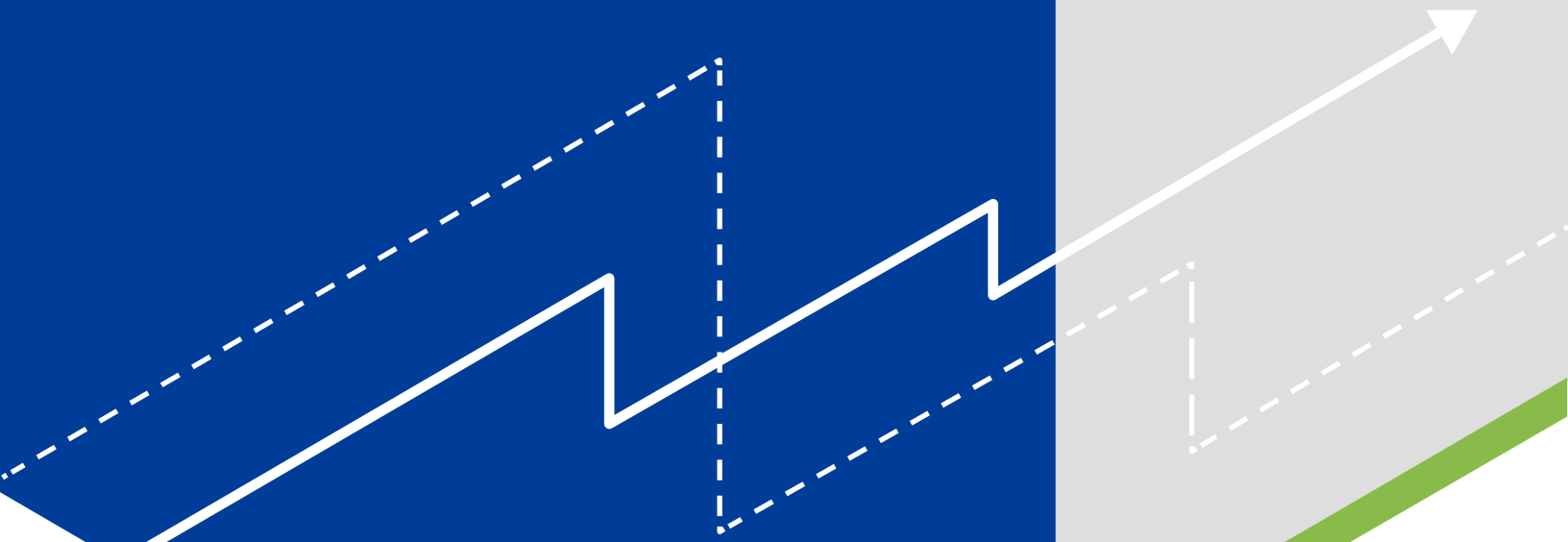
Artículo de liderazgo intelectual
de Forrester Consulting
encargado por IBM

Marzo de 2017

Visión Móvil 2020

El impacto de la movilidad, la Internet de las Cosas y la inteligencia artificial en el futuro de la transformación empresarial



FORRESTER®

Director del proyecto:
Heather Vallis,
Consultor superior de impacto en el mercado

Investigación de colaboración:
Grupo de investigación de seguridad y riesgo de Forrester

ACERCA DE FORRESTER CONSULTING

Forrester Consulting ofrece servicios de consultoría independientes, objetivos y basados en investigaciones para ayudar a los líderes a tener éxito en sus organizaciones. Los servicios de consultoría de Forrester Consulting abarcan desde una breve sesión estratégica hasta proyectos personalizados, además de permitirle ponerse en contacto directamente con analistas de investigación que aplican sus conocimientos especializados a los desafíos de negocios específicos de su empresa. Para obtener más información, visite forrester.com/consulting.

FORRESTER®

Resumen ejecutivo

A medida que la tecnología móvil adquiere más capacidades y acceso a los datos de la empresa, los dispositivos móviles continúan jugando un papel importante en la forma de trabajar del personal. Los trabajadores de la información ya no se limitan a utilizar sus PC; los smartphones, tablets y computadoras portátiles les ofrecen la flexibilidad que necesitan para elegir el dispositivo más adecuado al contexto de cada tarea. Internet de las Cosas (IoT) representa el próximo gran avance en la transformación empresarial cambiando la forma en que las empresas detectan, analizan y controlan sus mundos conectados. Sin embargo, a medida que aumenta el número de dispositivos y objetos que tienen acceso a los datos confidenciales de la organización, aumenta también la complejidad de la gestión y protección de una "superficie de ataque" cada vez más amplia. Los empleados esperan contar con gestión uniforme y capacidades en todos los dispositivos que utilizan para trabajar; no obstante, la mayor parte de las organizaciones adoptan un enfoque inconexo, utilizando diferentes equipos y herramientas para la gestión y seguridad de los terminales. Para reducir la cantidad de tensiones y la complejidad interna, las organizaciones necesitan considerar tanto un enfoque específico para sus dispositivos como un enfoque independiente de los dispositivos, según sus casos de uso, en un contexto en el que los controles independientes de dispositivos se centran en las capas de aplicación y de datos en todos los tipos de dispositivos, independientemente de su factor de forma.

La aplicación de técnicas de inteligencia artificial (IA), como la computación cognitiva y el aprendizaje automático, al análisis de todos los datos nuevos creados en este paradigma no solo hace posible la transformación, sino que también se hace necesaria a medida que aumenta la cantidad (y complejidad) de dispositivos. Las organizaciones serán capaces de aprovechar la abundancia de datos y obtener información de negocios para permitir una mayor convergencia en la gestión y seguridad de estos diferentes factores de forma de terminales, lo cual conducirá a un estado futuro de gestión unificada de terminales.

En octubre de 2016, IBM solicitó a Forrester Consulting que evaluara las formas en que las empresas están gestionando y protegiendo diversos factores de forma de terminales en la actualidad, y cómo las estrategias cambiarán en los próximos tres años. Al realizar una exhaustiva encuesta a 556 líderes de TI y de seguridad en los Estados Unidos, en el Reino Unido, en Alemania, en India y en Australia, Forrester constató que, si bien las empresas cuentan hoy con un enfoque descentralizado de gestión y protección de smartphones, tablets, computadoras portátiles e IoT, adoptarán un enfoque más consolidado (y cognitivo) hasta el año 2020.

