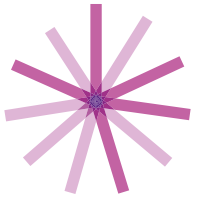
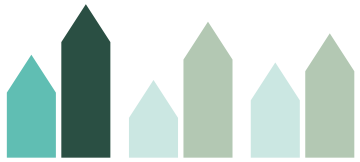
EL IMPERATIVO DE LA SEGURIDAD:
PROMOVER EL CRECIMIENTO DEL NEGOCIO EN LA ECONOMÍA DE LAS APLICACIONES >>

Con el patrocinio de ca technologies

COLEMAN PARKES RESEARCH

Índice





CÓMO USAR ESTE DOCUMENTO PDF INTERACTIVO

El grado de interactividad, que depende de su lector de PDF, varía entre tablets y smartphones. Es posible que las opciones interactivas no funcionen si abre el documento PDF en el modo de previsualización del correo electrónico. Le recomendamos que use Adobe Acrobat Reader.

INICIO (primera página) | **ÍNDICE** | **RETROCEDER** una página | **AVANZAR** una página

Resumen ejecutivo

La economía de las aplicaciones ha transformado el rostro de la seguridad en el campo de las TI. La línea divisora que separa el interior de la empresa del exterior ha quedado prácticamente disuelta. El perímetro de las redes corporativas no solo se ha movido, sino que se ha fragmentado. La nueva frontera de la seguridad se traza allí donde los usuarios deciden acceder a su red.

Sin embargo, este no es el único problema. Clientes, empleados y partners esperan disfrutar de acceso sin problemas, a todas horas y en todo lugar, sea cual sea el tipo de dispositivo o plataforma que usen.

Ante la complejidad del panorama, las estrategias convencionales de TI sobre seguridad ya no son válidas. Las organizaciones necesitan ser capaces de verificar la autenticidad de identidades muy distribuidas, procedentes de diversos orígenes, sin por ello causar fricciones en la experiencia que disfrutan los usuarios. Es preciso alcanzar un delicado equilibrio entre la firmeza de la protección y la satisfacción de los usuarios. Por eso es necesario adoptar un nuevo enfoque para la seguridad, centrado en la identidad. Un enfoque que se sirva del contexto, del análisis de comportamientos y de enfoques más predictivos para proporcionar una experiencia convincente al cliente, al tiempo que protege datos e identidades.

En última instancia, la seguridad centrada en la identidad permite forjar relaciones digitales de confianza con sus clientes, lo que constituye el mejor activo para el negocio dentro de las economía de las aplicaciones.

Teniendo esto en cuenta, CA Technologies encargó a Coleman Parkes Research que llevase a cabo una encuesta entre 1770 ejecutivos sénior corporativos y de TI, entre los que figuraban más de 100 directores de seguridad y directores de seguridad de la información. Les preguntamos acerca de sus prácticas de seguridad para las TI y el grado de adopción de los elementos clave dentro del concepto de seguridad centrada en la identidad.

Así nos fue posible identificar en qué se distingue la manera de actuar de los usuarios avanzados de la seguridad centrada en identidades y saber qué efectos tiene la seguridad sobre sus actividades.

Nuestros hallazgos hablan con claridad a favor de adoptar un nuevo modelo de seguridad digital, acorde con las demandas de la economía de las aplicaciones y capaz de promover mejoras tangibles que se reflejen en la rentabilidad.

La seguridad centrada en la identidad permite forjar relaciones digitales de confianza con sus clientes, lo que constituye el mejor activo para el negocio dentro de las economía de las aplicaciones.

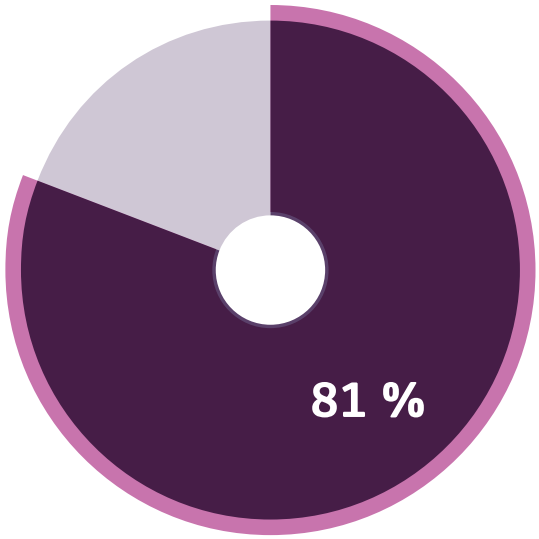
Esto es lo que reveló el análisis:

- **El 81 %** de las empresas admite que las necesidades de seguridad no deben provocar problemas ni estorbos, para evitar imponer a los usuarios requisitos demasiado molestos relacionados con la seguridad.
- **El 82 %** afirma que la seguridad centrada en la identidad es fundamental para sus actividades empresariales, pero **solo el 25 %** se pueden considerar usuarios avanzados de enfoques para la seguridad centrados en la identidad.
- En comparación, entre los usuarios avanzados del concepto de seguridad centrada en la identidad hay el doble de encuestados que han constatado una reducción de las infracciones de datos que entre los usuarios de conceptos básicos: **el 41 % frente al 21 %**.
- **El 91 %** de los usuarios avanzados de la seguridad centrada en la identidad han constatado una mejora de su alcance digital; el **87 %** en la experiencia del cliente y el **87 %** en la retención de clientes.
- Los usuarios avanzados de seguridad centrada en la identidad también afirman haber experimentado mejoras cuantificables en los resultados empresariales:
  - **El 47 %** confirma una mejora en el crecimiento del negocio.
  - **El 50 %** confirma una mejora en la productividad de los empleados.
  - **El 45 %** confirma una mejora en la satisfacción de los clientes.

"La seguridad es el principal motor de nuestro avance digital".

Director de tecnología, entidad gubernamental de EE. UU.

El **81 %** de las empresas admite que las necesidades de seguridad no deben provocar problemas ni estorbos, para evitar imponer a los usuarios requisitos demasiado molestos relacionados con la seguridad.



Introducción: Una nueva frontera

La revolución digital ha desplazado (y continúa desplazando) los objetivos de seguridad de las TI. Ha creado un mundo donde conviven múltiples canales, plataformas y dispositivos. Un panorama donde sus clientes, partners y empleados están siempre conectados y esperan que usted también lo esté.

