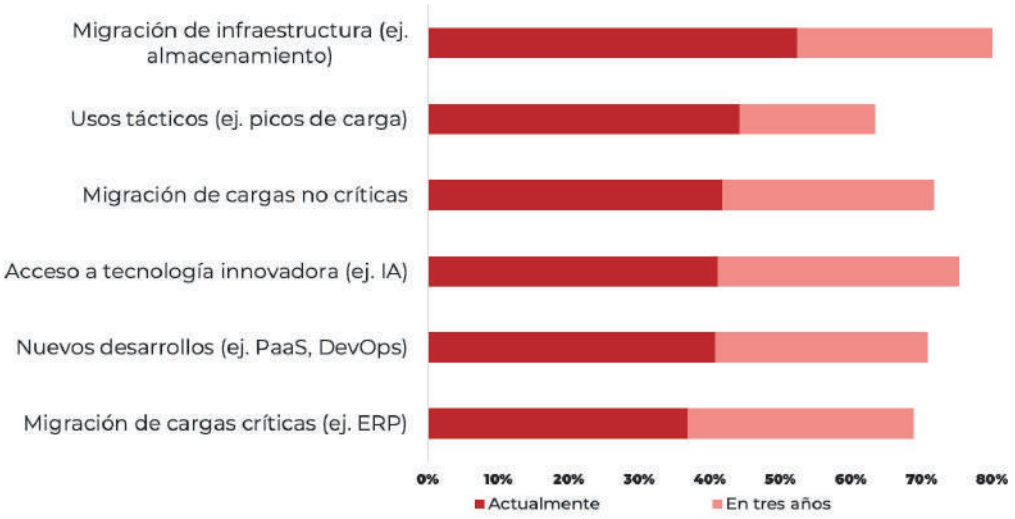
- Usos tácticos de cloud: Este ha sido el principal uso de cloud pública durante los últimos años. Las empresas la han utilizado y para resolver problemas puntuales como atender picos de carga. La motivación se ha centrado en conseguir eficiencias o sustituir CAPEX por OPEX.

- Migración de cargas: En una primera fase, las empresas comenzaron a migrar parte de su infraestructura motivadas por unos menores costes. Sin embargo, un número creciente de empresas empieza a mover cargas, incluso críticas, para agilizar el negocio. Como consecuencia, las empresas se están moviendo rápidamente hacia entornos híbridos y multicloud.

- Innovación digital: Las empresas que quieren innovar encuentran que muchas herramientas innovadoras se encuentran disponibles solo en cloud pública. Además, el proceso de innovación requiere un proceso de prueba y error. Una vez que funciona se necesita escalar rápido. Estas son las condiciones idóneas para que las empresas apuesten por cloud pública en su adopción de nuevas tecnologías digitales.

Actualmente, la migración de infraestructura es el principal uso de cloud pública. En el extremo opuesto se encuentran la migración de cargas críticas. Mirando a futuro, destaca el crecimiento que va a experimentar el uso de cloud pública para acceder a tecnología innovadora.

Gráfico 8. Principales usos de cloud pública



Fuente: IDG Research, 2019

5.1 Ciclo de seguridad en cloud

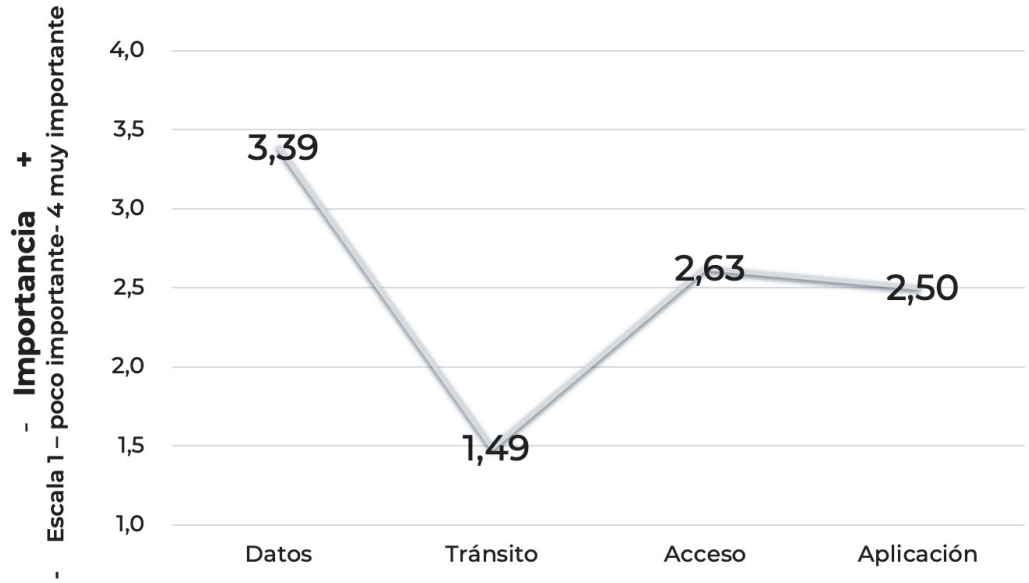
Las empresas han migrado a cloud pública sus cargas de trabajo sin una perspectiva de ciclo de vida del dato. Por eso, la seguridad está muy centrada en la protección del dato, y apenas se presta atención a proteger su tránsito. Hace falta analizar el ciclo de vida de los datos y determinar en qué etapas se encuentran las vulnerabilidades. En última instancia, la seguridad va a estar determinada por el eslabón más débil de la cadena. Algunos ejemplos que ilustran la importancia de una perspectiva de ciclo de vida son:

