Concepto “Bring Your Own Device (BYOD)” de Cisco

Libertad de elección de los dispositivos sin sacrificar la red de TI

Última actualización: 29 de agosto de 2013

Acerca de los autores

Neil Anderson, Director de arquitectura de sistemas, Systems Development Unit (SDU), Cisco Systems

Neil es Director de arquitectura de sistemas de Cisco, donde ha sido responsable del desarrollo de sistemas durante más de 10 años. Cuenta con más de 25 años de amplia experiencia en sistemas, como redes telefónicas públicas, sistemas de telefonía móvil y redes IP. En Cisco, Neil está dedicado a la infraestructura de redes empresariales, que abarca tecnologías emergentes, routing, switching, redes inalámbricas y movilidad, seguridad y vídeo. Neil es también coautor de cinco libros de la serie Networking Simplified publicados por Cisco Press.

TODOS LOS DISEÑOS, ESPECIFICACIONES, DECLARACIONES, INFORMACIONES Y RECOMENDACIONES (DENOMINADOS, DE FORMA GENERAL, “DISEÑOS”) DEL PRESENTE MANUAL SE OFRECEN “TAL CUAL”, CON LOS ERRORES QUE PUEDAN CONTENER. CISCO Y SUS PROVEEDORES RECHAZAN CUALQUIER GARANTÍA, EXPRESA O IMPLÍCITA, INCLUIDAS, SIN LIMITACIÓN, LAS GARANTÍAS DE COMERCIABILIDAD, ADECUACIÓN A UN FIN DETERMINADO E INCUMPLIMIENTO, ASÍ COMO LAS RESULTANTES DE GESTIONES, USO O PRÁCTICA COMERCIAL. NI CISCO NI SUS PROVEEDORES ASUMIRÁN EN NINGÚN CASO LA RESPONSABILIDAD POR CUALQUIER DAÑO INDIRECTO, ESPECIAL, CONSECUENCIAL O ACCIDENTAL, INCLUIDOS, SIN LIMITACIÓN, LA PÉRDIDA DE BENEFICIOS O LA PÉRDIDA O DAÑOS DE LOS DATOS DERIVADOS DEL USO INDEBIDO DE ESTE MANUAL, AUN CUANDO SE HUBIESE AVISADO A CISCO O SUS PROVEEDORES DE LA POSIBILIDAD DE QUE SE ORIGINASEN DICHOS DAÑOS.

LOS DISEÑOS ESTÁN SUJETOS A CAMBIOS SIN PREVIO AVISO. LA RESPONSABILIDAD DE LA APLICACIÓN DE LOS DISEÑOS RECAE EXCLUSIVAMENTE SOBRE LOS USUARIOS. LOS DISEÑOS NO CONSTITUYEN ASESORAMIENTO TÉCNICO O PROFESIONAL NI DE CUALQUIER OTRO TIPO DE CISCO, SUS PROVEEDORES O PARTNERS. EL USUARIO DEBE CONSULTAR A SUS PROPIOS ASESORES TÉCNICOS ANTES DE PROCEDER A LA IMPLEMENTACIÓN DE LOS DISEÑOS. LOS RESULTADOS PODRÍAN VARIAR EN FUNCIÓN DE FACTORES QUE CISCO NO HAYA PROBADO.

La implementación por parte de Cisco de la compresión del encabezado de TCP es una adaptación de un programa desarrollado por la Universidad de California, Berkeley (UCB), como parte de la versión de dominio público del sistema operativo UNIX de la UCB. Todos los derechos reservados. Copyright © 1981. Regentes de la Universidad de California.

Las direcciones de protocolo Internet (IP) y los números de teléfono utilizados en este documento no pretenden indicar direcciones y números de teléfono reales. Los ejemplos, los resultados en pantalla de los comandos, los diagramas topológicos de la red y otras figuras incluidas en el documento sólo tienen fines ilustrativos. El uso de direcciones IP o números de teléfono reales en el material ilustrativo no es intencionado, sino mera coincidencia.

Concepto “Bring Your Own Device (BYOD)” de Cisco

Concepto “traiga su propio dispositivo” de Cisco

Introducción

El concepto “traiga su propio dispositivo” (Bring Your Own Device o BYOD, por sus siglas en inglés) se ha convertido en una de las tendencias que más han influido e influirán a las organizaciones de TI. Este concepto define una tendencia a gran escala que están implementando los departamentos de TI y que supone un cambio drástico en el modo en que se utilizan los dispositivos en el lugar de trabajo.

¿Qué es BYOD? ¿Implica que los empleados tendrán que pagar por los dispositivos que utilicen para su trabajo? Es posible, pero BYOD es mucho más que eso. Se trata de que los usuarios finales puedan elegir los dispositivos informáticos y de comunicación que quieran utilizar con el fin de aumentar la productividad y la movilidad. Los dispositivos puede adquirirlos el empleador, el empleado o ambos. La implementación de BYOD supone que cualquier dispositivo pueda utilizarse en cualquier lugar, independientemente de quién sea su propietario.

En este documento se describe cómo afectará esta tendencia a la actividad empresarial, se analizan los desafíos que puede presentar a los departamentos de TI y se describen las tecnologías de Cisco® que forman parte de la solución. Cisco ofrece una completa arquitectura para superar los posibles desafíos y otorga a los usuarios finales la libertad de elegir los dispositivos que desean utilizar en su trabajo, sin privar por ello a los departamentos de TI del control que aplican para garantizar la seguridad y evitar la pérdida de datos.

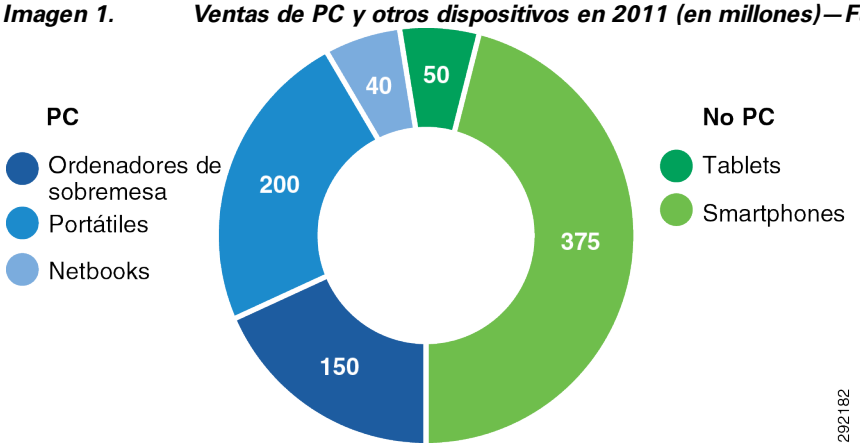
Objetivos empresariales

Para comprender los desafíos asociados con BYOD, resulta muy útil entender las tendencias empresariales que han propiciado la adopción de la iniciativa BYOD.