Actualmente, inmersos en la economía de las aplicaciones, los clientes esperan descargas veloces, acceso rápido, experiencias sencillas, sin interrupciones y una protección robusta. Si las medidas de seguridad que les propone les ralentizan, abandonarán su empresa y podrían llevarse el negocio a otro lado si no logra proteger sus datos.

El antiguo perímetro de la red ha desaparecido. La gente accede a la red desde cualquier lugar y en el momento que prefiere, desde la plataforma o el dispositivo que más le guste. Desde ya, es la identidad del usuario y no los cortafuegos la que constituye la frontera en la batalla por proteger los datos.

Por tanto, para triunfar, se exige que exista una relación bidireccional y de confianza entre el usuario y el negocio.

Se trata de un clima que requiere una visión de la seguridad más centrada en la identidad, que sitúe la identidad del usuario en el centro de los focos. El concepto de seguridad centrada en la identidad utiliza el contexto, el análisis de comportamientos y enfoques de seguridad más predictivos para verificar que los usuarios realmente son quienes afirman ser. Eso les permitirá acceder sin peligros a los datos de su empresa desde el dispositivo que prefieran, donde y cuando quieran.

"La seguridad es uno de los grandes obstáculos para cumplir las exigencias de velocidad que plantean los clientes".

Director de TI, asociación gubernamental de ámbito local de EE. UU.

La gente accede a la red desde cualquier lugar y en el momento que prefiere, desde la plataforma o el dispositivo que más le guste.

Sin embargo, la seguridad centrada en la identidad es algo más que un mero método eficaz para proteger datos. Si se aplica correctamente, puede ser un valioso impulsor del negocio. Le puede habilitar para ofrecer nuevos servicios con más rapidez. También abre la puerta a incrementar la implicación de los clientes y su fidelidad, dos ingredientes que dependen de la confianza. Y en un mundo digital, la seguridad es el principal motor de la confianza.

"La seguridad centrada en la identidad va a erigirse en el principal enfoque de la seguridad entre las compañías de telecomunicaciones".

Director de marketing, proveedor europeo de servicios de telecomunicaciones

Como parte de nuestro estudio de investigación para observar cómo trabajan las empresas para transformarse y adaptarse a la era digital, hemos examinado sus esfuerzos por adoptar un enfoque de la seguridad más centrado en la identidad. Hemos preguntado a ejecutivos que ocupan puestos directivos, a responsables de TI y seguridad de todo el mundo acerca de:

- Sus percepciones sobre la seguridad como elemento impulsor de las oportunidades de negocio.
- Los indicadores clave de rendimiento (KPI) esenciales que emplean para evaluar el impacto de la seguridad de las TI y qué resultados han constatado.
- La adopción de la seguridad centrada en la identidad, requisito para la economía de las aplicaciones.
- De qué manera afecta una aplicación más avanzada de la seguridad centrada en la identidad al rendimiento del negocio.

Este informe resume la información que hemos recabado. Profundiza en cómo pueden hacer evolucionar las organizaciones su seguridad para las TI con el fin de fomentar mejores resultados, ganar competitividad e incrementar el crecimiento dentro de la economía de las aplicaciones.

La seguridad centrada en la identidad es algo más que un mero método eficaz para proteger datos. Si se aplica correctamente, puede ser un valioso impulsor del negocio.

01. El estado de la seguridad en la economía de las aplicaciones

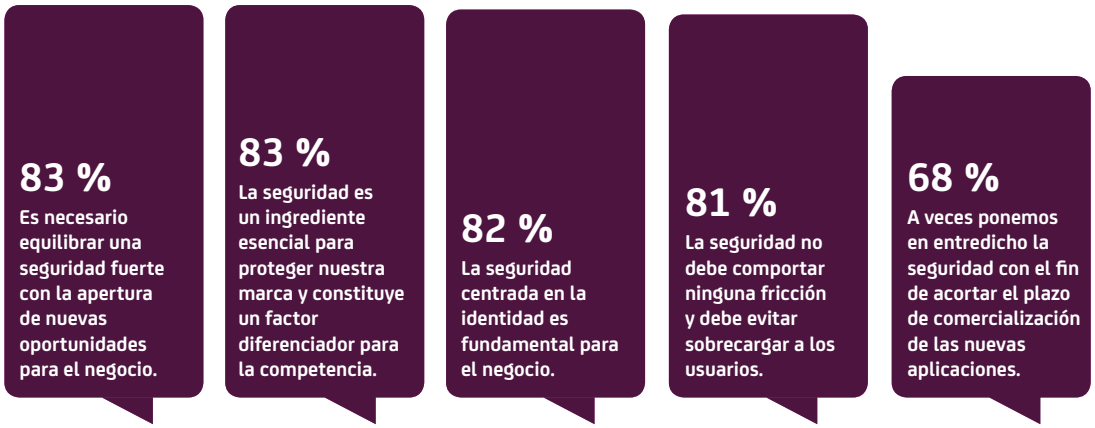
Nuestro estudio de investigación sugiere que las organizaciones reconocen cuál es el papel que puede desempeñar la seguridad en el actual entorno empresarial. Siguen focalizando su atención en los objetivos convencionales de la seguridad, como la protección contra infracciones y la garantía de la conformidad normativa. Pero al mismo tiempo, quienes respondieron a nuestra encuesta consideran que la seguridad también representa una oportunidad para expandir sus negocios y competir con más eficacia en la economía de las aplicaciones.

Más de cuatro quintas partes de los encuestados aceptan que la seguridad puede hacer realidad nuevas oportunidades de negocio, proporcionar una ventaja competitiva y brindar a empleados y clientes el acceso rápido, práctico y siempre disponible del que esperan disfrutar (véase la figura 1).

Esto se refleja en los indicadores clave de rendimiento (KPI) utilizados para evaluar el impacto de la seguridad en las TI. Es tan probable que se utilicen las métricas que miden el rendimiento del negocio (como el alcance digital, la experiencia y la satisfacción del cliente) o incluso más probable que las mediciones convencionales sobre la seguridad, como las infracciones y los malos resultados en las auditorías sobre conformidad con las normativas (véase la figura 2).

Más de cuatro quintas partes de los encuestados aceptan que la seguridad puede hacer realidad nuevas oportunidades de negocio, proporcionar una ventaja competitiva y brindar a empleados y clientes el acceso rápido, práctico y siempre disponible del que esperan disfrutar.

FIG. 1 LA ECONOMÍA DE LAS APLICACIONES REQUIERE QUE SE ADOPTE UN NUEVO PAPEL PARA LA SEGURIDAD, EN CALIDAD DE FACTOR IMPULSOR DEL NEGOCIO.