- Los datos en tránsito que se mueven hacia la nube o dentro de la misma deben protegerse mediante su cifrado.

- Los datos confidenciales deben cifrarse en reposo, para limitar la exposición al acceso de un administrador sin permisos adecuados. Además, debe ser posible establecer la trazabilidad de los accesos.

- En cualquier etapa del ciclo, la notificación de brechas por parte del proveedor debe estar alineada con los protocolos y políticas de la empresa, así como con las obligaciones legales o regulatorias (ej. notificar una brecha antes de 72 horas desde su descubrimiento).

Gráfico 9. Ciclo de vida de la seguridad en cloud



Fuente: IDG Research, 2019

5.2 Perfil de seguridad y adopción cloud

Los proveedores de servicios cloud han hecho grandes esfuerzos en demostrar la seguridad de su oferta. De hecho, la seguridad ha pasado de ser la principal barrera en la adopción de cloud a convertirse en un elemento de confianza. Esto ha provocado que muchas empresas relajen su foco en la seguridad, sin entender que están adoptando un modelo de seguridad compartida.

Los proveedores de cloud suelen hacer público su modelo de responsabilidad compartida. No obstante, este modelo cubre solo los casos genéricos. A medida que aparecen nuevas modalidades de cloud, como containers o serverless, así como en el caso de las APIs, las líneas divisorias entre proveedor y cliente no están claras. Esta tendencia se va a acrecentar cuando emerjan las arquitecturas edge y fog computing.

En síntesis, las empresas están adoptando cloud con diferente entendimiento de las implicaciones para la seguridad. A raíz del análisis de los resultados de este estudio se observan cuatro tipologías de empresas:

- Arriesgadas: Este grupo de empresas están moviéndose a cloud, pero poseen un escaso grado de madurez en el ámbito de la seguridad, tal y como refleja su bajo grado de inversión. Están extendiendo cloud a un número creciente de cargas antes de entender los nuevos enfoques de seguridad, lo que las lleva a estar incurriendo en riesgos.

- Seguras: Se trata de aquellas que hacen un uso intensivo de cloud acompañado de políticas adecuadas de seguridad.

- Conservador: Este grupo de empresas, a pesar de invertir por encima de la media en seguridad, son reticentes a utilizar cloud porque no confían en la seguridad o privacidad de cloud pública.

- Inmaduras: Estas empresas tienen poco interés en utilizar cloud pública. Además, tienen un bajo grado de madurez en el área de seguridad, con una inversión inferior a la media.

5.2.1 Migración a cloud y perfiles de seguridad

Como se ha visto en el apartado de prioridades, la seguridad cloud es relativamente importante, pero no mayoritaria en el mercado. Esto representa una oportunidad para que los proveedores se posicionen: el mercado de seguridad en cloud va a crecer inexorablemente, y puede que lo haga de forma repentina, si se produce algún ataque o incidencia a escala.

En este apartado se muestra la ubicación de cada uno de los grupos en función de dos variables: su grado de migración a cloud y su madurez en términos de seguridad. El grupo más destacado es el que se denomina como arriesgado, en el se encuentra el 40% de las empresas analizadas.

Gráfico 10. Migración a cloud y perfiles de seguridad

Fuente: IDG Research, 2019

Las estrategias recomendadas para cada uno de los grupos se presentan a continuación.

5.2.1.1 Segmento arriesgado: mover hacia el seguro

La recomendación estratégica para aproximarse a este segmento consiste en educar al cliente para proteger sus entornos cloud públicos e híbridos. Este grupo de empresas debe asumir que la seguridad en cloud representa un nuevo paradigma. Los aspectos a tener en cuenta son:

- Adoptar la seguridad compartida: establecer una matriz de responsabilidades en función del tipo de cloud pública utilizada para cada servicio.

- Conocer las diferencias entre la gestión, visibilidad y gobierno de los datos on premise y los datos en cloud, dado que en cloud pública las reglas las define el proveedor.