Dispositivos de consumo

Antes, las empresas proporcionaban a los empleados ordenadores de escritorio y portátiles, que solían ser las herramientas más avanzadas a las que estos tenían acceso. Con la proliferación de dispositivos de consumo, como portátiles, tablets, netbooks, smartphones, e-readers, etc., actualmente los empleados disponen de algunas de las herramientas de productividad más avanzadas para su uso personal. Pronto los empleados plantearon a sus departamentos de TI la siguiente cuestión: ¿por qué no utilizar en su trabajo esas herramientas que aumentan considerablemente la productividad? Muchas organizaciones de TI rechazaron en principio la idea por razones de seguridad y por la imposibilidad de ofrecer soporte y aprobar un número de dispositivos creciente.

Imagen 1. ***Ventas de PC y otros dispositivos en 2011 (en millones)—Fuente: Deloitte, 2011***



Durante el pasado año, la insistencia de los usuarios finales para aprovechar sus tablets y smartphones a fin de aumentar la productividad, incluso aunque ello suponga que ellos mismos deban adquirir los nuevos dispositivos, ha hecho que muchos departamentos de TI adopten políticas menos restrictivas para permitir a los empleados funciones básicas de conectividad o, cada vez más, el acceso total a la red de TI y a las aplicaciones corporativas. Esta tendencia es probablemente irreversible y las organizaciones de TI deberán adaptarse rápidamente al fenómeno de los dispositivos de consumo.

Varias necesidades, varios dispositivos

Muchas personas disponen de un ordenador de escritorio o un portátil, además de un teléfono móvil para llamadas de voz. La mayoría de teléfonos móviles se han sustituido por smartphones que pueden ejecutar aplicaciones e incluyen cámara y acceso a Internet. Un gran número de smartphones y tablets son tan potentes y tienen tanta funcionalidad como los ordenadores de escritorio y portátiles, por lo que ofrecen una nueva gama de usos y aplicaciones.

Se especula que en el futuro bastará un solo dispositivo para cubrir todas las necesidades informáticas, de comunicación y de aplicaciones.

No obstante, hoy en día la mayoría piensa que se seguirán utilizando varios dispositivos adaptados a usos específicos. Por ejemplo, un portátil no es, de hecho, tan portátil como un smartphone, por lo que es probable que los usuarios utilicen un smartphone para sus comunicaciones móviles. Las tablets son también dispositivos potentes, pero probablemente seguirán utilizándose ordenadores de escritorio y portátiles para la creación y edición de documentos. Por ello, es probable que los usuarios sigan utilizando varios dispositivos, pues la posibilidad de que se desarrolle un dispositivo que sirva para todas las tareas es reducida.

Imagen 2. *Variedad de dispositivos*

Como consecuencia de esta tendencia, aumenta el número de dispositivos que un mismo empleado o persona conecta a la red, a menudo de forma simultánea, lo que puede suponer un aumento considerable del número total de dispositivos conectados.

Superposición de la vida personal y laboral

Cada vez más, el trabajo se convierte en una actividad que las personas realizan, no un lugar al que acuden a diario. Una mayor capacidad de conectividad gracias al acceso remoto y móvil a la red corporativa ofrece a los empleados gran flexibilidad y mejora su productividad. También trae consigo que la diferencia entre vida personal y laboral sea cada vez menor, al añadir flexibilidad a los horarios de trabajo, pues los empleados pueden trabajar en el lugar y en el momento más oportuno, y esto en muchas ocasiones supone que se entrelacen las tareas laborales con las personales.

Uno de los efectos secundarios de esta flexibilidad es que los usuarios probablemente no deseen llevar sus dispositivos de trabajo y personales en todo momento y tener que alternar entre ellos. La mayoría de los empleados desea poder utilizar un único smartphone, tablet o portátil para el trabajo y para sus tareas personales y no tener que llevar consigo los dispositivos de la empresa.

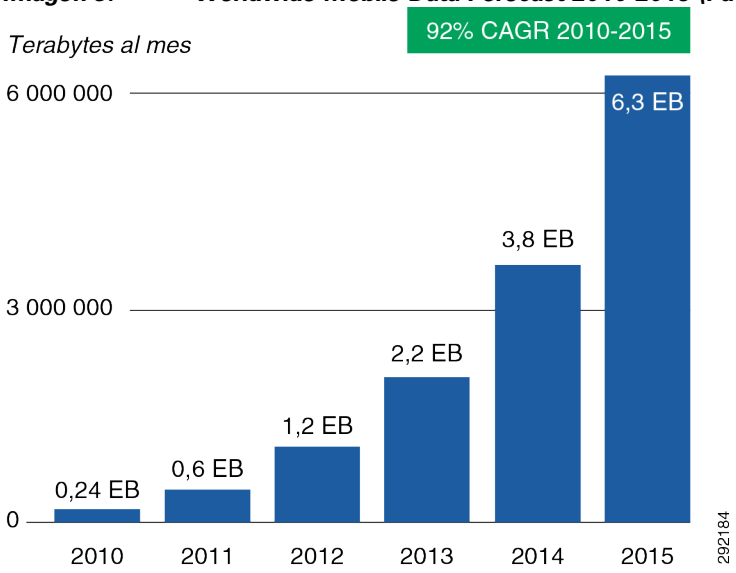
La propiedad de los dispositivos no está bien definida. A muchos empleados les gustaría utilizar su propio smartphone o tablet para acceder a las aplicaciones que utilizan para su trabajo, por ejemplo. Del mismo modo, muchas empresas se plantean la aplicación de programas de subvención, mediante los cuales se asigna a los empleados un dinero para la adquisición de los dispositivos, pero no tienen libertad a la hora de elegirlos.

La consecuencia de este solapamiento de tiempo y dispositivos es que los datos corporativos y personales estarán cada vez más mezclados en los dispositivos, lo que generará nuevos desafíos en materia de privacidad y seguridad.

Movilidad en cualquier momento y lugar

Se estima que los dispositivos móviles y el tráfico que generan en la red se multiplicarán por 26 entre 2010 y 2015, debido a la aparición de smartphones y tablets más potentes y a que los usuarios demandan cada vez más el acceso a Internet y a las aplicaciones desde cualquier lugar y siempre que lo deseen. Para lograrlo, será necesario que las empresas creen redes Wi-Fi, que los proveedores móviles creen redes 3G y 4G y que se establezcan redes Wi-Fi públicas para minoristas, municipios, etc.