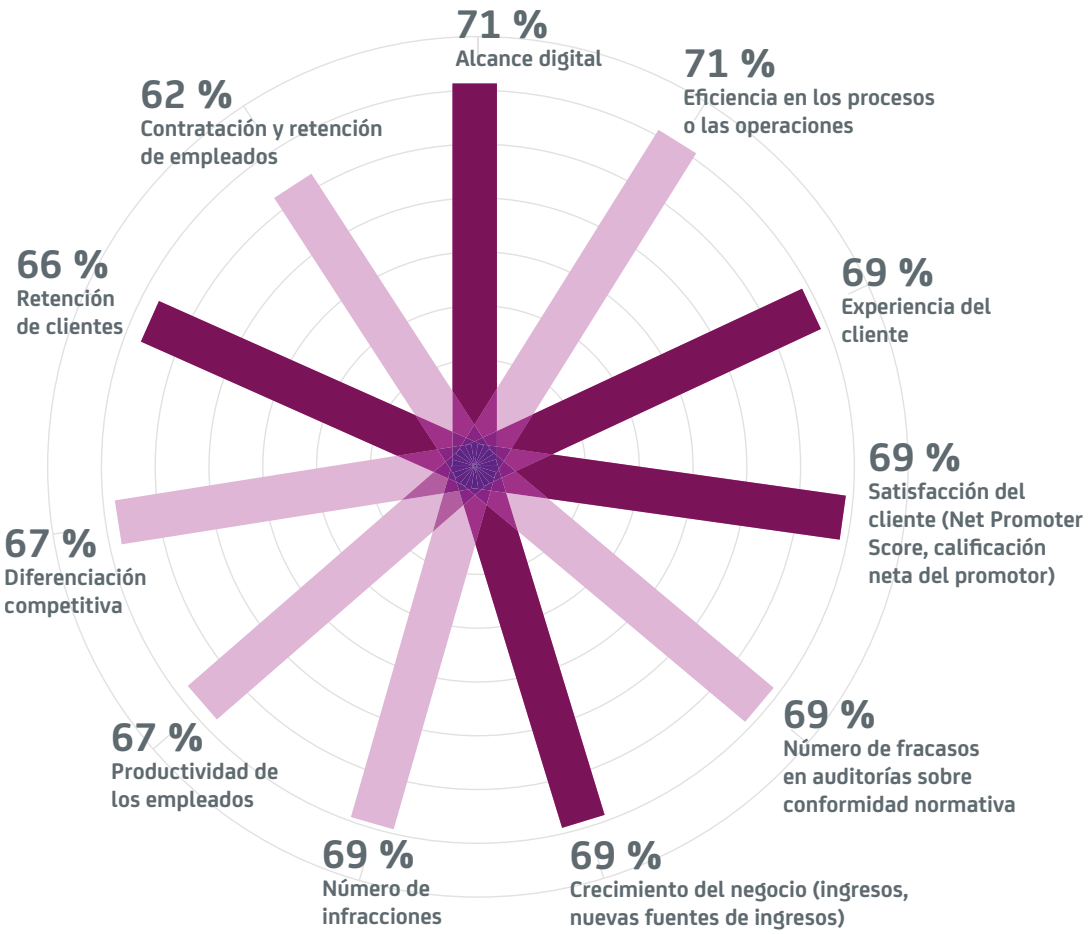
"Existe un tira y afloja entre, por un lado, una seguridad robusta y por otro lado, las interfaces de clientes y empleados".

Director de TI, asociación gubernamental de ámbito local de EE. UU.

Está claro que las empresas aprecian la seguridad en las TI como un factor impulsor fundamental para el negocio, además de como un medio de proteger los datos. Sin embargo, muchas deciden tomar atajos ante la presión de la economía de las aplicaciones. Un preocupante 68 % admite que pone entredicho la seguridad para hacer llegar sus aplicaciones al mercado más rápidamente.

Rebajar la prioridad que se otorga a la seguridad en la economía de las aplicaciones supone un grave riesgo. Gestionar identidades y accesos en miles de aplicaciones, servicios y dispositivos exige adoptar un enfoque mucho más sofisticado para proteger las identidades y los datos que los enfoques necesarios anteriormente.

FIG. 2 LAS MÉTRICAS EXTERNAS SOBRE LA ACTIVIDAD EMPRESARIAL FIGURAN ENTRE LOS PRINCIPALES INDICADORES CLAVE DEL RENDIMIENTO QUE SE USAN PARA MEDIR EL IMPACTO DE LA SEGURIDAD EN LAS TI.



02. Un nuevo enfoque de la seguridad

Ante la economía de las aplicaciones, el desafío consiste en verificar identidades muy distribuidas procedentes de un variado catálogo de fuentes, que incluye aplicaciones, sistemas, la nube y plataformas de redes sociales.

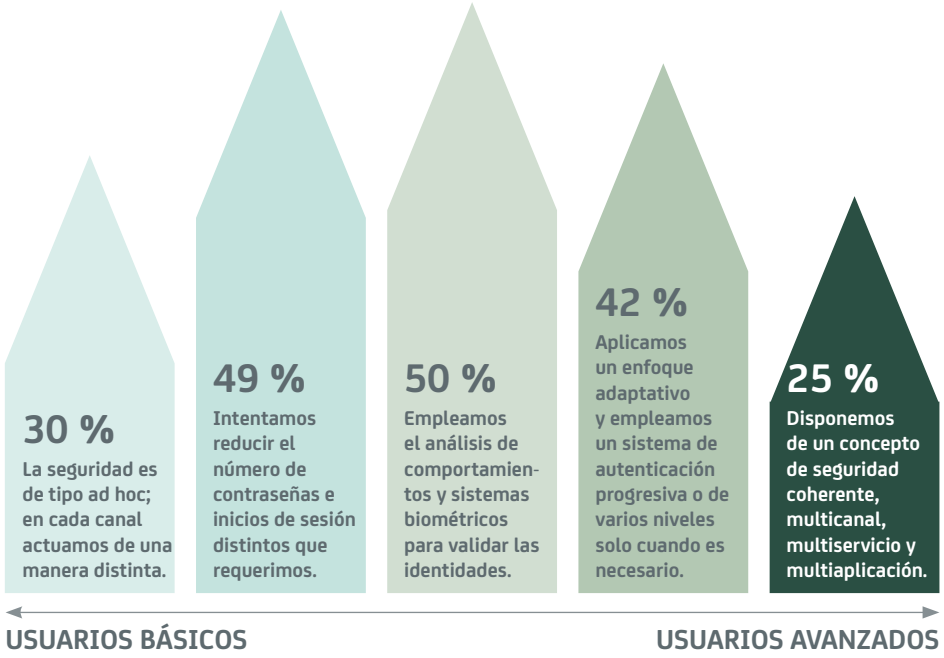
Ahora bien, hay que hacerlo sin que lo vean los usuarios. Los clientes ansían disfrutar de una experiencia a prueba de riesgos y libre de estorbos. Unos procesos de registro y autenticación incoherentes y torpes les desanimarán de inmediato y dificultarán los esfuerzos por entablar relaciones digitales fundamentadas en la confianza.