FORRESTER

CONCLUSIONES CLAVE

- **Las empresas cuentan con un enfoque de gestión de dispositivos y terminales en silos.** La computación de usuario final ya no consiste en un modelo único para todos los casos. Las organizaciones están pasando rápidamente del establecimiento de una PC y una imagen únicas para cada empleado a un enfoque que admite múltiples dispositivos para el personal. La IoT suele ser gestionada por las líneas de negocio,como parte de sus operaciones. Sin embargo, la mayoría de las empresas aún cuentan con equipos y herramientas independientes para gestionar todos estos dispositivos. La mayoría de las empresas encuestadas (el 74 %) informó que sus organizaciones adoptan un enfoque específico para la gestión de sus dispositivos y terminales.
- **La gestión se volverá más centralizada en los próximos tres años.** A medida que los entornos de terminales se vuelvan más complejos y las empresas aumenten el control sobre el costo de propiedad de la gestión de dispositivos y terminales, las organizaciones empezarán a realizar la transición de una gestión específica a una gestión independiente de los dispositivos. Hasta el año 2020, las organizaciones que cuentan con este enfoque más centralizado pasarán de representar un 26 % de todas las organizaciones a representar un 42 % de éstas.
- **Para el año 2020, muchas organizaciones contarán con una gestión unificada de terminales (UEM).** A medida que las organizaciones trabajen para adoptar un enfoque más integrado e independiente de los dispositivos, aumentará la implementación de la UEM. Si bien solo el 15 % de ellas cuenta hoy con un enfoque de gestión centralizado, el 54 % habrá implementado soluciones de UEM para el año 2020.
- **Para el 2020, la mayoría de las organizaciones utilizarán inteligencia artificial/computación cognitiva para sacar conclusiones a partir de los datos de** terminales. Con el esperado crecimiento exponencial de los datos de terminales obtenidos a partir de diversos dispositivos y objetos, para el año 2020 más del 80 % de las empresas utilizará IA/computación cognitiva para obtener información de negocios y de seguridad.

El 54 % de las organizaciones contará con soluciones de UEM para el año 2020.

FORRESTER®

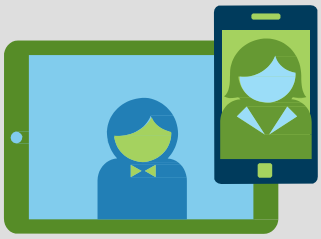
El entorno de dispositivos de negocios actual es complejo

Las empresas de hoy están ampliando las capacidades móviles que ofrecen a su personal. De hecho, el uso de dispositivos móviles para realizar tareas asociadas al trabajo se ha convertido en la norma para la mayoría de los empleados. Según un estudio reciente de Forrester, el 72 % de los empleados utiliza al menos semanalmente un dispositivo móvil para trabajar (véase la Figura 1).[1] No obstante, los dispositivos móviles representan solo una de las herramientas de que disponen los empleados de hoy; aproximadamente la mitad (el 49 %) de los trabajadores de la información utilizan al menos tres dispositivos para trabajar semanalmente.[2] En este ambiente de trabajo moderno, es importante que los empleados puedan seleccionar el dispositivo adecuado para cada tarea que realicen. Aunque los smartphones y tablets proporcionan a los empleados la flexibilidad necesaria para tener acceso a la información al instante o atender a los clientes en tiempo real, las computadoras portátiles y PC aún juegan un papel fundamental en el entorno de computación empresarial de hoy. Casi todos los trabajadores de la información (el 99 %) aún utilizan una desktop o computadora portátil al menos una vez a la semana.[3] Esta proliferación y sofisticación de los dispositivos presenta grandes retos de gestión para las empresas: aproximadamente un tercio (el 34 %) de los tomadores de decisiones de TI y de seguridad encuestados mencionaron el aumento en la cantidad de dispositivos admitidos por usuario entre sus cinco principales retos de gestión de terminales.

La proliferación de dispositivos admitidos por usuario es uno de los principales retos de gestión de terminales para **el 34 % de las organizaciones.**

Figura 1

Panorama de dispositivos de negocios: ya no se adopta un enfoque



El 72 % de los empleados utiliza al menos semanalmente

El 49 % de los trabajadores de la información utiliza al menos tres dispositivos para trabajar semanalmente

El 99 % de los trabajadores de la información utiliza

Base: 7342 trabajadores de la información de todo el mundo
Fuente: Forrester Data Global Business Technographics® Telecommunications And Mobility Workforce Survey, 2016

FORRESTER®

Las empresas están gestionando los dispositivos en silos

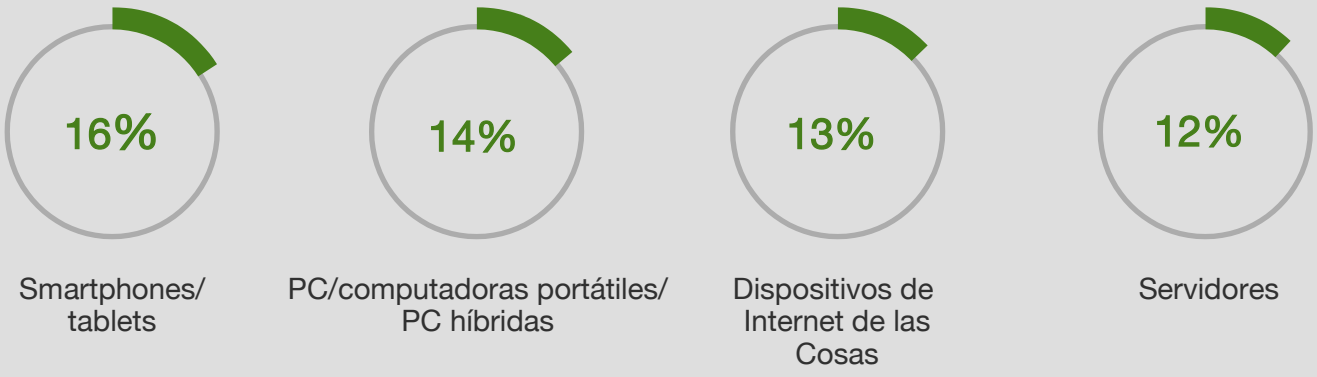
Para trabajar de manera eficiente y eficaz en un entorno de dispositivos diverso, los empleados necesitan contar con practicidad y uniformidad, independientemente del dispositivo que están utilizando. Lo ideal es que los datos y las herramientas disponibles en una PC también sean accesibles por medio de dispositivos móviles. Sin embargo, el enfoque descentralizado de gestión y protección de dispositivos que adoptan muchas organizaciones hace que esto sea difícil o incluso imposible de lograr.

LAS ORGANIZACIONES NO CUENTAN CON UN EQUIPO CENTRALIZADO DE GESTIÓN DE TERMINALES

A pesar del aumento en el uso de dispositivos variados, las organizaciones aún mantienen sus dispositivos en silos de gestión. Menos de una quinta parte de los tomadores de decisiones de TI y de seguridad encuestados informó que cuentan con un equipo dedicado para gestionar tanto los dispositivos móviles como los terminales tradicionales. De hecho, la mayoría de las empresas encuestadas indicaron que cuentan con grupos independientes para la gestión de dispositivos móviles (smartphones y tablets), PC, computadoras portátiles y PC híbridas; servidores y dispositivos de IoT (véase la Figura 2).

Figura 2

"Actualmente, ¿qué grupo de su organización es el principal responsable de la gestión de los siguientes dispositivos?"