Imagen 3. ***Worldwide Mobile Data Forecast 2010-2015 (Fuente: Cisco Visual Networking Index, 2011)***



Cuanto mayor sea el número de empleados que puedan acceder fácilmente a sus aplicaciones de trabajo mediante redes móviles y Wi-Fi, más se extenderán estas redes y, por tanto, mayor será la posibilidad de acceso. El resultado final es la conectividad permanente en cualquier lugar y en todo momento, y ello supone que las redes corporativas tendrán más dispositivos conectados con mayor frecuencia y será necesario por tanto que las aplicaciones estén disponibles de forma ininterrumpida.

Aplicaciones multimedia, de colaboración y de vídeo

Las comunicaciones de carácter personal y laboral emplean cada vez más elementos multimedia, lo que genera un aumento en el tráfico de vídeo y archivos multimedia de la red. Las aplicaciones de colaboración y la movilidad permanente seguirán haciendo que crezca el uso de elementos multimedia.

Con el uso por parte de los empleados de las aplicaciones de colaboración y la adopción de la movilidad como estilo de trabajo, la demanda de infraestructuras Wi-Fi y móviles será cada vez más pronunciada. Otro impulsor de esta tendencia es la integración de las funciones en dispositivos de consumo más potentes, que generalmente incluyen cámaras y vídeo de alta definición (HD). A medida que aumente el ancho de banda y los servicios 4G y Wi-Fi disponibles, serán más frecuentes las aplicaciones que permiten la transmisión de medios HD.

La experiencia con muchos smartphones y tablets es la mejor posible hoy por hoy, pero se espera que se alcance una mayor calidad de producción en el futuro. Los dispositivos de comunicación y colaboración seguirán alimentando la necesidad de disfrutar de aplicaciones móviles de vídeo HD y colaboración.

Desafíos para las organizaciones de TI

La adopción de BYOD presenta una serie de desafíos a las organizaciones de TI. Muchas de las ventajas de BYOD, como la posibilidad de utilizar cualquier dispositivo en cualquier lugar y con acceso permanente, se contraponen de algún modo a los requisitos de seguridad y soporte tradicionales de los departamentos de TI.

Opción de dispositivos y soporte

Tradicionalmente, los departamentos de TI elaboraban previamente una lista de dispositivos aprobados para el lugar de trabajo, que solía consistir en un ordenador de escritorio o un portátil estándar, y quizá un pequeño conjunto estandarizado de teléfonos móviles y smartphones. Los empleados podían elegir entre estos dispositivos, pero, por regla general, debían limitarse a la lista de dispositivos aprobados.

Con la implementación de BYOD, los departamentos de TI deben abordar el problema de forma diferente. Los dispositivos evolucionan a tal velocidad que no resulta práctico aprobar previamente cada una de las marcas o diseños Tampoco es útil que las organizaciones de TI ofrezcan el mismo nivel de soporte para cada uno de los dispositivos que los empleados puedan llevar al lugar de trabajo.

De ahí que la mayoría de las organizaciones de TI deban establecer, a nivel general, el tipo de dispositivos a los que permitirán el acceso a la red, excluyendo quizá alguna categoría o marca por motivos de seguridad u otros factores. También deben considerar el tipo de asistencia, como la adopción de más modelos de soporte asistido por TI o de autoasistencia.

Mantener el acceso seguro a la red corporativa

La posibilidad de elegir el dispositivo no tiene por qué afectar al nivel de seguridad. Los departamentos de TI deben establecer unos requisitos mínimos de seguridad que cumplan todos los dispositivos que se utilicen en la red corporativa, y que incluyan seguridad Wi-Fi, acceso a VPN y quizá software complementario de protección contra malware.

Además, debido al gran número de dispositivos del mercado, resulta fundamental poder identificar cada dispositivo que se conecta a la red y autenticar tanto el dispositivo como a la persona que lo utiliza.

Incorporación de nuevos dispositivos

La mayoría de las implementaciones de BYOD supondrán la incorporación de una amplia gama de dispositivos, como ordenadores de sobremesa, portátiles, netbooks, smartphones, tablets, e-readers y dispositivos de colaboración. Es probable que algunos dispositivos sean propiedad de la empresa y estén gestionados por ella, mientras que otros los habrá adquirido el empleado y sea este quien deba encargarse también del soporte.

La incorporación de nuevos dispositivos (el uso de un dispositivo en la red por primera vez) debería realizarse idealmente de forma sencilla y con la mínima intervención del departamento de TI, especialmente en el caso de los dispositivos adquiridos por los empleados. Es necesario además que los departamentos de TI puedan aplicar actualizaciones en los dispositivos de nueva incorporación si ello es necesario.

La incorporación debería realizarse idealmente sin intervención de clientes, es decir, sin necesidad de la instalación previa de software. Esto supone una ventaja adicional: si se implementa correctamente un modelo de incorporación de autoservicio, podrá ampliarse fácilmente para permitir también el acceso de invitados.

Aplicación de políticas de uso de la empresa

Las empresas cuentan con una amplia gama de políticas que deben aplicar en función del sector y de su normativa, así como de las políticas explícitas propias de la empresa. La adopción de BYOD debe proporcionar un modo de hacer cumplir las políticas, que pueden suponer un mayor desafío para dispositivos de consumo como tablets y smartphones.

Otra complicación surge al realizar tareas personales y profesionales con un mismo dispositivo. Es probable que los smartphones se utilicen para llamadas profesionales y personales y que las tablets tengan instaladas aplicaciones de uso laboral y personal. El acceso a Internet, el uso de archivos compartidos de igual a igual o el uso de las aplicaciones pueden estar sujetos a diferentes políticas si el usuario los utiliza con carácter personal en su propia red o si lo hace en la red corporativa en sus horas de trabajo.

Visibilidad de los dispositivos en la red

Tradicionalmente, los empleados disponían de un único ordenador de escritorio o portátil en la red y posiblemente un teléfono IP de escritorio. Cuando un empleado solicitaba asistencia del departamento de TI, resultaba muy sencillo localizar el dispositivo del usuario en la red y resolver el problema.