La seguridad centrada en la identidad constituye un enfoque que contribuye a garantizar que sus prácticas de seguridad no repercutan negativamente sobre la experiencia general que viven los usuarios. Asimismo, requiere que se decante por controles de IAM (gestión de identidades y accesos) más adaptables y asuma un enfoque más proactivo y predictivo para prevenir y detectar las infracciones de datos.

Hemos creado un modelo de madurez para evaluar el grado de adopción y utilización actual de tres elementos claves de la seguridad centrada en identidades por parte de las organizaciones:

1. **Experiencia del cliente** (véase la figura 3). Enfoques coherentes y multicanal de la seguridad, sirviéndose de análisis de comportamientos y técnicas de adaptación, que darán como resultado un sistema de seguridad menos intrusivo. Tan solo una de cada cuatro empresas utiliza un concepto de seguridad coherente, multiaplicación, multidispositivo y multicanal con el fin de mantener un alto nivel de calidad en la experiencia que ofrece a los clientes. Una minoría (el 42 %) adopta un enfoque adaptativo, mientras que la mitad sí explota el análisis de comportamientos.

FIG. 3 LOS ENFOQUES MULTICANAL Y COHERENTES DE LA SEGURIDAD IMPULSAN LA MEJORA DE LA EXPERIENCIA DE CLIENTE, PERO POCAS EMPRESAS ESTUDIADAS LOS HAN LOGRADO.



"La seguridad debe presentar un rostro más amable para el usuario, sin sacrificar su solidez. La clave es asegurarnos de que podemos verificar si un usuario es un cliente, un empleado o un hacker, de que podemos proteger los datos de clientes y empleados y garantizar que las transacciones no sufran inconvenientes".

Vicepresidente de tecnología y conformidad normativa, corporación bancaria de EE. UU.

2. **Gestión de accesos e identidades** (véase la figura 4). La seguridad centrada en la identidad también requiere un enfoque más adaptativo de los controles de IAM (gestión de accesos e identidades). Casi el 70 % dispone de controles de IAM centralizados y automatizados, pero solamente una de cada 10 empresas pueden adaptarlos para responder a los riesgos.

"En el futuro, la gestión de accesos e identidades será el principal motivo de preocupación para la seguridad".

Director de marketing, proveedor europeo de servicios de telecomunicaciones

3. **Detección de infracciones** (véase la figura 5): Los procesos proactivos y predictivos pueden mejorar en gran medida la capacidad de una organización para detectar y prevenir las infracciones de datos. No obstante, solo el 37 % utiliza el análisis para detectar y prevenir de forma proactiva las infracciones de datos. Menos de la mitad de ese grupo (el 16 %) puede predecir el riesgo de infracciones antes de que ocurran.

Tras plantear a los participantes cuestiones sobre estos tres ingredientes de la seguridad centrada en la identidad, calificamos sus respuestas. Tomando esos resultados como base, agrupamos sus organizaciones por categorías, como usuarias avanzadas, básicas o limitadas de la seguridad centrada en la identidad.

Lo que nos encontramos es que solamente el 25 % de las empresas se clasifican como usuarias avanzadas. La mayor proporción, con mucho, es la representada por las empresas que son usuarias básicas (64 %), mientras que el 11 % disponen únicamente de capacidades centradas en la identidad que son limitadas... o directamente inexistentes.

FIG. 4 LOS CONTROLES DE GESTIÓN DE ACCESOS E IDENTIDADES CON NATURALEZA ADAPTATIVA MEJORAN LA SEGURIDAD CENTRADA EN LA IDENTIDAD, PERO POCAS DE LAS ENTIDADES ESTUDIADAS LOS HAN ADOPTADO.

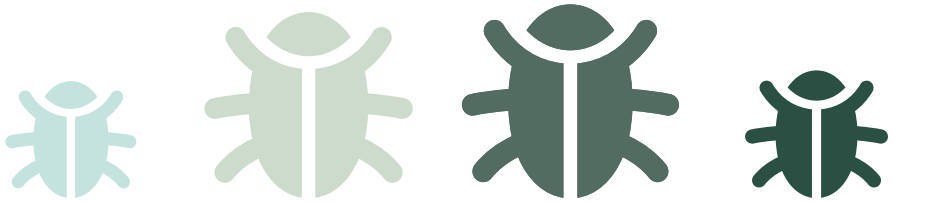
20 %
Controles predominantemente manuales

69 %
Controles predominantemente centralizados y automatizados

11 %
Controles de tipo adaptativo basados en los riesgos

USUARIOS BÁSICOS — **USUARIOS AVANZADOS**

FIG. 5 LOS ANÁLISIS PROACTIVOS Y PREDICTIVOS AYUDAN A DETECTAR Y PREVENIR LAS INFRACCIONES DE DATOS, PERO POCAS DE LAS ENTIDADES ENCUESTADAS LOS UTILIZAN.



13 %
Revisión ocasional, solamente de las notificaciones sobre actividades

34 %
Análisis parcial con funciones de alertas y notificación inteligentes

37 %
Enfoque proactivo: análisis en profundidad con respuesta en tiempo real ante eventos e incidentes

16 %
Enfoque predictivo: capacidad para prever los riesgos antes de que se produzca una infracción