- Prepararse para una gestión multicloud, entendiendo las variaciones en los modelos de operación de cloud que ofrece cada proveedor.

- Alinear las herramientas de gestión del proveedor cloud con las políticas en la empresa.

- Identificar cómo cambia el cumplimiento regulatorio en cloud respecto a on premise.

- Distinguir entre “lift and shift” y la refactorización de una aplicación.

- Fomentar un gobierno robusto antes de subir datos a cloud, para evitar que se trasladen las ineficiencias que puedan existir on premise.

- Asegurar la visibilidad completa de datos en cloud, incluyendo el data discovery. Ya no se trata de responder a un requerimiento judicial, sino a la petición de un cliente.

- Coordinar las responsabilidades sobre cloud y el dato, en el caso en que estén separadas en el organigrama.

5.2.1.2 Segmento seguro: optimizar la inversión en seguridad

En este caso, la estrategia recomendada hacia este segmento consiste en ayudarles a optimizar las inversiones que están realizando. El foco en este grupo de empresas está en orquestar las soluciones para alcanzar una mayor resiliencia de las operaciones. Los aspectos a tener en cuenta son:

- Asegurar que existe un control y visibilidad consistentes de la seguridad en los entornos híbridos
- Seguridad gobernada a lo largo de toda la organización, en particular cuando se trata de una organización descentralizada
- Descubrir el coste total de la seguridad, incluyendo casuísticas como el coste de bajar datos de la nube para protegerlos
- Identificar cómo la seguridad en cloud permite una mejor resiliencia en las operaciones

- Coordinar las responsabilidades sobre cloud y el dato, en el caso en que estén separadas en el organigrama.

5.2.1.3 Segmento inmaduro: concienciar de la “security-first” cuando se muevan a cloud

La estrategia más aconsejable en relación con este segmento consiste en preparar a las empresas para que cuando decidan ir a cloud lo hagan de forma segura. Los aspectos a tener en cuenta son:

- Educar en los nuevos paradigmas de seguridad en cloud.

- Entender los diferentes modelos de cloud pública y sus implicaciones para la seguridad.

- Preparase para operar en un entorno híbrido.

5.2.1.4 Segmento conservador: Aproximación caso a caso

Este segmento es el que tiene más reticencias a migrar cargas a cloud, debido a la desconfianza hacia la seguridad y privacidad de cloud pública. La estrategia que se plantea es un descubrimiento gradual, basado en casos individuales:

- Identificar las oportunidades en cloud que no están disponibles bajo ningún otro modelo tecnológico (ej. analíticas avanzadas, empresas de nicho que solo ofrecen su servicio en modo cloud).

- Plantear casos de uso donde cloud presenta ventajas de agilidad e innovación (ej. experimentación, ensayo y error, lanzamiento de nuevos productos).

5.2.2 Desarrollos en cloud y perfiles de seguridad

El desarrollo seguro en cloud es uno de los aspectos que recibe menos atención en las empresas, dado que tiende a priorizarse la agilidad.

Esta sección muestra la ubicación de cada uno de los grupos en función de dos variables: su grado de desarrollo en cloud y su madurez en términos de seguridad. El grupo más destacado es el que se denomina como conservador, en el que se encuentra el 25% de las empresas analizadas.

Gráfico 11. Desarrollos en cloud y perfiles de seguridad

Fuente: IDG Research, 2019

5.2.2.1 Segmento conservador: Concienciar de cómo cloud permite habilitar DevOps y DevSecOps

La recomendación estratégica para aproximarse a este segmento consiste en educar al cliente en las nuevas metodologías y cómo cloud es el mejor entorno para las mismas.

- Mostrar casos de éxito con métricas de ahorros de tiempo y seguridad.

- Educación en DevOps y DevSecOps apoyadas en cloud.

- Comparativa de casos de negocio y modelos de coste entre desarrollos on-premise y cloud.

- Explorar pilotos a pequeña escala para nuevos desarrollos en cloud.

5.2.2.2 Segmento seguro: Crecer con el cliente – expandir las oportunidades de innovación segura

La estrategia más recomendable hacia este segmento es acelerar el crecimiento en el uso de cloud para los desarrollos.

- Exportar mejores prácticas.

- Documentar los límites de la seguridad compartida en cloud, en particular en áreas como containers.

5.2.2.3 Segmento arriesgado: Introducir la seguridad en los desarrollos, desde el principio del proyecto

La estrategia que se propone para este segmento consiste en ayudar a los responsables de seguridad a ganar visibilidad sobre los nuevos desarrollos y facilitar la incorporación de la seguridad desde el principio.

- Identificar en qué puntos de control del desarrollo pueden establecerse revisiones de seguridad.

- Conocer las implicaciones de coste de introducir seguridad en un desarrollo, en particular si se trata de DevOps - DevSecOps.