Con la adopción de BYOD, es probable que cada empleado cuente con tres, cuatro o incluso más dispositivos conectados a la red simultáneamente. Muchos de los dispositivos incluyen varios modos que permiten pasar de Ethernet por cable a Wi-Fi o redes móviles 3G/4G, por lo que es posible alternar entre los diferentes modos de conectividad durante la misma sesión. Es primordial para los departamentos de TI disponer de las herramientas necesarias para poder visualizar todos los dispositivos de la red corporativa y más allá de ella.

Protección y prevención de la pérdida de datos

Uno de los principales desafíos derivados de la implementación de BYOD es garantizar la protección de los datos corporativos. Cuando un recurso corporativo, como un portátil, se utiliza para acceder a los datos y aplicaciones de la empresa, por lo general lo controla el departamento de TI y es probable que esté sujeto a políticas de uso más restrictivas.

En algunos sectores deben cumplirse normativas de confidencialidad como HIPAA, reglamentos de cumplimiento de seguridad como PCI, o normativas de seguridad con carácter general, como Sarbanes-Oxley, entre otras. Las empresas deben demostrar que con la adopción de BYOD es posible adherirse al cumplimiento de estas normas, lo que puede resultar más complicado que con los dispositivos propiedad de la empresa y gestionados por ella.

Un smartphone o tablet propiedad del empleado es muy probable que se utilice de forma habitual para aplicaciones empresariales y para tareas personales. Los servicios de almacenamiento y uso compartido de archivos en la nube son útiles para gestionar datos personales, pero pueden generar una potencial filtración de datos.

Los departamentos de TI deben establecer una estrategia de protección de los datos corporativos en todos los dispositivos, ya sean gestionados por la empresa o autogestionados por el empleado. Dicha estrategia puede incluir una partición empresarial segura en el dispositivo que actúe como un contenedor para los datos corporativos, que pueden de este modo controlarse de forma estricta. Puede incluir además la necesidad de una aplicación de estructura de escritorio virtual (VDI) para permitir el acceso a los datos confidenciales sin almacenarlos en el dispositivo.

Revocación del acceso

En un momento determinado del ciclo de vida de un dispositivo o empleado, puede que sea necesario revocar el acceso al dispositivo. Esto podría deberse a la pérdida o robo del dispositivo, a la finalización del contrato del empleado o incluso a un cambio en el cargo del empleado dentro de la compañía.

Es necesario que los departamentos de TI puedan revocar rápidamente el acceso que se haya autorizado para cualquier dispositivo, así como borrar de forma remota parte o la totalidad de los datos (y aplicaciones) en él incluidos.

Posibilidad de nuevos vectores de ataque

Dado que los dispositivos que acceden a la red corporativa incluyen una gran variedad de funciones y que el departamento de TI podría no ser capaz de analizar, clasificar y aprobar cada dispositivo, existe la posibilidad de nuevos vectores de ataques de seguridad.

Por ejemplo, muchas tablets tienen capacidad de admitir una WLAN ad hoc. Si un dispositivo autenticado tiene otros dispositivos vinculados a él a través de una WLAN ad hoc, usuarios y dispositivos no autenticados podrían acceder a la red corporativa a través del dispositivo autenticado. Esto también se aplica en el caso de la vinculación de un portátil mediante Bluetooth a través de un smartphone.

El desafío para los departamentos de TI es cómo permitir el uso del creciente número de dispositivos y funciones sin perder el control para hacer cumplir las políticas, como la desactivación automática de la función de WLAN ad hoc en un dispositivo conectado autorizado.

Garantizar la fiabilidad y el rendimiento de la red LAN inalámbrica

A medida que aumenta el dominio del acceso inalámbrico, las expectativas de rendimiento y fiabilidad son las mismas que las esperadas de una red por cable, incluidas la conectividad fiable, el rendimiento y el tiempo de respuesta de las aplicaciones, así como las cada vez más numerosas aplicaciones de voz, vídeo y otras aplicaciones de colaboración en tiempo real.

Este cambio fundamental requiere que los departamentos de TI modifiquen el nivel de servicio de la red WLAN corporativa para pasar de un nivel cómodo a un nivel de red de negocio de extrema importancia, similar a la red por cable. El diseño y el funcionamiento de la red WLAN deben incluir la alta disponibilidad, el control del rendimiento y la mitigación, además del roaming sin fallos.

Gestión del aumento en el número de dispositivos conectados

El creciente número de dispositivos conectados a la red, probablemente varios dispositivos por usuario conectados simultáneamente, puede traer consigo la escasez de direcciones IP, ya que la mayoría de los planes de IP anteriores se crearon contando con un número menor de dispositivos. Esto podría hacer más acuciante la necesidad de realizar implementaciones de IPv6 tanto en la frontera de Internet como dentro de la red de la empresa.

Desafíos para los usuarios finales

La demanda de iniciativas BYOD se debe en gran medida al deseo de los usuarios de poder elegir los dispositivos que utilizan para su trabajo. Desde la perspectiva del usuario, estos son algunos de los desafíos que se presentan:

Sencillez

Las soluciones y tecnologías BYOD evolucionan a gran velocidad. Sin embargo, uno de los principales desafíos consiste en simplificar la conexión a los recursos corporativos y el uso de los mismos. El número de opciones de dispositivos, la variedad de tipos de conexión y ubicaciones, y la falta de enfoques adoptados ampliamente pueden suponer un obstáculo para los usuarios.

Cada marca y formato de dispositivo puede requerir pasos ligeramente diferentes para su incorporación y conexión. Los pasos y medidas de seguridad podrían variar también en función del modo y el lugar en el que el usuario intente la conexión. Por ejemplo, la red Wi-Fi de la empresa podría requerir el uso de credenciales, mientras que la conexión a través de una zona Wi-Fi pública podría requerir credenciales, una red privada virtual (VPN) y otros pasos de seguridad.

Por último, cualquier solución BYOD debe ser tan sencilla como sea posible para los usuarios, proporcionar una experiencia común independientemente del lugar o el momento de la conexión y ser similar para todos los dispositivos en la medida de lo posible.

Uso de dispositivos personales para el trabajo

BYOD permite realizar tareas personales y profesionales en el mismo dispositivo. Las listas de contactos, el correo electrónico, los archivos de datos, las aplicaciones y el acceso a Internet pueden presentar también importantes desafíos. Idealmente, los usuarios desearían separar sus datos y actividades personales de los profesionales. Las fotos, mensajes de texto y llamadas personales, así como los sitios de Internet visitados con carácter particular, están sujetos a las políticas de privacidad personal, mientras que los documentos, archivos y aplicaciones que utilizan datos corporativos, y el historial de navegación de Internet durante las horas de trabajo deberán regirse por las políticas corporativas.