USUARIOS BÁSICOS — **USUARIOS AVANZADOS**

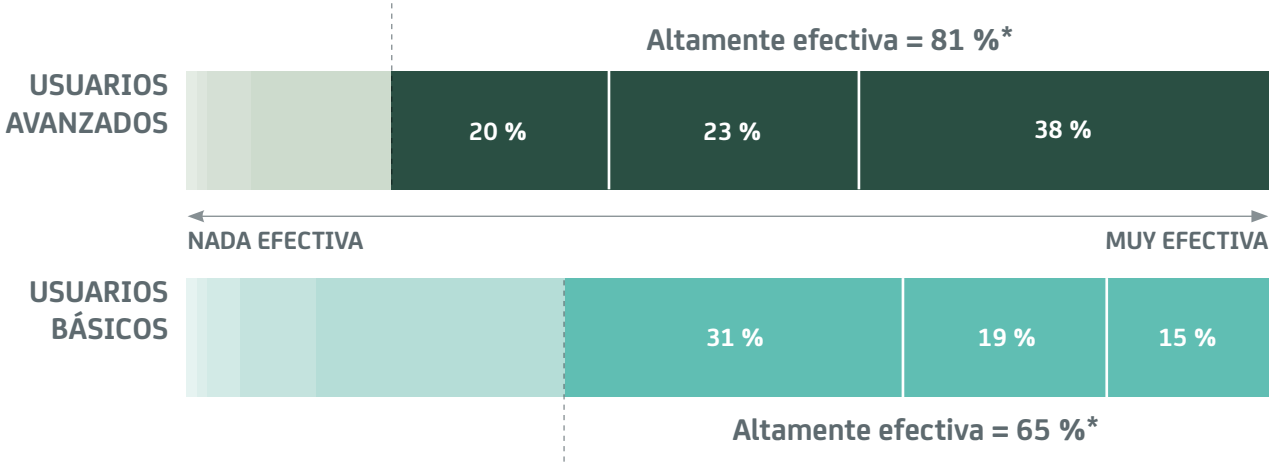
03. Impacto significativo sobre el negocio de la seguridad centrada en la identidad

La siguiente etapa de nuestro análisis consistía en comprobar si existía una correlación entre la utilización madura de la seguridad centrada en la identidad y los resultados comerciales. Para ello, comparamos el comportamiento del negocio entre los usuarios básicos y avanzados.

Nuestro análisis observó que entre los usuarios avanzados de la seguridad centrada en la identidad es mucho más probable creer que la seguridad les diferencia de los competidores- Cerca del 81 % afirma que su estrategia de seguridad es diferenciadora, en comparación con el 65 % entre los usuarios básicos (véase la figura 6).

Los usuarios avanzados también conceden un nivel de prioridad muy superior a todos los objetivos de seguridad por los que preguntamos (véase la página 8). Lo más significativo es que son mucho más propensos que los usuarios básicos a aprovechar la seguridad como herramienta habilitadora de nuevas iniciativas de negocio y relaciones comerciales (el 55 % frente al 34 %).

FIG. 6 LA SEGURIDAD CENTRADA EN LA IDENTIDAD POTENCIA LA DIFERENCIACIÓN RESPECTO DE LA COMPETENCIA.

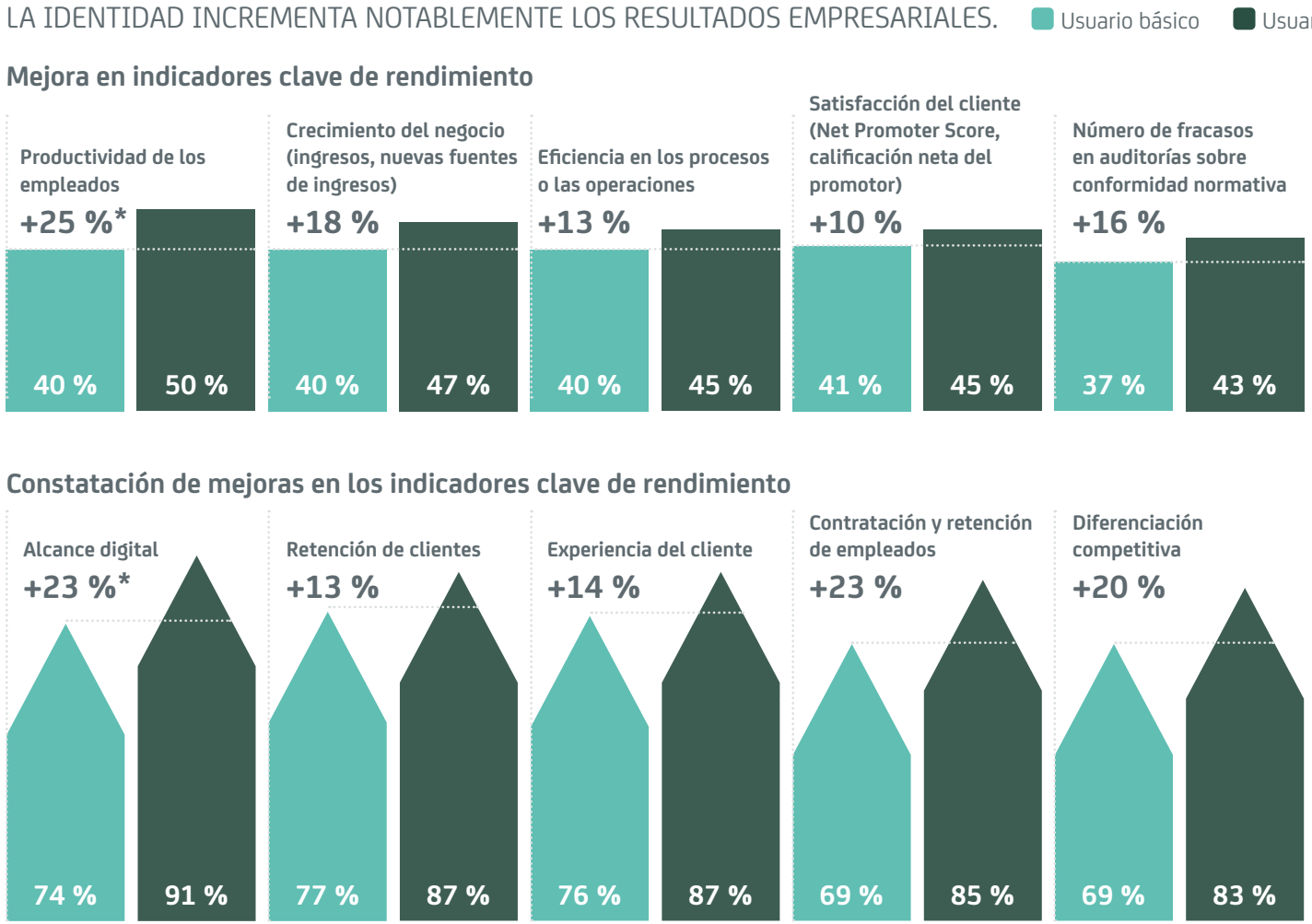


* % Calculado con las tres calificaciones más altas sobre 10, donde 10 es “Muy efectiva” y 1 es “Nada efectiva”

Al fijarnos en el impacto de la seguridad de las TI sobre los indicadores claves de rendimiento empleados para evaluarlo, obtuvimos una imagen similar. Los usuarios avanzados del concepto de seguridad centrada en la identidad señalan más mejoras en todas las medidas de seguridad y empresariales por las que preguntamos.