- Evaluar críticamente el modelo de externalización, en particular en relación con la securización de desarrollos, y clarificar la asignación de responsabilidades.

5.2.2.4 Inmaduro: Educar al cliente

La estrategia que se plantea hacia este segmento es de sensibilizar al responsable de seguridad y responsables de desarrollo sobre las nuevas metodologías y cómo securizarlas.

- Identificar lagunas de conocimiento:

  . Metodologías ágiles y DevOps
  . Containers y microservicios.

  . Innovación en cloud e innovación por combinación.

  . Desarrollos nativos en cloud.

- Ofrecer modelos como servicio donde el cliente no tenga recursos propios.

6. Percepción de proveedores

Para todas las cargas de trabajo existe ya una alternativa tecnológica de despliegue en cloud. Esto hace que exista una amplia cantidad de proveedores cloud que traen sus propios enfoques hacia el gobierno y la seguridad.

Para proteger los entornos de cloud pública, es importante decidir en qué tipo de proveedor debe apoyarse la empresa. Las opciones van desde operadores hasta integradores, o los propios proveedores del servicio de cloud pública.

Actualmente las empresas están protegiendo su cloud pública mediante una combinación de un equipo interno con los proveedores del servicio cloud. La involucración de otros actores como integradores u operadores para su securización es incipiente. Algunos motivos por los que esto se produce son:

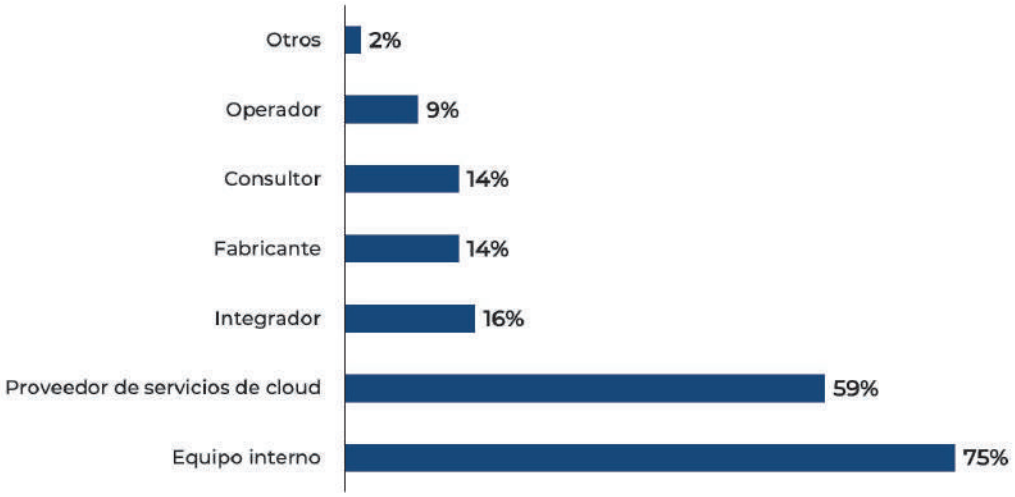
- Riesgo proveedor. Muchos proveedores nativos en cloud han construido su solución sobre otros servicios creando un conjunto de dependencias internas. Su solución consiste en una red compleja de componentes conectados de terceros operando de forma orquestada. Por ejemplo, los proveedores de SaaS a menudo construirán su servicio en las plataformas IaaS existentes. La seguridad requiere entender en detalle las limitaciones de la responsabilidad, incluyendo las políticas de interrupción del servicio, relacionadas con el riesgo proveedor.

- Las decisiones de seguridad se toman a posteriori. La decisión de moverse a cloud no se toma teniendo en cuenta su securización. En consecuencia, las opciones con las que cuenta el departamento de seguridad están condicionadas por una elección de proveedor cloud que ya ha sido realizada.

- Capacidades propias. Algunas empresas cuentan con equipos dedicados a cloud que poseen una visión integrada, pero esto es la excepción. Lo más habitual es que el departamento de seguridad esté compuesto por perfiles no especializados. Esto hace necesario recurrir al conocimiento experto de un partner.

- Grado de madurez cloud. A medida que las empresas vayan avanzando en su transformación, los entornos multicloud van a convertirse en la norma. En este contexto, las capacidades que traen los integradores, consultoras y operadores van a ser necesarias para gestionar la seguridad de estos entornos.

Gráfico 12. Proveedor en el que se apoyan en la adopción de seguridad en cloud.