Algunas empresas supeditan las conexiones con dispositivos propiedad de los empleados a la firma de un acuerdo por el cual la empresa puede supervisar el cumplimiento, a la aceptación de políticas de uso y a otras acciones destinadas a proteger los datos corporativos. En algunos casos, podría incluirse el borrado remoto de todos los datos del dispositivo (que podrían incluir datos personales), que obviamente puede ser una causa de enfrentamiento entre el departamento de TI y los usuarios si no se aborda correctamente.

Obtener la productividad y la experiencia necesarias

Tal y como se ha tratado anteriormente, uno de los principales generadores de iniciativas BYOD es que los empleados desean aprovechar en su trabajo las herramientas de productividad que utilizan habitualmente en sus dispositivos personales. Las empresas quieren obtener y sacar partido de esa productividad pero también necesitan aplicar las políticas y medidas de seguridad necesarias para proteger los datos corporativos.

Si estas medidas de seguridad son demasiado severas, podrían anular las ganancias en la productividad. Por ejemplo, una queja habitual es que las empresas que bloquean el acceso a las aplicaciones empresariales y a los datos mediante la implementación de clientes VDI en dispositivos tablet rebajan la experiencia del usuario hasta el punto que el empleado no obtiene la experiencia propia de una tablet. Es probable que los clientes VDI mejoren, incluida la experiencia del usuario, pues continúan creciendo las implementaciones de tablets y smartphones.

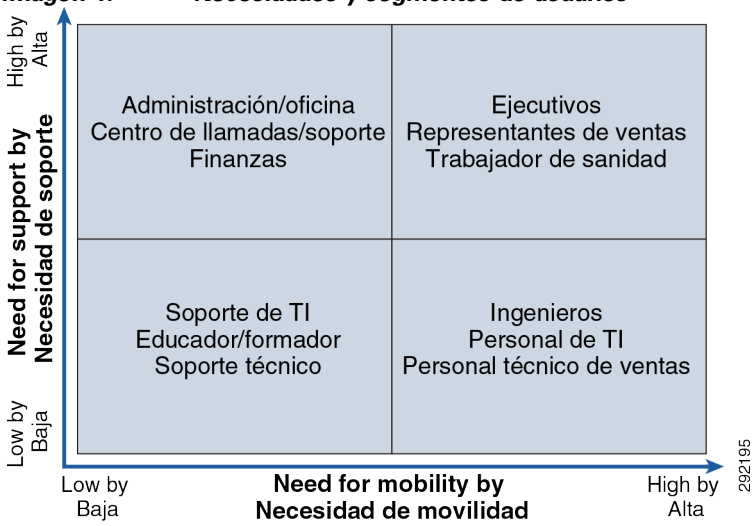
Consideraciones para la adopción de BYOD

Para cualquier adopción generalizada de BYOD, deben tenerse en cuenta previamente ciertas consideraciones.

Comprender las necesidades y segmentos de los usuarios

Es importante tener en cuenta que existen diferentes segmentos de usuarios en cualquier implementación de BYOD. Se recomienda realizar un análisis de los segmentos de usuarios dentro de la empresa para poder entender las necesidades y el nivel de soporte necesarios. Un ejemplo de ello se muestra en Imagen 4.

Imagen 4. ***Necesidades y segmentos de usuarios***



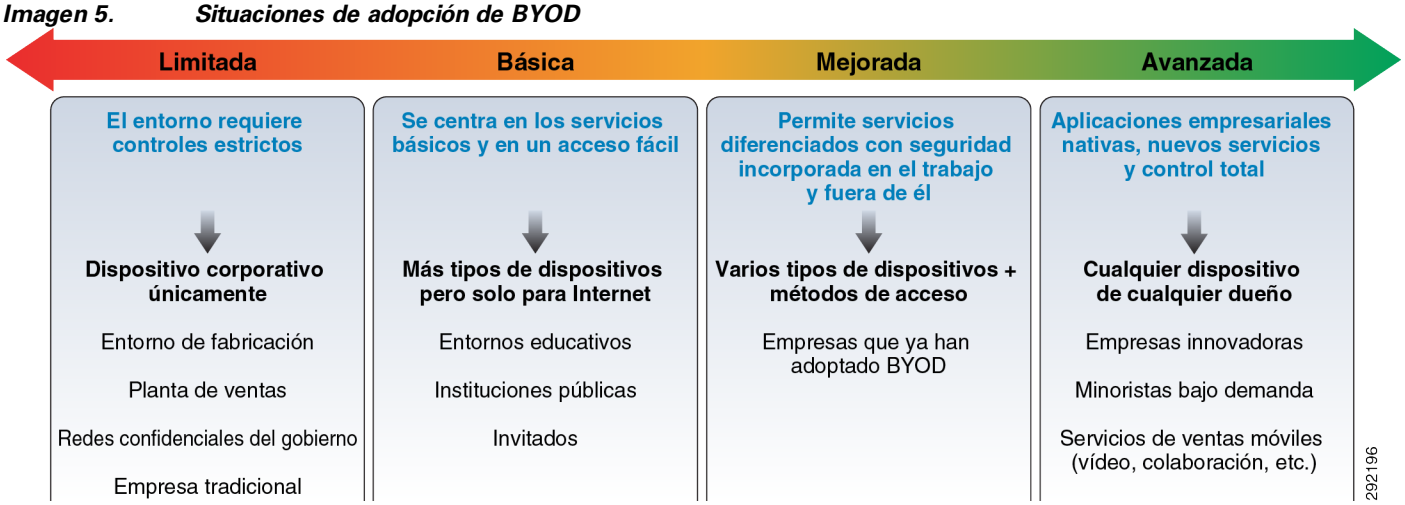
Cada empresa es diferente. Imagen 4 analiza las funciones de los empleados teniendo en cuenta las necesidades de movilidad y aplicaciones móviles, y el probable nivel de asistencia que necesitarán. Las implementaciones de BYOD son sencillas en el caso de usuarios que solo requieren niveles bajos de asistencia de TI y que probablemente utilizan comunidades de autoasistencia en las que se comparten las mejores prácticas. Las implementaciones serán más complejas con usuarios con mayor necesidad de movilidad y que necesitarán un mayor nivel de asistencia, como es el caso de los ejecutivos.

Realizar este tipo de análisis ayudará a comprender las políticas de derechos y los modelos de asistencia, y puede evitar frustraciones y gastos excesivos en el presupuesto de TI.