Los diferenciales entre los usuarios avanzados y los básicos oscilan entre el 10 % hasta nada menos que el 25 % (véase la figura 7). Por ejemplo, el 87 % de los usuarios avanzados anuncian una mejora significativa de la experiencia del cliente, frente a tan solo el 76 % de los usuarios básicos. En el ámbito de contratación y retención de empleados se registra un impacto aún mayor: el 85 % de los usuarios avanzados constatan la existencia de una mejora, en comparación con tan solo el 69 % de los usuarios básicos.

FIG. 7 EL PASO DEL USO BÁSICO AL AVANZADO DE LA SEGURIDAD CENTRADA EN LA IDENTIDAD INCREMENTA NOTABLEMENTE LOS RESULTADOS EMPRESARIALES.



* % de mejora en los indicadores clave de rendimiento al pasar de un usuario básico a uno avanzado

En términos de protección de datos, mientras cerca de un tercio de todos los usuarios sigue observando cómo aumentan las infracciones de seguridad, resulta significativo que para los usuarios avanzados sea casi el doble de probable haber experimentado una reducción del número de infracciones de datos sufridas, en comparación con los usuarios básicos. Dos quintas partes (el 41 %) de los usuarios avanzados lo consiguieron el año pasado, a pesar de estar inmersos en un clima cada vez más complicado para la seguridad. Compárese este dato con el 21 % (menos de la cuarta parte) de los usuarios básicos (véase la figura 8).

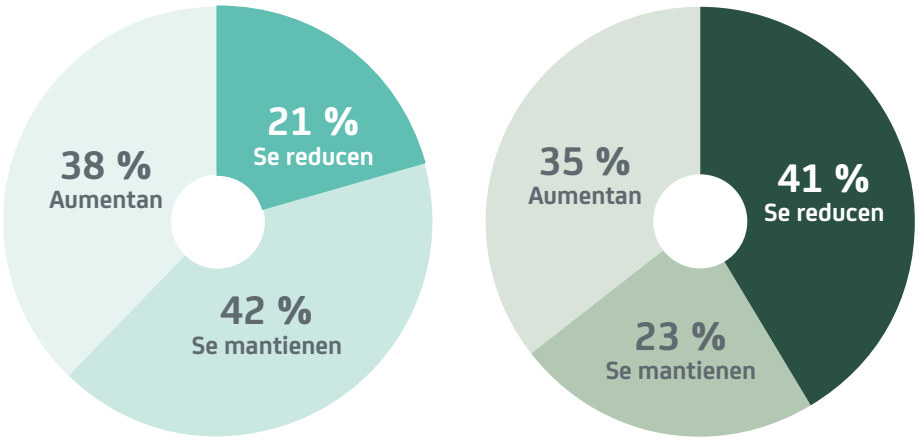
Tarjeta de puntuación del impacto de la transformación digital sobre el negocio

También evaluamos el impacto de la seguridad centrada en la identidad sobre los proyectos de transformación digital de las entidades participantes en el estudio.

Para ello, usamos la Tarjeta de puntuación del impacto de la transformación digital sobre el negocio, que concebimos como parte de nuestro estudio sobre los esfuerzos de transformación digital de las empresas. La Tarjeta de puntuación evalúa el efecto general de las iniciativas digitales de las organizaciones, de acuerdo con 14 indicadores claves de rendimiento del mundo de la empresa, que son esenciales para lograr una transformación con éxito.

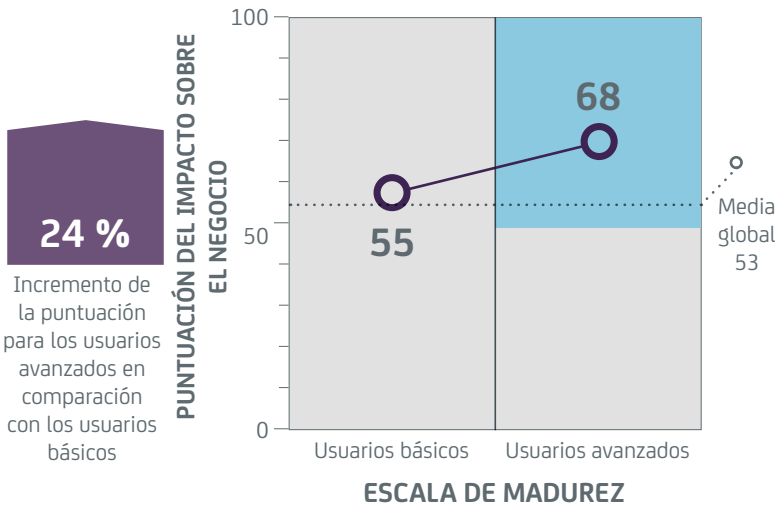
Hemos comparado los resultados de la Tarjeta de puntuación correspondiente a usuarios básicos y avanzados del concepto de seguridad centrada en la identidad. La puntuación media de los usuarios avanzados fue de 68 sobre un máximo de 100, comparado con tan solo el 55 para los usuarios básicos. Esto arroja una mejora del 24 % (véase la figura 9).

FIG. 8 EL PASO DEL USO BÁSICO AL AVANZADO DE LA SEGURIDAD CENTRADA EN LA IDENTIDAD REDUCE LAS INFRACCIONES DE DATOS.



Porcentaje de empresas que constatan que las infracciones de datos han aumentado, se han mantenido o se han reducido.
(Los porcentajes no suman 100 en total debido al redondeo)

FIG. 9 EL USO AVANZADO DE LA SEGURIDAD CENTRADA EN LA IDENTIDAD INCREMENTA LOS RESULTADOS EMPRESARIALES DE LA TRANSFORMACIÓN DIGITAL.



04. Lecciones de los usuarios avanzados de la seguridad centrada en la identidad

El mensaje está claro: las empresas que han adoptado la seguridad centrada en la identidad y la aplican con madurez fomentan el crecimiento de sus beneficios en todos los aspectos. Entonces, ¿qué es lo que hacen para lograr que su seguridad sea mucho más efectiva?