Base: 556 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles
Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

FORRESTER®

LOS TERMINALES SE GESTIONAN A NIVEL DE DISPOSITIVO

Dada la falta de conexión entre los equipos que gestionan los factores de forma de los terminales de negocios, no es de sorprender que el enfoque general de gestión y protección de los dispositivos también sea inconexo. Según nuestra encuesta, el 74% de las organizaciones están utilizando un enfoque específico para sus dispositivos, gestionando los factores de forma de dispositivos de manera independiente. Esto probablemente se debe en parte a las limitaciones de las herramientas tradicionales de gestión de PC. En una encuesta a los tomadores de decisiones del sector de telecomunicaciones realizada por Forrester, el 49% de los encuestados dijeron que invirtieron en herramientas de gestión de dispositivos móviles de negocios (EMM) porque sus herramientas de gestión de PC no ofrecían la capacidad de gestionar dispositivos móviles.[4] El resultado es que la mayoría de las organizaciones utilizan una solución para gestionar sus PC y otra solución para gestionar sus dispositivos móviles. Si bien esto no representa un gran inconveniente para la realización de tareas de gestión básicas, cualquier tarea de aplicación de parches, implementación de software, aplicación de políticas y configuración podría resultar difícil. Afortunadamente, los sistemas operativos para PC están aproximándose a los sistemas operativos para dispositivos móviles en lo que respecta a la facilidad de gestión y seguridad. Un enfoque separado para la gestión de terminales presenta varios retos, entre los que se incluyen los siguientes:

- **Los terminales se gestionan mediante diferentes consolas.** Utilizar soluciones diferentes para gestionar los dispositivos de negocios significa trabajar en por lo menos dos consolas distintas, con diferentes interfaces de usuario (UI) y funciones. El 30% de los tomadores de decisiones de TI y de seguridad encuestados identificaron la "necesidad de tener acceso a múltiples consolas para gestionar diferentes terminales" como uno de sus cinco principales retos de gestión de terminales. Estas herramientas separadas también hacen que resulte difícil distribuir el software en entornos empresariales complejos (el 35% de los encuestados). Además, como no cuentan con una solución de gestión única para la gestión de múltiples dispositivos, las organizaciones no tienen una visibilidad consolidada de todos los terminales, un problema mencionado por el 26% de los encuestados (véase la Figura 3).

El 74% de las organizaciones están adoptando un enfoque de gestión de terminales específico para sus dispositivos.

Figura 3

"¿Cuáles son los principales retos de gestión de terminales de su organización?" (Seleccione hasta cinco opciones)

Base: 556 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles
Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

La continua supervisión y aplicación de políticas es **el principal reto de gestión de terminales.**

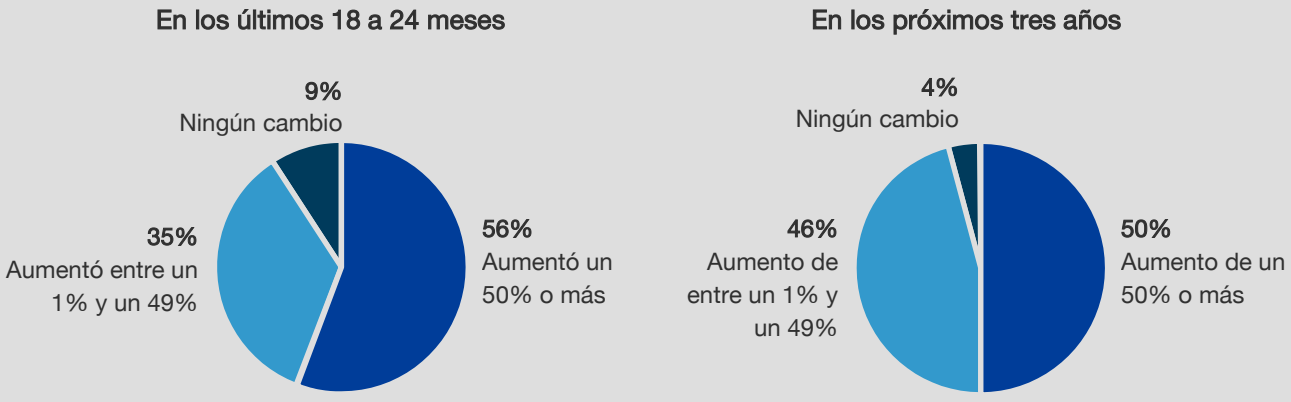
› **Cada solución de gestión necesita integrarse por separado con otros sistemas.** La continua supervisión y aplicación de políticas es el principal reto de gestión de terminales de la encuesta, mencionado por el 35% de los encuestados. Para que sea posible establecer una supervisión uniforme, así como políticas y controles coherentes para todos los dispositivos, las soluciones de gestión de dispositivos necesitan integrarse con otras soluciones empresariales, como las de control de acceso a la red (NAC) y de gestión de identidades y acceso (IAM). Sin embargo, el 30% de los encuestados mencionaron la falta de integración entre soluciones específicas entre sus principales retos. Cuando los dispositivos se gestionan mediante soluciones diferentes, es necesario realizar una integración entre sistemas para cada solución de gestión, lo cual significa que se deben llevar a cabo varias integraciones. La duplicación de esfuerzos aumenta la probabilidad de que se produzcan errores, lo que puede afectar la experiencia de los empleados y crear deficiencias en materia de seguridad.

FORRESTER®

- **Volúmenes cada vez más grandes de datos de terminales se recopilan mediante herramientas diferentes.** El 56% de los encuestados indicó que la cantidad de datos recopilados por sus organizaciones aumentó entre un 1% y un 49% en los últimos 18 a 24 meses, y el restante 35% de los encuestados informó que esta cantidad aumentó un 50% o más (véase la Figura 4). Y este flujo de datos no hará más que aumentar en los próximos años: mientras que el 46% de los encuestados prevé que la cantidad de datos de terminales recopilada se incremente entre un 1% y un 49% en los próximos tres años, el restante 50% de éstos están preparándose para enfrentar un crecimiento de un 50% o más. Las organizaciones pueden obtener información de inteligencia significativa a partir de los datos de terminales, en especial para fines de detección y resolución de amenazas. Sin embargo, la recopilación de datos de terminales mediante herramientas distintas significa que las organizaciones no cuentan con visibilidad de todos los diferentes dispositivos, lo que aumenta el riesgo de que amenazas potenciales no se resuelvan de manera oportuna. Además, la fragmentación de los datos hace que resulte difícil sacar conclusiones que podrían fundamentar mejoras de negocios y operacionales.
- **Es difícil asegurar la seguridad de los dispositivos.** A medida que aumenta la cantidad de dispositivos que tienen acceso a los datos empresariales, también se amplía la "superficie de ataque" de la organización. Según un estudio reciente de Forrester, el 49% de los trabajadores de la información que utilizan un smartphone al menos semanalmente para trabajar eligieron su dispositivo por cuenta propia, en lugar de seguir una lista aprobada por la empresa o de utilizar un teléfono emitido por ésta.[5] Garantizar la seguridad de estos dispositivos representa un gran reto. Más del 30% de los encuestados mencionaron “impedir que los usuarios registren dispositivos no autorizados” y “asegurar que los dispositivos propios de los empleados sean confiables” entre sus principales retos.

Figura 4

“¿Cuánto ha cambiado la cantidad de datos de terminales recopilados por su organización en los últimos 18 a 24 meses? ¿Cuánto cambiará en los próximos tres años?"