Elección de una estrategia de adopción de BYOD

Las diferentes empresas abordarán la implementación de BYOD con diferentes expectativas entre los múltiples escenarios de adopción posibles. Todas las empresas precisan de una estrategia de BYOD, incluso si su intención es rechazar cualquier dispositivo excepto los que hayan sido aprobados y sean gestionados por el departamento de TI. Imagen 5 muestra una serie de posibles situaciones de adopción que se corresponden con la mayoría de las empresas.

Imagen 5. ***Situaciones de adopción de BYOD***



Las empresas pertenecientes a sectores con un gran nivel de regulación, como el sector financiero o las agencias gubernamentales de seguridad, podrían necesitar un enfoque más restrictivo en la adopción de BYOD para proteger los datos confidenciales. Es posible que los dispositivos deban someterse a un control y gestión estrictos, como en el enfoque de TI tradicional, que puede seguir siendo válido en estos casos.

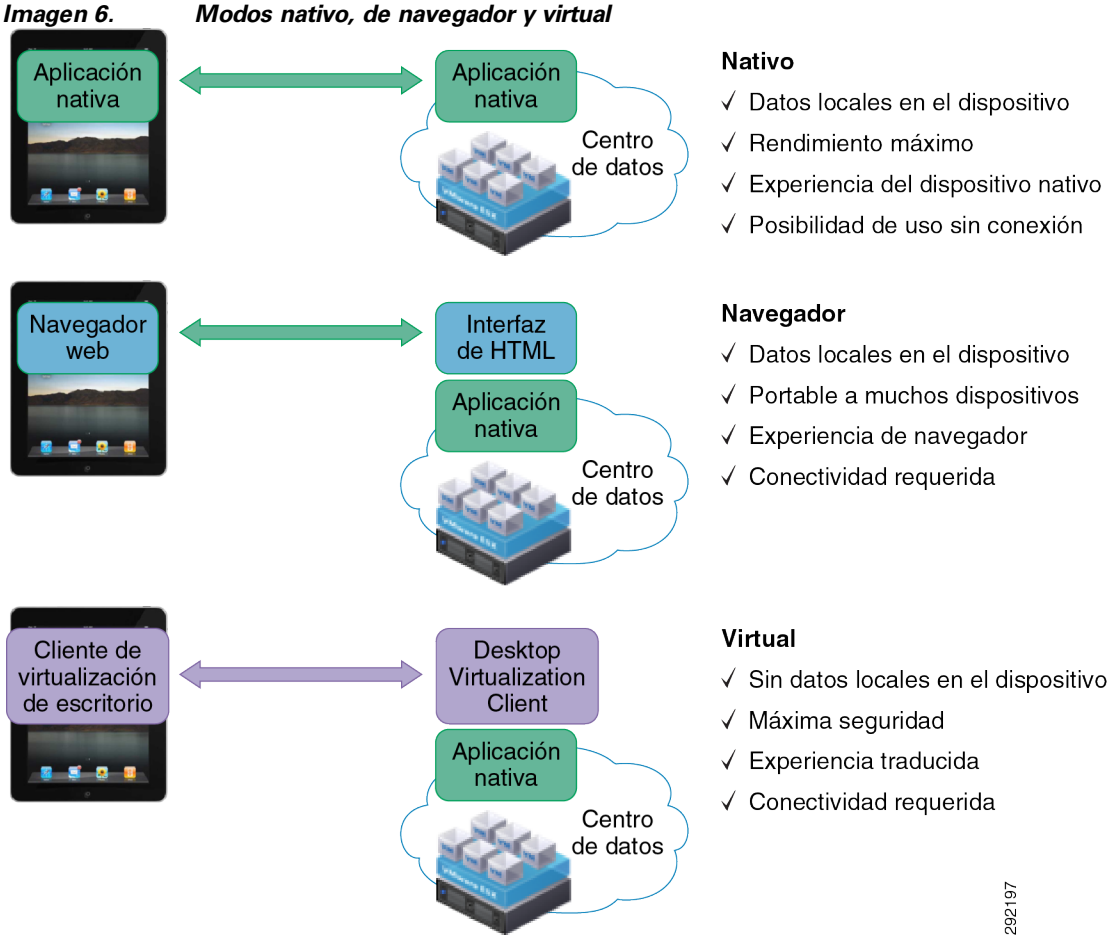
Para muchas empresas, la adopción puede abarcar desde permitir un conjunto de dispositivos con acceso restringido a las aplicaciones, hasta la aplicación completa de BYOD, que fomenta la amplia adopción de muchos de los tipos de dispositivos, si no todos, y la implementación de medidas de seguridad que permitan el acceso a un gran número de aplicaciones y datos empresariales. En el sentido más amplio, algunas compañías adoptarán una estrategia de "móvil primero", por la cual se dará prioridad al desarrollo de sus propias aplicaciones internas en tablets y smartphones, con lo que se persigue lograr una ventaja frente a la competencia al aprovechar un conjunto más amplio de herramientas y dispositivos.

Ser capaces de entender la posición actual y futura de su empresa dentro del espectro de situaciones de adopción resulta de gran utilidad para determinar la estrategia general, los derechos y las políticas de seguridad aplicables para la iniciativa BYOD.

Consideración de estrategias de aplicaciones

La seguridad y la prevención de la pérdida de datos corporativos es una de las principales preocupaciones a la hora de implementar BYOD. Es importante entender las tres posibles arquitecturas de aplicación y los desafíos que representan: modos nativo, de navegador y virtual. Puede verlos en Imagen 6.

Imagen 6. ***Modos nativo, de navegador y virtual***



En el modo nativo, las aplicaciones que se ejecutan en el dispositivo se comunican directamente con el servidor de aplicaciones del Data Center que las aloja (o nube). Los datos pueden intercambiarse y almacenarse directamente en el dispositivo BYOD. Normalmente, el rendimiento de las aplicaciones y la experiencia de usuario dependen del dispositivo en particular. Esto quiere decir que una aplicación empresarial funcionará del mismo modo que cualquier otra aplicación instalada en el dispositivo. Se mantienen todas las ventajas de productividad y el comportamiento del dispositivo y las aplicaciones pueden personalizarse para ofrecer una experiencia óptima.

Cada vez está más extendido el uso del enfoque de navegador para el acceso a las aplicaciones dada la facilidad de portabilidad entre dispositivos y sistemas operativos. Básicamente, puede utilizarse cualquier dispositivo con un navegador HTML estándar para acceder a la aplicación. Las desventajas son similares a las del modo nativo, es decir, el hecho de que los datos se intercambien y almacenen directamente en el dispositivo BYOD supone ciertos riesgos de seguridad y pérdida de datos. Además, la experiencia de usuario podría verse reducida.