Fuente: IDG Research, 2019

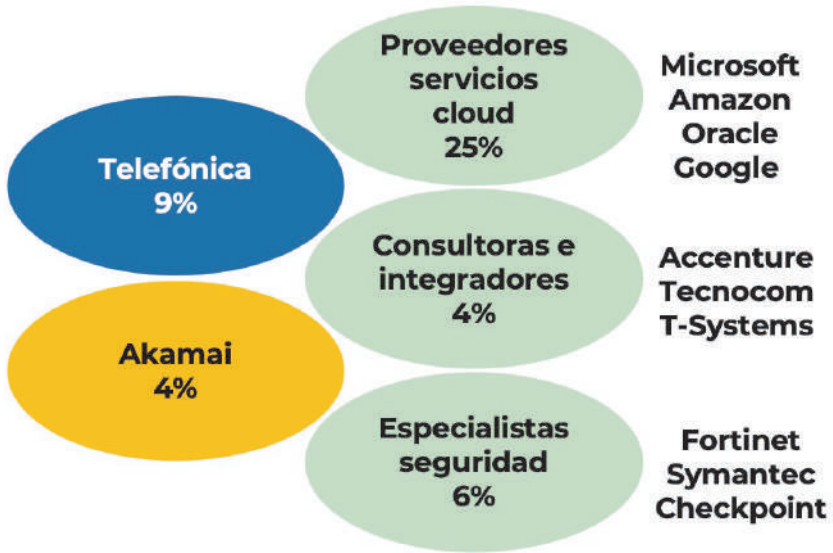
6.1 Percepción sobre Telefónica y Akamai

La percepción tanto de Akamai como de Telefónica es más sólida en las grandes empresas que en las medianas. Existen distintas razones que van desde el posicionamiento de marca en estos segmentos hasta la necesidad de apostar por las soluciones que ofrece cada proveedor.

Por otro lado, existe una alta fragmentación en el mercado de seguridad que incluye a las soluciones de cloud. Los proveedores entran resolviendo un problema específico y aunque crecen ampliando su cartera de soluciones, frecuentemente siguen siendo percibidos en relación con su herencia.

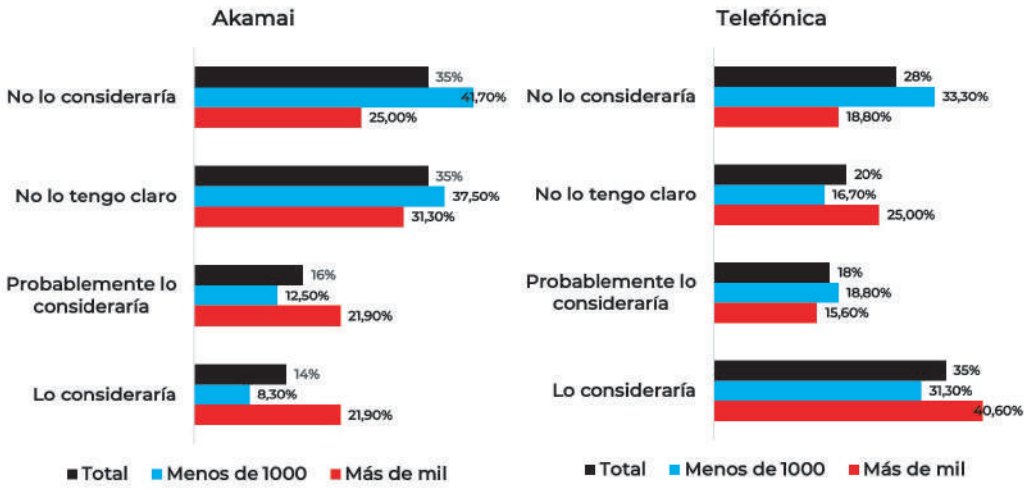
En este contexto, el awareness de las dos empresas es de un 9% en el caso de Telefónica y un 4% para Akamai. Este dato es positivo, dado que a las empresas consultadas se les pedía que nombraran un único proveedor. No obstante, al sumar las respuestas por categorías, los actores nombrados con mayor frecuencia son los proveedores de servicios de cloud. Las menciones a integradores o consultoras son marginales. Por último, hay un grupo significativo que no se decanta por ninguna marca, sino que responde de forma genérica (ej. fabricante).

Gráfico 13. Reconocimiento de proveedores



Fuente: IDG Research, 2019

Gráfico 14. Percepción sobre Telefónica y Akamai



Fuente: IDG Research, 2019

Al ser preguntadas las empresas de forma explícita por su valoración tanto de Telefónica como de Akamai los resultados han sido:

- Telefónica: Las grandes empresas se inclinarían más por Telefónica en comparación con las medianas. No obstante, sigue existiendo un grupo de indecisos significativo. Por último, en el caso de las grandes empresas solo un 19% tienen claro que no consideraría a Telefónica, esta proporción aumenta en las medianas.