Base: 556 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles
Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

FORRESTER

La IoT aumenta la complejidad de gestión

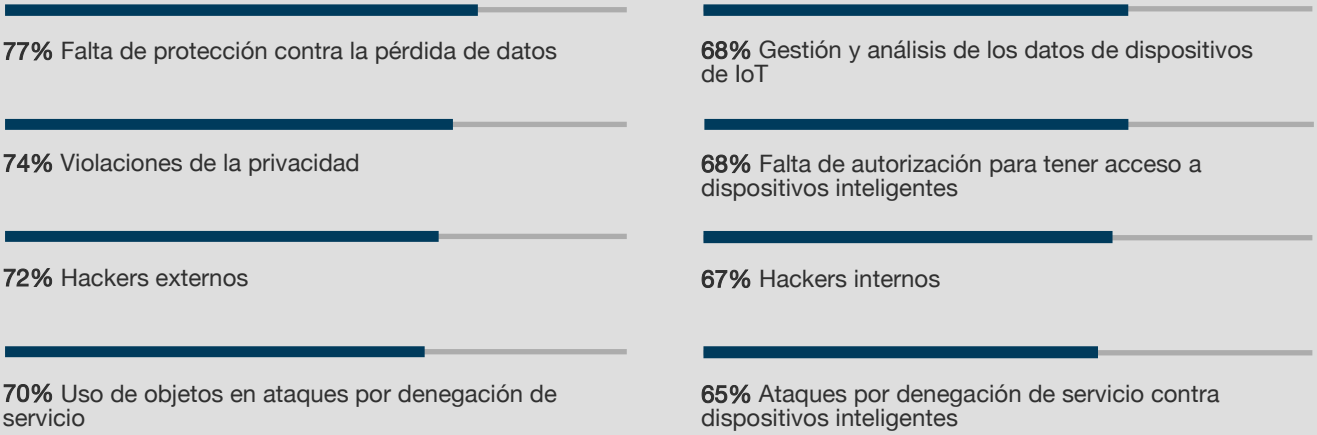
Para la mayoría de las organizaciones, no se trata de decidir si se debe o no adoptar la IoT, sino de cuándo esto debe ocurrir. El 57% de los profesionales de TI y de seguridad encuestados indicaron que sus organizaciones gestionan dispositivos de IoT; el 88% de ellos prevén que tendrán que gestionar estos dispositivos hasta el 2020. No obstante, a muchos (el 68%) de los encuestados les preocupa mucho o extremadamente la gestión y el análisis de los datos de dispositivos de IoT.

Las empresas están adoptando dispositivos y aplicaciones de IoT que cambiarán significativamente su manera de hacer negocios y atender a sus clientes.[6] Sin embargo, a medida que aumenta el uso de estos dispositivos en los entornos empresariales, también se amplían los riesgos de seguridad asociados a su implementación. A medida que los dispositivos de IoT se vuelven más sofisticados (pasando de ser objetos con poca inteligencia a ser dispositivos totalmente autónomos y conectados), la cantidad y la confidencialidad de los datos recopilados, analizados y utilizados para fundamentar decisiones aumentan significativamente.[7] Entre los encuestados, las principales preocupaciones incluyen la falta de protección contra la pérdida de datos (un 77%), las violaciones de la privacidad (un 74%), los hackers externos (un 72%) y el uso de dispositivos de IoT en ataques por denegación de servicio (un 70%) (véase la Figura 5). Para minimizar los riesgos y mantenerse competitivas, las organizaciones necesitarán elaborar una estrategia para gestionar y proteger los dispositivos y aplicaciones de IoT, así como también para analizar el gran volumen de datos recopilados.

El 88% de las organizaciones prevén que tendrán que gestionar dispositivos de IoT hasta el 2020.

Figura 5

"Al considerar la Internet de las Cosas (IoT), ¿qué tan preocupada está su organización por los siguientes elementos?"



Base: 556 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles
Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

FORRESTER

Visión móvil 2020

El actual enfoque de gestión orientado hacia los dispositivos es no solo complejo, sino también costoso. La necesidad de contar con diferentes herramientas y equipos de gestión significa que las organizaciones están dedicando recursos considerables a tareas y funciones que podrían ser redundantes e ineficientes. A medida que más dispositivos se incorporan a la organización, aumenta la demanda de una experiencia de computación más fluida por parte de los empleados. Aunque en el pasado los usuarios tenían experiencias muy diferentes en dispositivos móviles y en sus PC, los sistemas operativos para PC actuales están eliminando esta diferencia. Con el aumento del control sobre los costos de la gestión de este entorno, las empresas necesitarán hacer que su estrategia de gestión de terminales evolucione.

Mirando al futuro, para el año 2020 **la consolidación de equipos y herramientas** será esencial **para reducir el costo de gestión de dispositivos móviles y otros endpoints.**

LA REDUCCIÓN DEL TCO DE LA GESTIÓN DE DISPOSITIVOS Y TERMINALES SERÁ FUNDAMENTAL

Las empresas están bajo presión para reducir sus gastos generales en TI, volverse más eficientes y centrarse en el costo total de propiedad (TCO) de sus inversiones. Si bien el 73% de los encuestados informó que sus organizaciones están priorizando la reducción del TCO de la gestión de dispositivos y terminales, la presión no hará más que aumentar en los próximos años. Para el año 2020, el 81% de las organizaciones considerarán la reducción del TCO como una prioridad principal (véase la Figura 6). Sin embargo, las empresas de hoy necesitarán superar los retos de los distintos sistemas, herramientas y equipos, así como del exceso de datos, para cumplir con la obligación de reducir los costos de gestión.

LA CONSOLIDACIÓN JUGARÁ UN PAPEL CLAVE EN LA REDUCCIÓN DEL TCO

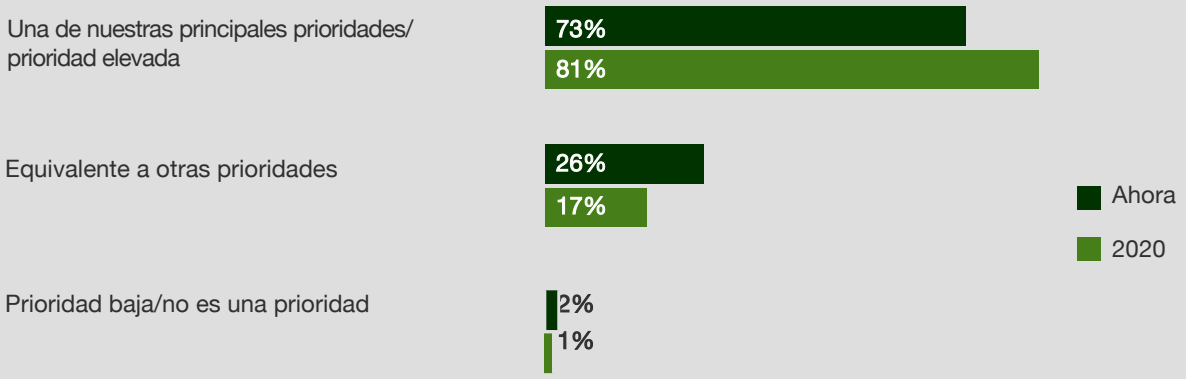
Las empresas necesitarán desarrollar un plan para responder a los retos de gestión de dispositivos y terminales y reducir el TCO, y deberán comenzar en el nivel fundamental. Mirando al futuro, para el año 2020 la consolidación de los equipos y herramientas será esencial para reducir el costo de gestión de dispositivos móviles y otros terminales. El estudio reveló que las organizaciones esperan enfrentar el TCO al eliminar silos departamentales por medio de un equipo de gestión centralizado (el 83%) y al consolidar su software de gestión en una plataforma o un proveedor único (el 72%) (véase la Figura 7). Otras medidas de reducción de los costos incluyen el uso de una licencia para múltiples plataformas con el fin de simplificar la facturación (el 78%), la transición a un modelo de suscripción de software (el 73%) y la transición a la nube, con un entorno de software como servicio (SaaS) o un entorno híbrido (el 71%).