Por el contrario, en el modo virtual las aplicaciones se encuentran en el servidor de aplicaciones del Data Center (o la nube) y se representan en el dispositivo a través de un cliente VDI. Los datos no se almacenan localmente en el dispositivo BYOD. Solo la información que se visualiza puede intercambiarse y utilizarse en el dispositivo BYOD. Aunque este método ofrece la máxima protección de los datos, la experiencia del usuario puede no ser tan buena debido al paso del servidor de aplicaciones al diseño, y del sistema operativo nativos al dispositivo BYOD. Aquellos que ya han adoptado este enfoque han proporcionado comentarios que son en cierto modo negativos.

Es importante tomar decisiones sobre qué modo, nativo o virtual, se utilizará para la arquitectura de la aplicación. Muchas empresas podrían optar por un enfoque híbrido y aplicar el modo nativo para muchas aplicaciones empresariales estándar y el modo virtual para un subconjunto de aplicaciones que requieran unos requisitos de confidencialidad de los datos más estrictos.

Ampliación de la colaboración a los dispositivos BYOD

En última instancia, los usuarios no solo quieren conectarse a la red para acceder a aplicaciones de datos, sino también para colaborar con otras personas. Al igual que en los espacios de trabajo tradicionales, los usuarios que utilizan dispositivos BYOD desean acceder a los servicios de voz, vídeo y teleconferencia de su empresa.

Los enfoques independientes, como depender de las comunicaciones de telefonía móvil de los smartphones, pueden ofrecer cierta eficacia. Sin embargo, para disfrutar de una verdadera eficacia, es necesario adoptar un enfoque integrado que consiga que los usuarios estén fácilmente accesibles dentro de los directorios y sistemas de telecomunicaciones de la empresa. Otro aspecto a considerar es cómo ampliar entonces estos servicios a dispositivos sin capacidades de voz de telefonía móvil, como los iPads de Apple.

Una solución BYOD completa debe dar respuesta a la forma de ampliar el conjunto completo de aplicaciones de colaboración a los dispositivos BYOD, incluidas las tecnologías integradas de voz, vídeo, mensajería instantánea, teleconferencia, uso compartido de aplicaciones y telepresencia. Toda solución debe tener en cuenta no solamente a los empleados que utilizan dispositivos BYOD, sino también a otros usuarios que intenten colaborar con ellos.

Disponer de un acuerdo de usuario final que abarque todos los aspectos relevantes

A pesar de que no forma parte de la arquitectura de red, debe considerarse el uso de un acuerdo de usuario final (EUA) antes de llevar a cabo la implementación de BYOD. Debido a la mezcla de datos personales y corporativos, y los riesgos potenciales que supone el uso de dispositivos propiedad del empleado para la actividad profesional, resulta fundamental el establecimiento de políticas y su comunicación a los empleados con la suficiente antelación.

Las organizaciones de TI deberán estar familiarizadas con la legislación, incluida la ley sobre el abuso y fraude informático Computer Fraud and Abuse Act, la ley de interceptación de comunicaciones Wiretap Act y la ley de asistencia en comunicaciones Communications Assistance for Law Enforcement Act (CALEA).

¿En qué consistirán las políticas de la empresa? ¿Se monitorizarán las comunicaciones? ¿Se aplicarán las políticas en el aspecto personal además del profesional? Las áreas que se tratarán incluyen las siguientes, aunque no se limitan a ellas:

- Mensajería de texto
- Llamadas de voz
- Navegación por Internet
- Mensajería instantánea
- Correo electrónico
- Información de GPS y ubicación geográfica
- Aplicaciones compradas/instaladas
- Fotografías y vídeos almacenados
- Borrado del dispositivo

Por ejemplo, muchas empresas filtran y monitorizan con regularidad el acceso a Internet con el fin de garantizar el cumplimiento de las políticas contra el acceso a sitios web no autorizados en el trabajo. La mayoría de dispositivos BYOD tienen acceso directo a Internet mediante red Wi-Fi pública o acceso a Internet móvil 3G/4G. Sería normal contar con una política de control del acceso a sitios web no autorizados en un dispositivo conectado a través de la red corporativa. ¿Se aplicará la misma política si el empleado decide acceder a esos sitios desde su propio dispositivo con carácter privado a través de una red pública de acceso a Internet?

Otro ejemplo sería la aplicación habitual de políticas contra el envío de mensajes inapropiados que contengan fotos muy personales a través de correo electrónico o mensaje de texto utilizando un dispositivo propiedad de la empresa o la red corporativa. ¿Se aplicarán las mismas políticas a los mensajes de correo electrónico o mensajes de texto personales en un dispositivo propiedad del empleado? ¿Se monitorizarán las comunicaciones? ¿Qué contenido no se monitorizará?

Recientemente ha habido varias disputas legales relacionadas con casos en los que un empleador había borrado de forma remota los datos del dispositivo propiedad de un empleado, tanto los profesionales como los de carácter personal. Como empleado, imagine cuál sería su sorpresa si al utilizar su nueva tablet para acceder a la red corporativa aceptara inconscientemente que el departamento de TI borre todas sus fotos familiares. Algunas situaciones de interceptaciones potencialmente ilegales en las que los empleados alegaban que sus empresas estaban monitorizando sus conversaciones por mensajería de texto de forma ilegal al no haber sido informados de ello, también suponen ciertos desafíos.

La clave para evitar responsabilidades legales es notificar en todo momento. Debe dejarse claro a los empleados en una política por escrito que deberán aceptar el modo en el que la empresa tratará las comunicaciones y los datos con carácter corporativo y personal en el dispositivo BYOD. También debe estar claro a qué derechos renuncia el empleado al aceptar el EUA con el fin de poder acceder a la red con un dispositivo de su propiedad.

Disponer de una política sobre dispositivos perdidos o robados

También es importante que las empresas dispongan de un plan sobre qué hacer en caso de pérdida o robo de los dispositivos. ¿Cuál es el proceso de notificación que deben seguir los empleados? ¿Qué pasos deben seguirse para impedir el acceso a la red corporativa? ¿Cuál es el proceso para borrar de forma remota los datos almacenados en el dispositivo?

Las diferentes soluciones del mercado ofrecen diversos grados de acceso remoto al dispositivo para borrar datos o aplicaciones con el fin de garantizar su confidencialidad. Deben tenerse en cuenta los tipos de datos que se almacenarán en los dispositivos BYOD e integrar planes de mitigación en la estrategia general BYOD antes de la implementación.