- Akamai: Las grandes empresas también tienen mayor inclinación hacia Akamai de lo que lo hacen las medianas. El grupo de empresas indecisas es muy elevado, lo que refleja un mayor desconocimiento de la empresa o su propuesta de valor. Por último, destacar que existe una bolsa de empresas importante entre las medianas que no considerarían a Akamai.

7. Recomendaciones de IDG Research

7.1 Recomendaciones generales

- Antes de ofrecer productos o servicios de seguridad, por parte del proveedor es necesario:

• Determinar la capacidad interna de ejecución de las áreas de seguridad, lo que condicionará qué tipo de soluciones se pueden implementar con éxito.

• Tener en cuenta quién va a ser el usuario final de las soluciones. El departamento TI, el de seguridad o el usuario – y sus necesidades de especialización o formación.

- Las empresas que se encuentran en fases más avanzadas de su transformación digital tienden a incrementar con más rapidez sus inversiones en seguridad. En estas empresas algunas palancas de venta son:

• Soluciones que liberan tiempo del responsable de seguridad de las operaciones para poder dedicarlo a la estrategia.

• Soluciones con una menor inversión global; es decir, incluyendo no sólo el coste de la solución y su implantación sino también costes de formación o concienciación en el usuario final.

La aproximación comercial no puede ser la misma para todas las empresas. Este estudio ha identificado cuatro perfiles de empresas con características homogéneas: proactivas, expansivas, reactivas y que infra-invierten. El objetivo es proporcionar una referencia para identificar a qué grupo pertenece cada empresa, aproximarse de manera diferencial a cada segmento.

7.2 Recomendaciones por segmento

- Segmento proactivo: alinearse con el crecimiento del negocio.
Este segmento de empresa permite mensajes más sofisticados, que miren al futuro y no solo con un enfoque táctico y pragmático.

• Las áreas de crecimiento de la inversión se encuentran en la innovación, en la creación de nuevos servicios y su protección.

• Separar bien qué parte es nueva de la parte existente, más sometida a competencia.

• Alinearse con las prioridades de acceso, entendiendo qué actores lo necesitan (clientes, empleados o terceros), y tener claridad en cómo se alinea con la regulación.

• Entender el impacto de la solución en la organización (o en el cliente final), de forma que se alinee explícitamente con las políticas de seguridad en la empresa. Por ejemplo, puede acelerar un nuevo producto o un proceso de cumplimiento.

- Segmento expansivo: acelerar su evolución para convertirse en proactivo.
En este segmento de empresas, los proveedores deben ser capaces de entender el negocio para facilitar que el responsable de seguridad vincule el producto a los riesgos de negocio en la organización, y no solo a la tecnología:

• Entender las prioridades de negocio, y buscar soluciones fácilmente comunicables a la organización.

• Combinar un entendimiento de las prioridades y necesidades presentes (aplicaciones y dato) con las necesidades futuras (accesos).

• Foco en el responsable de seguridad, liberando recursos y facilitando sus tareas para dedicar más tiempo a la estrategia.

- Segmento reactivo: enfoque pragmático.
En este segmento de empresas la venta debe ir acompañada de un esfuerzo de concienciación para que la seguridad obtenga más recursos.

· Buscar soluciones tácticas a la problemática del día a día.

· Alinearse con la efectividad en proteger la infraestructura y la organización frente amenazas.

· Centrar la propuesta de valor en términos de mayor impacto con la mínima inversión en soluciones.

- Segmento que infra-invierte: venta orientada a coste.
La seguridad está en una segunda fase, primero está la inversión digital. Sector en el que los esfuerzos comerciales son poco rentables, dado que tienen que atravesar un período de maduración. La perspectiva es de medio-largo plazo.

· Buscar productos con proposición de valor sencilla e inmediata y escaso esfuerzo comercial.

· Conocer comparativas de coste frente a productos competitivos.

7.3 Recomendaciones sobre la protección de cloud

Este informe ha puesto de manifiesto que existe un grupo significativo de empresas que están adoptando cloud sin haber internalizado los nuevos paradigmas de seguridad que ello conlleva. Aunque existe una concienciación creciente entre las grandes empresas, todavía es una asignatura pendiente para el grueso del mercado.

Este informe distingue entre dos tipos de oportunidades: migraciones arriesgadas y desarrollos conservadores.

- Migraciones arriesgadas a cloud. En el caso de las migraciones a cloud, un alto porcentaje de empresas están asumiendo riesgos. Este es un nicho de mercado al que deben dirigirse prioritariamente los proveedores:

· Adoptar la seguridad compartida: establecer una matriz de responsabilidades en función del tipo de cloud pública utilizada para cada servicio.

· Detectar las diferencias entre la seguridad on premise y cloud que no ha abordado la empresa en su migración.

· Ofrecer una seguridad homogénea para entornos híbridos, y aplicable a la organización en su conjunto.