La reducción del TCO de dispositivos y terminales será una prioridad elevada o principal para **el 81% de las empresas.**

Figura 6

"Para su organización, ¿qué tan prioritaria es la reducción del costo total de propiedad (TCO) de la gestión de dispositivos y terminales?"

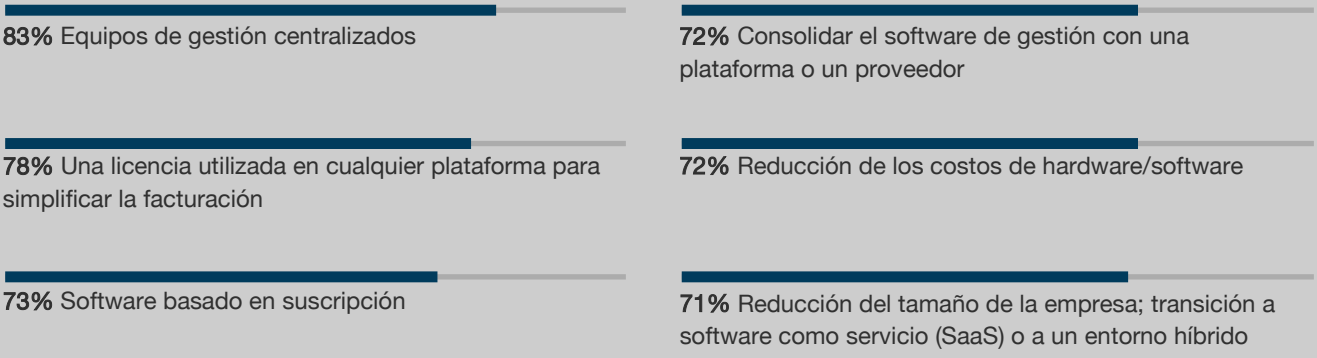
"¿En qué medida prevé usted que la reducción del TCO de la gestión de dispositivos y terminales será una prioridad para su organización para el año 2020?"



Base: 548 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles que están familiarizados con la priorización del TCO de gestión de dispositivos/terminales de su organización
(Es posible que los porcentajes no sumen un 100% debido al redondeo)
Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

Figura 7

"Pensando en el año 2020, ¿cuál es la probabilidad de que su organización utilice cada uno de los siguientes métodos para reducir el costo total de propiedad (TCO) de la gestión de dispositivos móviles y terminales?"
(Porcentajes de las respuestas "probable" o "muy probable")



Base: 556 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

FORRESTER

LA GESTIÓN DE TERMINALES EMPEZARÁ A ORIENTARSE HACIA UN ENFOQUE INDEPENDIENTE DE LOS DISPOSITIVOS

Los controles independientes de los dispositivos se centran en la seguridad de las capas de aplicación y de datos en todos los tipos de dispositivos, independientemente del factor de forma. A medida que las organizaciones avancen hacia la consolidación organizacional y tecnológica, también necesitarán cambiar su enfoque de gestión de dispositivos y terminales. Hoy, la mayoría de las organizaciones (el 74%) adoptan un enfoque específico para sus dispositivos; sin embargo, las organizaciones empezarán a abandonar este enfoque de gestión de dispositivos en silos a lo largo de los próximos tres años. Hasta el año 2020, el 42% de las organizaciones esperan realizar la transición a un enfoque independiente de los dispositivos, lo que representa un aumento frente al 26% actual.

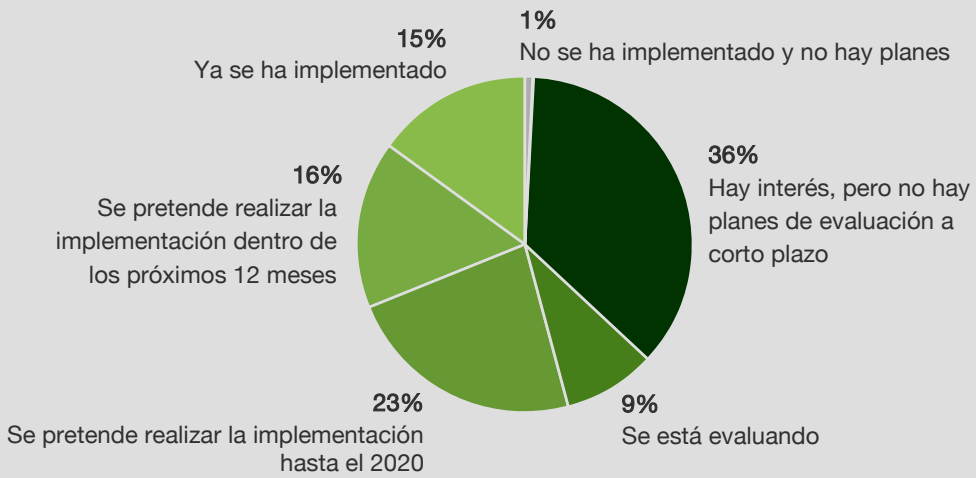
Hasta el año 2020, el 42% de las organizaciones esperan realizar la transición a un enfoque de gestión independiente de los dispositivos, lo que representa un aumento frente al **26% actual.**

LA GESTIÓN UNIFICADA DE TERMINALES SENTARÁ LAS BASES PARA LA CONSOLIDACIÓN

La gestión unificada de terminales (UEM) es un enfoque para proteger y controlar tanto terminales tradicionales como dispositivos móviles, de manera uniforme, desde una única consola. Si bien algunas organizaciones (el 15%) han adoptado la UEM hasta la fecha, la implementación empezará a aumentar a medida que las organizaciones se esfuerzan para adoptar un enfoque de gestión más integrado e independiente de los dispositivos. El 16% de las organizaciones adoptarán la UEM dentro de los próximos 12 meses; para el año 2020, el 54 % de éstas contarán con este enfoque (véase la Figura 8).

Figura 8

"¿Cuáles son los planes de su organización para implementar la gestión unificada de terminales?"



Base: 556 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles
Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

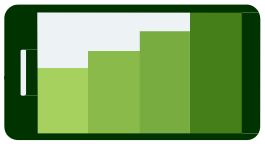
La implementación de la UEM aumentará durante los próximos tres años, a medida que las organizaciones se esfuercen para adoptar un enfoque de gestión más integrado e independiente de los dispositivos.

FORRESTER

La adopción de la UEM se basará en diversos factores, incluidos los siguientes:

- **Proliferación de dispositivos.** Entre los encuestados de las organizaciones que utilizan o planean implementar la UEM, el principal factor impulsor para la adopción es la mayor necesidad de gestionar el número de dispositivos en rápido aumento, mencionada por el 43% de ellos. Lo que ha estimulado este crecimiento es la afluencia de dispositivos propios de los empleados: el 32% de los encuestados informó que las políticas de BYOD (Traiga su propio dispositivo) para smartphones, tablets, computadoras portátiles y desktops constituyen el impulso para la adopción de la UEM (véase la Figura 9).