En primer lugar, se toman la seguridad en las TI mucho más en serio: el 81 % invierte más en la prevención de las infracciones, en comparación con el 55 % de los usuarios básicos. Además, son menos propensos a tomar atajos: el 58 % de los usuarios avanzados sacrifican la seguridad para lograr que sus aplicaciones lleguen más rápidamente al mercado, en comparación con el 70 % de los usuarios básicos.

También es más probable que hagan uso de lo que se conoce como "DevSecOps". La mayoría de los usuarios avanzados de la seguridad centrada en la identidad (el 54 %) aplica esta práctica, en comparación con el 33 % de los usuarios básicos.

DevSecOps es un ingrediente crucial en la economía de las aplicaciones. Cuando su negocio depende de la tecnología digital, no vale incorporar las funciones de seguridad a sus aplicaciones a última hora. De una manera similar al concepto DevOps, que integra las operaciones de TI en una fase más temprana del ciclo de desarrollo del software, DevSecOps adelanta la seguridad a una etapa más adelantada del proceso de desarrollo. Así se garantiza que sus aplicaciones la incorporen desde el primer instante.

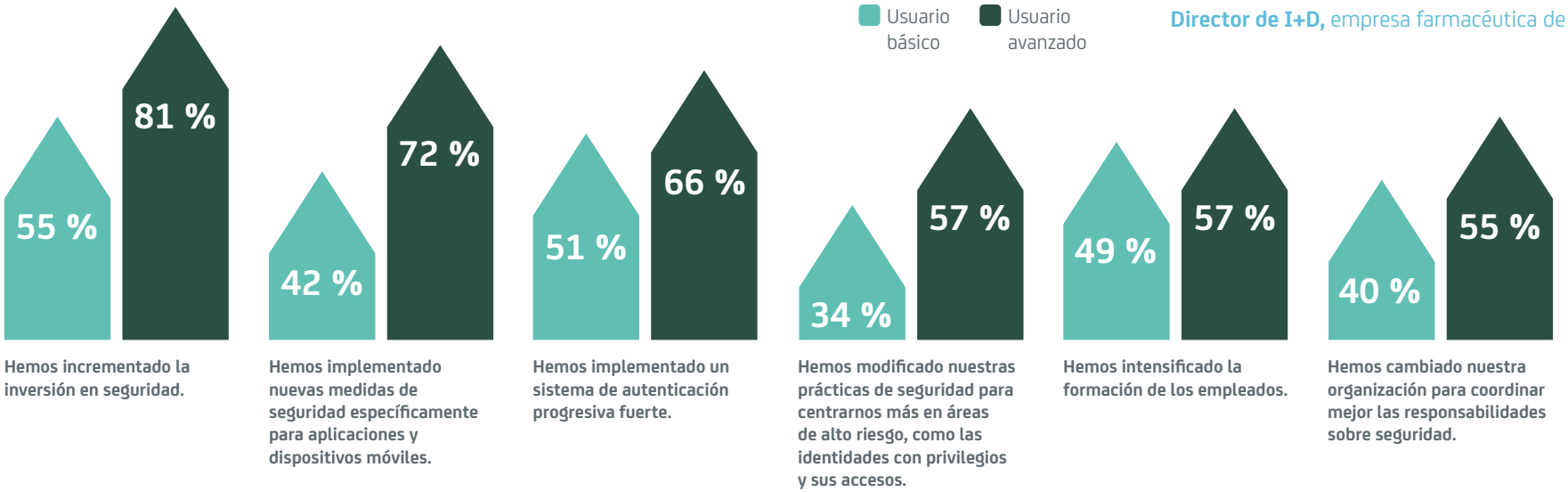
Finalmente, los usuarios avanzados hacen más por coordinar su enfoque de cara a la prevención de infracciones con las realidades que impone la economía de las aplicaciones (véase la figura 10).

Es bastante más probable que implementen soluciones de seguridad específicas para aplicaciones y dispositivos móviles (el 72 % frente al 42 %); que reconfiguren las prácticas de seguridad para proteger áreas de alto riesgo, como las identidades con privilegios (el 57 % frente al 34 %); que implementen un sistema de autenticación progresiva fuerte (el 66 % frente al 51 %) y que reestructuren el negocio para reforzar la responsabilidad respecto a la seguridad (el 55 % frente al 40 %).

"Nuestro mayor dolor de cabeza en relación con la seguridad es que ahora todo el mundo dispone de acceso remoto. Durante los dos años pasados, nuestros responsables de seguridad para las TI se han centrado en la autenticación".

Director de I+D, empresa farmacéutica de EE. UU.

FIG. 10 MOTIVOS PARA EL DECLIVE DE LAS INFRACCIONES DE SEGURIDAD

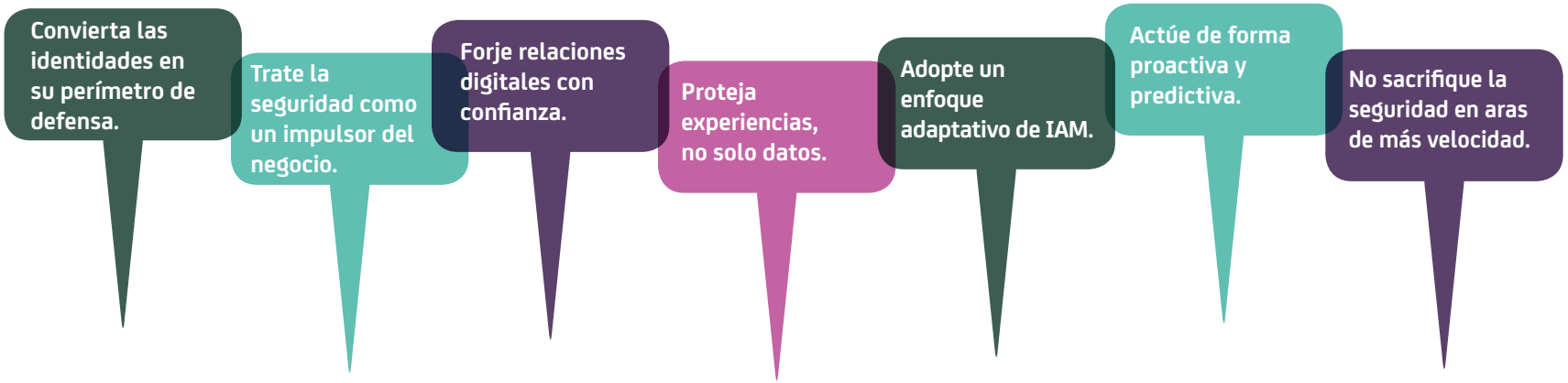


05. Seguridad efectiva centrada en la identidad: hoja de ruta

Nuestro estudio propugna con rotundidad las ventajas que reportaría a la empresa decantarse por el enfoque de la seguridad centrado en la identidad. ¿Pero cómo empezar? ¿Cómo se consigue que funcione en su caso? ¿Y cómo es posible asegurarse de que mejore los resultados y estimule el crecimiento?