- Desarrollos conservadores. Llevar los desarrollos a cloud no es una prioridad entre las empresas analizadas. Prueba de ello es que existe un grupo significativo de empresas que llevando a cabo fuertes inversiones en seguridad no están llevando sus desarrollos a cloud. En este grupo de empresas los proveedores tendrán que:

· Concienciar de cómo cloud permite habilitar DevOps y DevSecOps.

· Mostrar casos de éxito con métricas de seguridad y ahorros de tiempo.

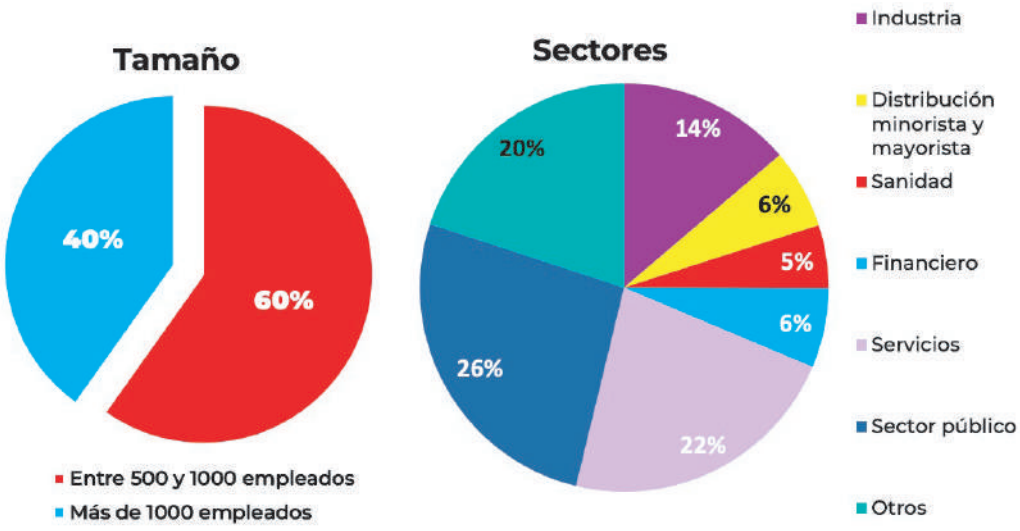
· Plantear pilotos con mínimo riesgo para la empresa.

Anexo 1. Demografía de la muestra

Para la realización de este informe se han llevado a cabo 101 encuestas a empresas de más de 500 empleados. Para ello se realizó un cuestionario estructurado durante el mes de mayo de 2019.

El desglose de las empresas según actividad y tamaño se describe en el siguiente gráfico.

Gráfico 15. Demografía de la muestra de empresas.



Fuente: IDG Research, 2019

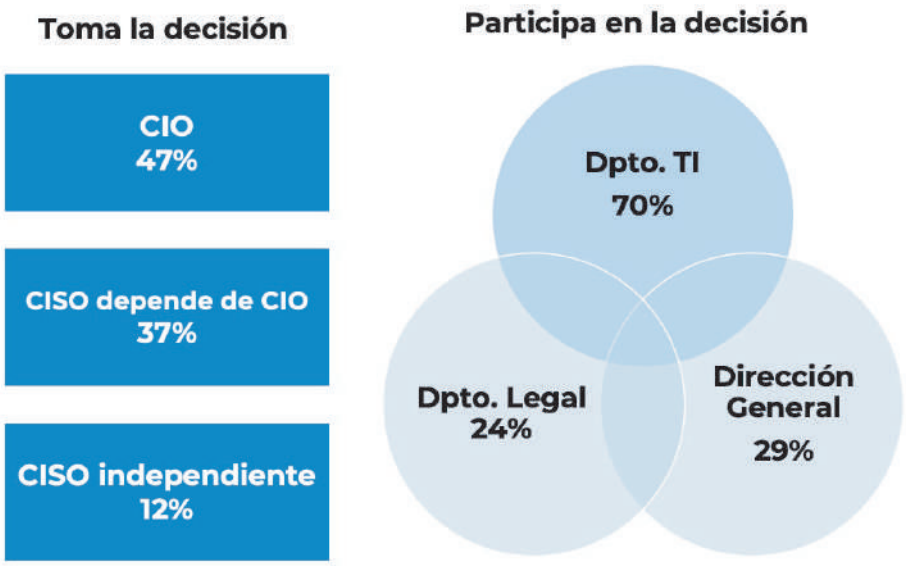
Anexo 2. Decisión sobre el presupuesto

Las decisiones de inversión están mayoritariamente centralizadas alrededor de un responsable de seguridad. Este frecuentemente depende del área de tecnología. Sin embargo, a medida que la seguridad entra en el negocio, la participación de otros departamentos como legal o la dirección general va cobrando relevancia.