  Una de las principales razones por las que los empleados están llevando a la oficina no solo sus propios dispositivos móviles, sino también sus PC, es que las PC de hoy han evolucionado, funcionando como dispositivos móviles. Los modernos sistemas operativos para computadoras portátiles están aproximándose a la facilidad de gestión y seguridad de los sistemas operativos para dispositivos móviles. De hecho, el 40% de los encuestados mencionaron la creciente adopción de Windows 10 y macOS como un factor impulsor para la implementación de la UEM.
- **Centralización de la gestión de terminales.** La UEM proporciona un punto central mediante el cual las organizaciones cuentan con visibilidad y control de todos los dispositivos de los empleados. Este enfoque centralizado de gestión significa que las organizaciones pueden consolidar tanto los equipos como las herramientas de gestión de terminales, reduciendo las tareas y funciones redundantes, así como también el TCO. Aproximadamente un tercio de los encuestados están recurriendo a la UEM para centralizar los equipos (el 37%) y las herramientas de gestión de terminales (el 33%), mientras que el 41% de ellos consideran la UEM como una forma de reducir los costos de gestión de terminales.



El **principal factor impulsor** para la adopción de la UEM es **la mayor necesidad de gestionar el número de dispositivos en rápido aumento.**

Figura 9

"¿Cuáles son los factores que han impulsado su organización a la implementación de la UEM?"

43% Mayor necesidad de gestionar la cantidad en rápido crecimiento de dispositivos

41% Demanda, por parte de los usuarios, de acceso a los datos en cualquier momento y lugar, y desde cualquier dispositivo

41% Esfuerzo de reducción del costo total de propiedad

40% Aumento de la adopción de Windows 10 y macOS

39% Capacidad de realizar análisis y obtener información (computación cognitiva) a partir de todos los terminales

37% Simplificación de los informes y la gestión de la conformidad propiedad

37% Consolidación de los equipos para la gestión de los terminales

37% Migración a un modelo de gestión de software como servicio (SaaS)

33% Consolidación de las herramientas de gestión de terminales

32% Política de BYOD para smartphones, tablets, computadoras portátiles y desktops

Base: 304 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles en empresas que planean implementar la UEM hasta el 2020
Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

FORRESTER

- **Demanda de acceso a los datos en cualquier momento y lugar.** Los empleados ya no necesitan mantenerse en sus escritorios, ya que pueden realizar tareas de trabajo utilizando múltiples dispositivos todos los días. Para poder trabajar de manera efectiva, necesitan contar con acceso a los mismos datos y aplicaciones, independientemente del dispositivo que están utilizando. Aproximadamente dos quintas partes de los tomadores de decisiones de TI y de seguridad encuestados indicaron que la decisión de implementar la UEM se debe a esta demanda de acceso a los datos desde múltiples dispositivos por parte de los usuarios finales.
- **Necesidad de mejores capacidades de análisis en todos los terminales.** El 39% de los encuestados mencionaron la capacidad de realizar análisis y obtener información a partir de todos los terminales como un factor impulsor para la adopción. Aunque ciertamente es posible recopilar datos específicos de los dispositivos por medio de herramientas de gestión de dispositivos individuales, a menos que estas herramientas estén integradas con otros sistemas de gestión e inteligencia, las organizaciones contarán con una visión incompleta. Esta información es fundamental cuando se trata de detectar campañas de amenazas que abarcan varios tipos de terminales, como la detección de movimientos laterales entre un smartphone corporativo y la computadora portátil de un empleado, o cualquier ataque contra usuarios específicos que abarque varios factores de forma de terminales. La UEM no solo actúa como un punto de integración para otros sistemas críticos para la empresa, sino que también consolida los datos de los terminales para permitir que se realicen análisis más significativos y se obtenga información empleable.

LAS EMPRESAS APROVECHARÁN LA INTELIGENCIA ARTIFICIAL PARA INTERPRETAR LOS DATOS DE LOS TERMINALES

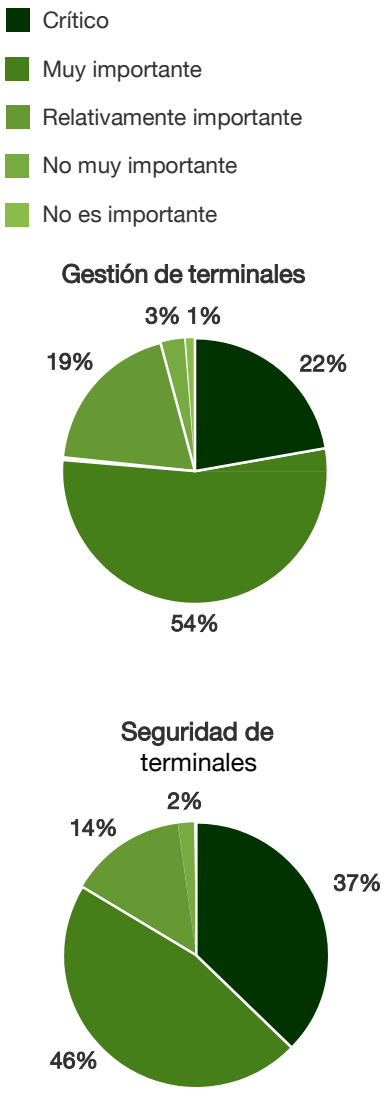
La inteligencia artificial (también conocida como IA o computación cognitiva) existe desde 1950, pero se ha vuelto cada vez más popular en los últimos años gracias a los avances en el aprendizaje profundo y en el almacenamiento y procesamiento de datos.[8] Según un estudio reciente de Forrester, las inversiones en IA/computación cognitiva aumentarán más de un 300% en 2017, en comparación con 2016.[9] La IA/computación cognitiva está evolucionando rápidamente para automatizar varias tareas manuales, mejorando la capacidad que tienen las empresas de generar información de negocios empleable, obtener eficiencias operacionales e identificar y enfrentar amenazas. La IA/computación cognitiva ha permitido que personas y sistemas actúen conjuntamente de manera más colaborativa y eficiente.

Las inversiones en IA/computación cognitiva **aumentarán un 300%** en 2017.

A medida que aumente el volumen de datos recopilados a partir de los terminales y que las empresas trabajen para consolidar la gestión de dispositivos y terminales, la IA/computación cognitiva se volverá una necesidad. Según los encuestados, más del 80 % de las organizaciones implementarán IA/computación cognitiva hasta 2020 para analizar el volumen de datos de terminales que recopilan, que es amplio y está creciendo rápidamente. Los profesionales de TI y de seguridad encuestados reconocen el valor de la aplicación de IA/computación cognitiva a los datos de los terminales de sus organizaciones, y la mayor parte de éstos afirman que juega un papel muy importante en sus estrategias de gestión (el 76%) y seguridad (el 83%) de terminales (véase la Figura 10).

Figura 10

"¿Qué tan importante es el papel que juega (o jugará) la inteligencia artificial/ computación cognitiva en la estrategia de gestión y seguridad de terminales de su organización?"



Base: 481 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles de las empresas que han implementado, planean implementar o están considerando im plementar la IA/computación cognitiva Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

FORRESTER

Los encuestados identificaron tanto los beneficios de seguridad como los beneficios de negocios asociados al uso de la IA/computación cognitiva:

- **Aplicación de IA/computación cognitiva a la seguridad.** La IA/computación cognitiva puede ayudar a las organizaciones a mejorar significativamente sus capacidades de detección y resolución de amenazas, lo que incluye la capacidad de analizar amenazas en tiempo real (el 80%), mejorar las eficiencias del proceso de seguridad (el 79%), reconocer patrones en los datos de seguridad que representen amenazas (el 78%) y proponer o automatizar medidas correctivas (el 74%) (véase la Figura 11).