Por experiencia propia, sabemos que las siguientes medidas son cruciales para implementar con éxito un concepto de seguridad centrado en la identidad:

1. **Convierta la identidad en su perímetro de defensa.** Ahora los usuarios constituyen su límite de seguridad y acceden a la red desde cualquier parte, a todas horas. Es necesario que sepa con certeza si son quienes afirman ser y que solamente les permita acceder a la información y los servicios que les correspondan. Esto implica considerar la autenticación basada en riesgos combinada con enfoques basados en análisis para comprobar las identidades.
2. **Debe tratar la seguridad como un impulsor del negocio.** Dentro de la economía de las aplicaciones, la seguridad no solo sirve para reducir los riesgos, sino también para estimular el crecimiento del negocio. Nuestro estudio demuestra que un enfoque centrado en la identidad puede reportar una serie de ventajas que mejoren la rentabilidad. Así pues, debe integrar los indicadores de rentabilidad del negocio en el marco de la evaluación de la seguridad.
3. **Céntrese en forjar relaciones digitales de confianza**. Los activos más importantes de que dispone son las relaciones digitales que establece con los clientes. Necesitan confiar en que su empresa entiende cuáles son sus necesidades al interactuar con ella, tener la seguridad de que protege sus identidades y datos con el máximo celo.
4. **Proteja experiencias, no solo datos**. Es preciso que la seguridad sea firme, pero además no debe provocar fricciones. Los clientes ansían disfrutar de interacciones sin problemas y experiencias de calidad; cualquier inconveniente les resultará desagradable. Eso implica ofrecer accesos con inicio de sesión único, capacidades en régimen de autoservicio y mecanismos de autenticación coherentes pero flexibles, que den servicio mientras los usuarios eligen diversas aplicaciones y dispositivos.
5. **Adopte un enfoque adaptativo de la gestión de accesos e identidades (IAM)**. Nuestro estudio pone de relieve que los usuarios maduros de la seguridad centrada en identidades disponen de controles de IAM que se pueden adaptar de inmediato para responder ante riesgos, lo que aporta notorias mejoras para la experiencia de usuario.
6. **Actúe de forma proactiva y predictiva**. Las funciones de análisis avanzado pueden ayudarle a esquivar de manera proactiva las amenazas para la seguridad, en lugar de acudir siempre a apagar fuegos. Además, pueden llevar la seguridad un paso más allá: le ayudarán a detectar, reaccionar y adaptar los procesos de seguridad para abordar el riesgo de infracciones antes de que estas se produzcan.
7. **No sacrifique la seguridad en aras de más velocidad**. La presión por lanzar aplicaciones nuevas a toda velocidad ha crecido debido a la economía de las aplicaciones. Por eso hoy es más importante que nunca asegurarse de integrar la seguridad desde el primer momento; nada de ponerla en entredicho justo al final. Plantéese la posibilidad de adoptar un enfoque de DevSecOps para asegurarse de cubrir todas las consideraciones sobre seguridad en las etapas iniciales del proceso de desarrollo.



Más información

Metodología de investigación del estudio

CA Technologies encargó a Coleman Parkes Research que entrevistase a una serie de ejecutivos acerca del alcance y el impacto de las actividades relacionadas con la transformación digital sobre sus organizaciones.

Encuestamos a 1770 personas que ocupan puestos directivos sénior o son responsables de tomar decisiones sobre las TI (incluidos 106 directores de seguridad o directores de seguridad de la información) que trabajan para grandes empresas, repartidos por 21 países de las regiones de América, EMEA y Asia-Pacífico y Japón (APJ). Las organizaciones estudiadas presentan ingresos anuales superiores a los 1000 millones de dólares USD (o 500 millones en algunas economías más reducidas).

Estos fueron los países representados en la encuesta:

América	**EMEA**	**APJ**
Brasil	Alemania	Australia
Estados Unidos	España	China
	Francia	Corea
	Italia	Hong Kong
	Países Bajos	India
	Reino Unido	Indonesia
	Sudáfrica	Japón
	Suecia	Malasia
	Suiza	Singapur
		Tailandia

Estos fueron los sectores de actividad representados en la encuesta:

- Automoción
- Banca y servicios financieros
- Empresas de titularidad pública nacionales
- Energía y servicios públicos
- Fabricación
- Medios de comunicación y ocio
- Minoristas
- Sanidad
- Telecomunicaciones
- Transporte y logística

La investigación y el análisis se llevaron a cabo entre mayo y junio de 2016.

Acerca de CA Technologies

CA Technologies (NASDAQ: CA) crea software que impulsa la transformación de las empresas y les permite aprovechar las oportunidades que brinda la economía de las aplicaciones. El software se encuentra en el corazón de cada empresa, sea cual sea su sector. Desde la planificación hasta la gestión y la seguridad, pasando por el desarrollo, CA trabaja con empresas de todo el mundo para cambiar la forma en que vivimos, realizamos transacciones y nos comunicamos, ya sea a través de la nube pública, la nube privada, plataformas móviles, entornos de mainframe o entornos distribuidos. www.ca.com/es

Acerca de Coleman Parkes Research

Coleman Parkes Research es una empresa especializada en reclutar y entrevistar a encuestados de nivel sénior distribuidos por diversos mercados globales, sectores verticales y áreas funcionales, correspondientes a un amplio abanico de clientes. Desde la investigación sobre liderazgo de opinión para las relaciones públicas y las campañas de marketing hasta el análisis de las oportunidades de ganancias/pérdidas, con de prueba de los mensajes sobre productos y realizando entrevistas en profundidad a ejecutivos: nos encargamos de todo. Coleman Parkes Research colabora con los clientes para formular estrategias de eficacia probada, que obtienen información y perspectivas sobre los mercados basándose en los requisitos específicos individuales y las hipótesis clave. colemanparkes.com/

Acerca de Grist

Servicios editoriales y de creatividad. Grist es una agencia de marketing de contenidos y liderazgo de opinión, que trabaja en el ámbito B2B y cuya labor ha sido ya objeto de premios. Trabajamos con la herencia editorial de The Economist y Financial Time imbricada en nuestro ADN y tenemos una perspectiva clara del futuro digital. www.gristonline.com