En las empresas más avanzadas, la seguridad está saliendo del ámbito de la tecnología para formar parte de la operativa de los negocios digitales. En estas, la seguridad es un pilar sobre el que descansa la confianza del cliente, empleados y partners. No obstante, para la mayoría de las empresas ni los departamentos de seguridad, ni las unidades de negocio han internalizado este hecho. Esto queda recogido por la escasa participación en las decisiones de seguridad de otras áreas distintas a seguridad o IT.

El siguiente gráfico sintetiza la situación actual de las empresas con más de 500 empleados.

Gráfico 16. Toma de decisiones y participación en la misma.



Fuente: IDG Research, 2019

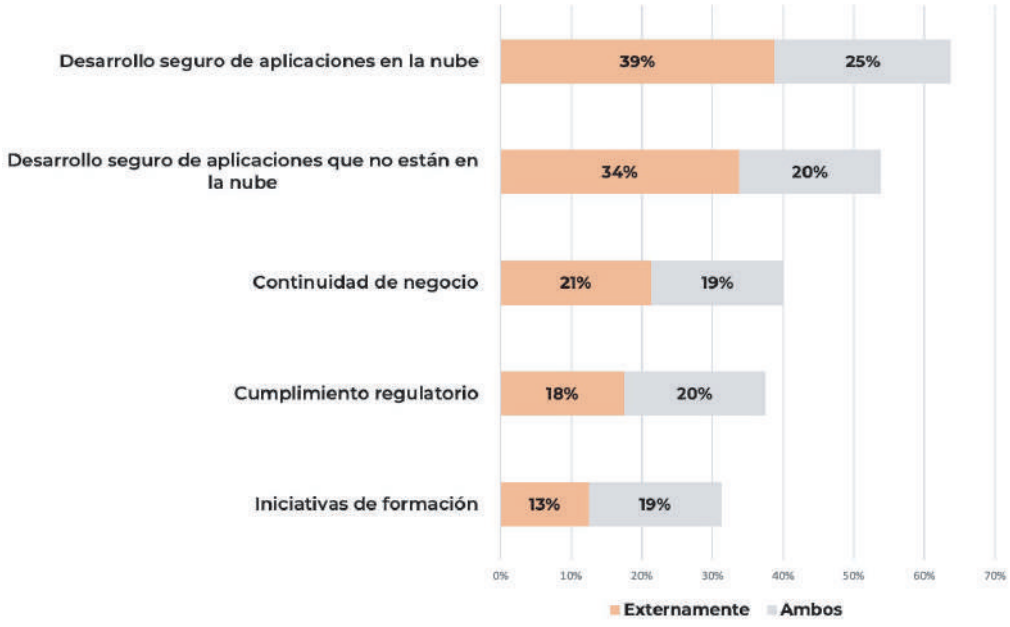
Anexo 3. Propensión hacia la externalización

En general el departamento de seguridad percibe que su actividad es crítica para el negocio y tiene escasa propensión a externalizar. Sin embargo, muchas empresas tienen limitaciones de recursos especializados lo que las obliga a recurrir a terceros. Algo que puede apreciarse en aquellas empresas que infra invierten en seguridad.

Por otro lado, la decisión no siempre está en sus manos. Por ejemplo, cuando está incluida en un contrato de outsourcing más amplio o se accede como servicio. En este sentido, el desarrollo seguro de aplicaciones es una de las áreas en las que existe mayor propensión a externalizar.

Cuando la aplicación está desarrollada por un tercero el papel del departamento de seguridad en el desarrollo está centrado en la revisión y validación de las políticas llevadas a cabo. Mientras que cuando se desarrolla internamente surgen unos retos diferentes: entran en conflicto la necesidad de reducir el tiempo de entrega con la necesidad de securizar. Aquí las metodologías ágiles priman la velocidad y no tienen integrada la seguridad. Prueba de ello es que metodologías como DevSecOps son muy incipientes.

Gráfico 17. Áreas con propensión a externalizar.



Fuente: IDG Research, 2019

SEGURIDAD en CLOUD

Alberto Belle
Fernando Maldonado
@FmaldonadoF

Analistas principales de
IDG Research
@IDGResearch_ES

© Todos los contenidos, textos e imágenes son propiedad de IDG COMMUNICATIONS, S.A.U. o de terceros a los que se han adquirido sus derechos de explotación, y están protegidos por los derechos de Propiedad Intelectual e Industrial. El usuario únicamente tiene derecho a un uso privado de los mismos, sin ánimo de lucro, y necesita autorización expresa para modificarlos, reproducirlos, explotarlos, distribuirlos o ejercer cualquier derecho perteneciente a su titular.

IDG
RESEARCH SERVICES
Calle Velázquez, 105 - 5ª planta
28006 Madrid
Teléfono +3491 349 6600
research@idg.es