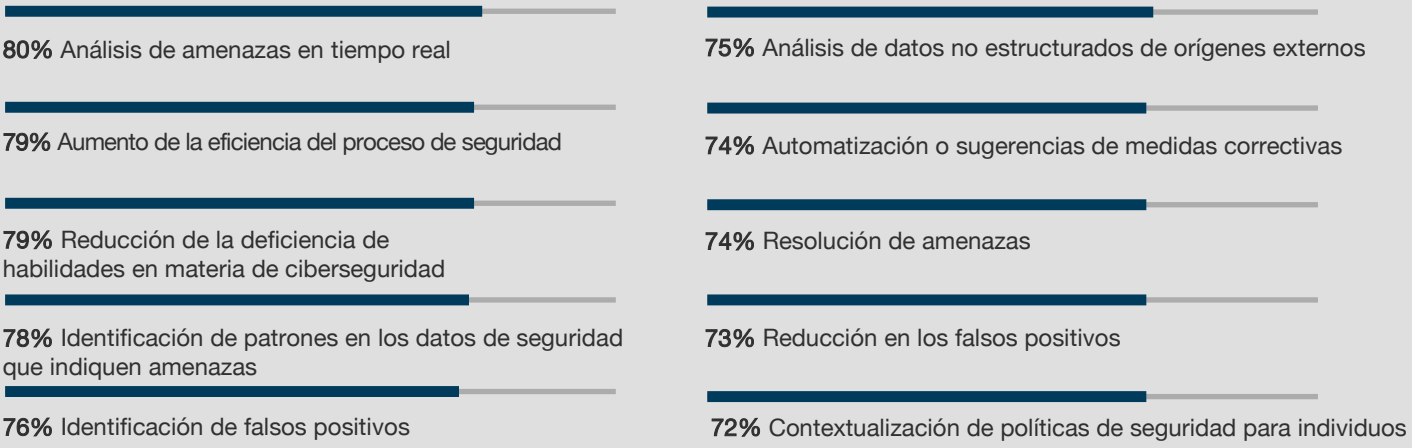
  Las tecnologías de IA/computación cognitiva pueden analizar con eficiencia los datos estructurados o de terminales, identificando patrones y estableciendo relaciones más rápidamente que los analistas humanos, para ayudar a detectar amenazas e identificar falsos positivos. La IA/computación cognitiva también se puede emplear para automatizar los procesos manuales de seguridad (como la correlación entre datos de amenazas, la investigación de amenazas y las alertas de investigación) al permitir que los analistas realicen consultas simultáneamente a partir de varios orígenes de datos no estructurados, acelerando el proceso de investigación. Por ejemplo, la prevención y detección del *ransomware* moderno requiere información sobre todos los ejecutables en el terminales, así como sobre el comportamiento en memoria, para detener las variantes avanzadas de malware que no utilizan archivos. Establecer correlaciones y sacar conclusiones a partir de estos datos resultaría muy difícil sin el uso de IA/computación cognitiva.

- **Utilización de la IA/computación cognitiva para mejorar la productividad y la obtención de información.** La mayoría de los encuestados afirmaron que la IA/computación cognitiva también puede impulsar las eficiencias empresariales y la productividad. El 81% de éstos indicaron que la tecnología puede ayudar a lograr mejoras moderadas o significativas en materia de eficiencias operacionales y administrativas (véase la Figura 12). Además de esto, la IA/computación cognitiva puede ayudar a superar deficiencias de dotación de personal y habilidades, mencionadas por el 75% y el 71% de los encuestados, respectivamente. Al automatizar tareas y funciones, la gestión de dispositivos puede volverse más eficiente, menos manual y más rentable.

  La IA/computación cognitiva puede ofrecer información sólida a las empresas, mediante interfaces cognitivas en sistemas complejos, analítica avanzada y tecnologías de aprendizaje automático. Esta tecnología puede acelerar la toma de decisiones de negocios, ayudando a eliminar la brecha entre la obtención de información y la adopción de medidas. Los encuestados valoran el uso de la IA/computación cognitiva con este propósito: más de tres cuartas partes afirmaron que la tecnología podría mejorar su capacidad de sacar conclusiones a partir de datos no estructurados de software de movilidad (el 77%), analizar los datos de IoT (el 76%), proporcionar información de negocios clave para beneficiar a la empresa (el 76%) y, en última instancia, ayudar en la toma de decisiones basadas en los datos (el 76%).

Figura 11

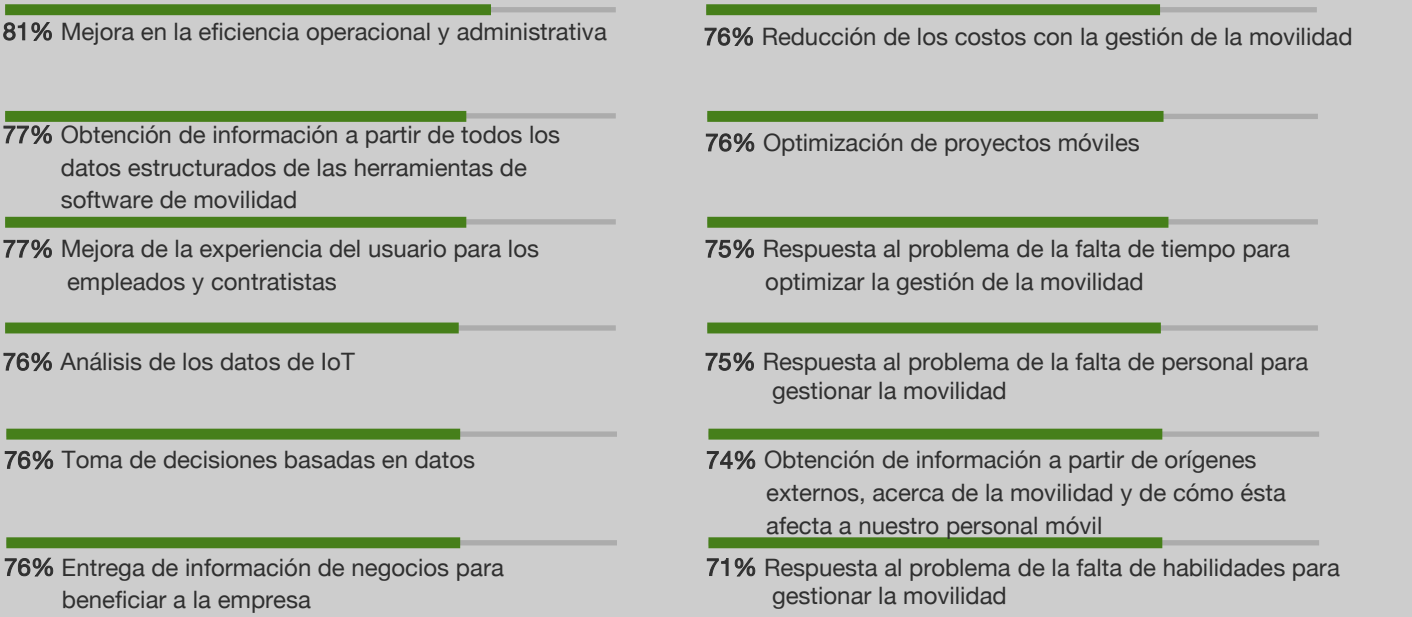
"En qué medida la inteligencia artificial/computación cognitiva ha mejorado o podría mejorar las capacidades de su organización en los siguientes ámbitos de productividad o percepción de negocios?" (Porcentajes de las respuestas "mejora moderada" o "mejora significativa")



Base: 481 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles en empresas que han implementado, planean implementar o están implementando soluciones de IA/computación cognitiva
Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

Figura 12

"En qué medida la inteligencia artificial/computación cognitiva ha mejorado o podría mejorar las capacidades de su organización en los siguientes ámbitos de productividad o percepción de negocios?" (Porcentajes de las respuestas "mejora moderada" o "mejora significativa")



Base: 481 profesionales de TI y de seguridad responsables de la gestión y seguridad de clientes, terminales o dispositivos móviles en empresas que han implementado, planean implementar o están implementando soluciones de IA/computación cognitiva
Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

FORRESTER®

Qué significa esto

La proliferación de dispositivos obligará a la mayoría de las organizaciones a buscar formas de simplificar las prácticas de gestión y seguridad de los dispositivos de usuarios finales. Hoy, la mayor parte de las organizaciones tratan los dispositivos móviles, las PC y la IoT separadamente, pero esto cambiará en los próximos tres a cinco años, a medida que más equipos de TI adopten herramientas que les permitan realizar una gestión unificada de terminales. La adopción se acelerará gracias a los nuevos avances informáticos, como los avances en el campo de la inteligencia artificial, la computación cognitiva y el procesamiento de lenguaje natural, permitiendo que los administradores realicen consultas rápidas en sus entornos y adopten medidas coordinadas para PC, dispositivos móviles y puntos de control de IoT. Además, las nuevas capacidades de análisis presentarán oportunidades para que los equipos de seguridad y gestión de terminales obtengan información más completa y significativa a partir de la creciente cantidad de datos de terminales, reduciendo a la vez las dificultades operacionales y el TCO.

Figura 13

Fuente: Estudio de Forrester Consulting encargado por IBM, enero de 2017

FORRESTER

Recomendaciones clave

Empiece hoy mismo a orientar su estrategia de gestión de terminales hacia la UEM:

Identifique formas de reducir sus dificultades operacionales. La UEM presenta oportunidades en áreas como las operaciones de seguridad, la automatización de la gestión y la inteligencia de negocios. Considere proveedores que ofrezcan integración con las herramientas que utiliza su personal e identifique ámbitos en los que la analítica avanzada y la automatización puedan serle de ayuda.

Redoble la apuesta en los controles basados en aplicaciones y datos. Su estrategia de UEM se verá complementada por sólidas tecnologías de seguridad y gestión a nivel de aplicaciones y datos, como los contenedores de datos que protegen el e-mail corporativo, la navegación web y las aplicaciones empresariales. Si aún no lo ha hecho, empiece a pasar de centrarse en la seguridad y la gestión orientadas hacia los dispositivos a centrarse en estrategias basadas en aplicaciones y datos. Esto le permitirá proteger lo que realmente importa (sus aplicaciones y datos confidenciales), aumentando al mismo tiempo su tolerancia al riesgo a nivel de dispositivo.

Comprenda que la IoT representa una gran oportunidad para muchos sectores. Los líderes de TI y de seguridad necesitan trabajar con las líneas de negocio para comprender las oportunidades y los retos asociados a la IoT, y también necesitan empezar a hablar con los proveedores de UEM acerca de cómo éstos pueden ayudar en la gestión de terminales.

Unifique su inteligencia y control de seguridad. Una vez que se haya unificado la inteligencia de terminales, la analítica avanzada y la IA/computación cognitiva se podrán aplicar a los datos recopilados para sacar conclusiones de negocios que puedan impulsar ventajas competitivas y acelerar la contención de los eventos de seguridad.

FORRESTER®

Apéndice A: metodología

En este estudio, Forrester Consulting realizó una encuesta en línea a 556 organizaciones de los EE. UU., del Reino Unido, de Alemania, de India y de Australia, para evaluar las formas en que las empresas están gestionando y protegiendo diversos factores de forma de terminales en la actualidad, y cómo las estrategias cambiarán en los próximos tres años. Entre los participantes de la encuesta se encuentran líderes de TI y de seguridad de organizaciones con 1.000 o más empleados. Se obtuvo una distribución uniforme de encuestados para las organizaciones con entre 1.000 y 9.999 empleados, así como para las organizaciones con 10.000 o más empleados. Se ofreció un pequeño incentivo a los encuestados, como forma de agradecer por el tiempo dedicado a la encuesta. El estudio se llevó a cabo en enero de 2017.

Anexo B: material complementario

ESTUDIOS DE FORRESTER RELACIONADOS

“Build A Cross-Functional Mobile Security Team”, Forrester Research, Inc., 22 de febrero de 2017

“The State Of Enterprise Mobile Security: 2016 To 2017”, Forrester Research, Inc., 12 de enero de 2017

“Predictions 2017: Artificial Intelligence Will Drive The Insights Revolution”, Forrester Research, Inc., 2 de noviembre de 2016

“Quick Take: Your Next Security Analyst Could Be A Computer”, Forrester Research, Inc., 10 de mayo de 2016

“Secure IoT As It Advances Through Maturity Phases”, Forrester Research, Inc., 7 de enero de 2016

“The Forrester Wave™: Enterprise Mobile Management, Q4 2015”, Forrester Research, Inc., 4 de diciembre de 2015

Apéndice C: notas finales

ESTUDIOS DE FORRESTER RELACIONADOS

[1] Fuente: Forrester Data Global Business Technographics® Telecommunications And Mobility Workforce Survey, 2016.

[2] Fuente: Forrester Data Global Business Technographics Telecommunications And Mobility Workforce Survey, 2016.

[3] Fuente: Forrester Data Global Business Technographics Telecommunications And Mobility Workforce Survey, 2016.

[4] Fuente: Forrester Data Global Business Technographics Mobility Survey, 2015.

[5] Fuente: Forrester Data Global Business Technographics Telecommunications And Mobility Workforce Survey, 2016.

[6] La Internet de las Cosas (IoT), o lo que Forrester denomina "el mundo conectado", combina tecnologías que permiten a dispositivos, objetos y elementos de infraestructura interactuar con sistemas de supervisión, analítica y control en redes de tipo Internet. Las soluciones compatibles con IoT son muy prometedoras y tienen el potencial de revolucionar la experiencia del cliente, aumentar la seguridad, mejorar el estado de los dispositivos y eliminar la ineficiencia.

[7] Fuente: “Secure IoT As It Advances Through Maturity Phases”, Forrester Research, Inc., 7 de enero de 2016.

[8] Forrester define la inteligencia artificial (IA) como la teoría y las capacidades que tienen el objetivo de simular la inteligencia humana por medio del aprendizaje y la experiencia. Hoy, la IA actúa principalmente como una inteligencia adicional, ya que mejora la inteligencia de los seres humanos al ofrecerles conocimiento contextual a partir de datos a los que la mente humana no puede tener acceso y que ésta puede procesar por sí sola.

[9] Fuente: “Predictions 2017: Artificial Intelligence Will Drive The Insights Revolution”, Forrester Research, Inc., 2 de noviembre de 2016.