Arquitectura BYOD de Cisco

Cisco ofrece una completa arquitectura de la solución BYOD que combina elementos en toda la red para lograr un enfoque unificado que garantice el acceso seguro de los dispositivos, visibilidad y control mediante políticas. Para superar todos los desafíos que se han descrito anteriormente, la implementación de BYOD no debe realizarse de forma aislada, sino que debe integrarse en la red inteligente.

La solución BYOD de Cisco se basa en la arquitectura Cisco Borderless Network y asume que se siguen las mejores prácticas en el diseño de las infraestructuras de red en las implementaciones en instalaciones, sucursales, frontera de Internet y oficina en casa.

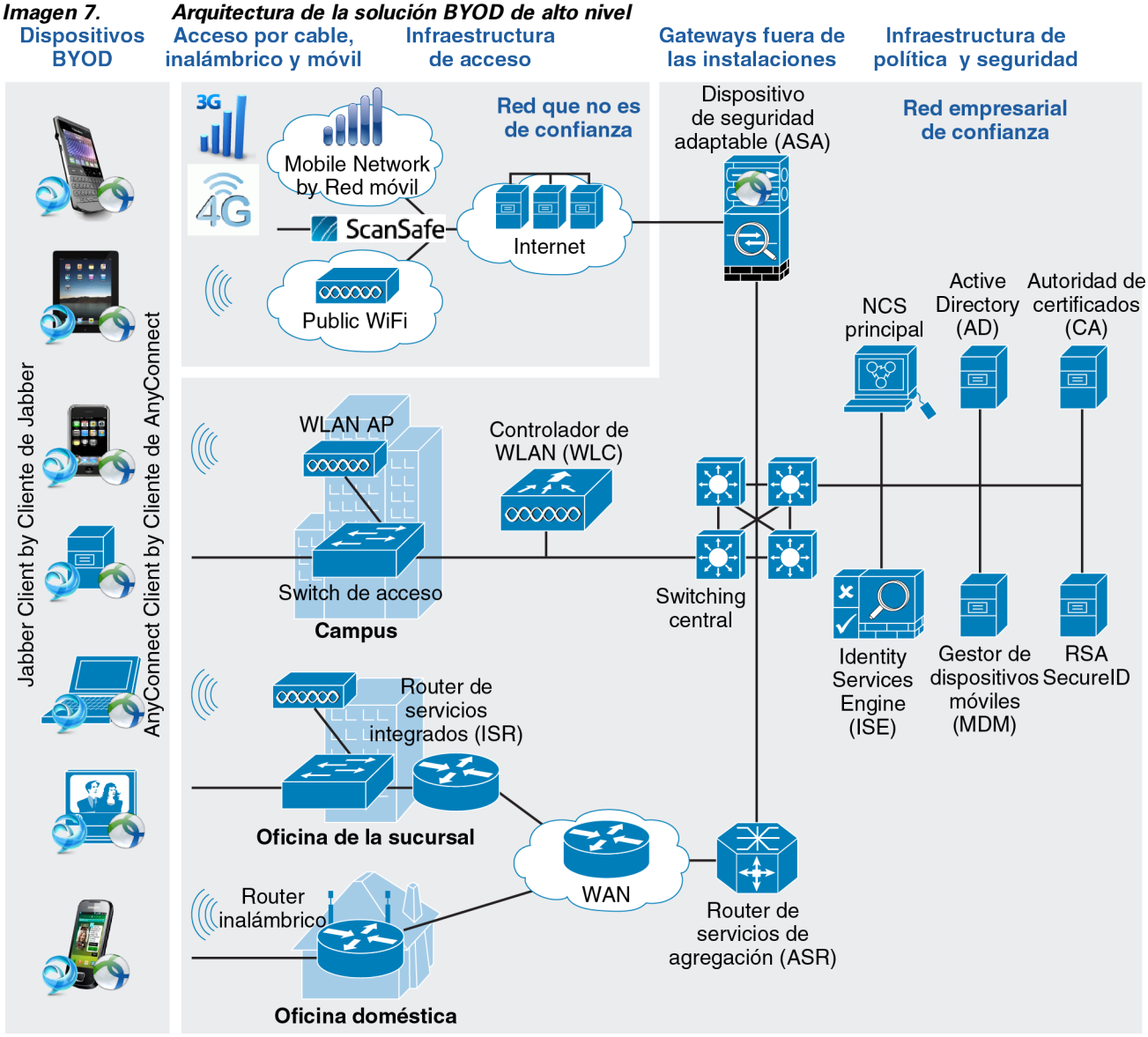
Arquitectura de solución de alto nivel

Una solución BYOD completa debe proporcionar acceso a la red por cable, Wi-Fi, remoto y móvil; debe admitir la mayoría de tipos y marcas de dispositivos; y debe aplicar las diversas políticas a todo el espectro de negocios y sectores. Además, puesto que los dispositivos pasan de un contexto a otro, por ejemplo, de una red Wi-Fi corporativa a una red móvil 3G/4G pública, la solución BYOD debe ser capaz de proporcionar acceso seguro sin que ello afecte a la calidad de la experiencia de usuario.

Es fundamental para cualquier estrategia BYOD considerar el acceso completo a la red corporativa, lo que implica no solo el acceso a la WLAN de la empresa, sino también el acceso por cable en las principales instalaciones, el acceso por cable e inalámbrico en sucursales y oficinas en casa, y el acceso remoto a través de Internet, 3G/4G móvil y zonas Wi-Fi públicas. Cualquier diseño que no tenga en cuenta la amplia gama de posibles contextos de acceso a la red resultará insuficiente a la hora de ofrecer una solución gestionable y ampliable para los departamentos de TI.

Imagen 7 muestra la arquitectura de solución de alto nivel y los principales componentes de la solución BYOD de Cisco.

Imagen 7. ***Arquitectura de la solución BYOD de alto nivel***



Componentes de las soluciones de Cisco

En las siguientes secciones se describen los diferentes componentes de Cisco que forman parte de la arquitectura de la solución y la función que desempeñan.

Switches Cisco Catalyst

Los switches Cisco Catalyst®, entre los que se incluyen los switches Catalyst de las series 3000, 4000 y 6000, proporcionan acceso por cable a la red y gestión de las solicitudes de autenticación de acceso a la red con 802.1x Además, los switches de acceso ofrecen alimentación a través de Ethernet (PoE) para dispositivos que requieren alimentación, como estaciones de trabajo VDI, teléfonos IP y puntos de acceso WLAN.

Routers de servicios integrados de Cisco

Los routers de servicios integrados (ISR) de Cisco, como ISR 1900, ISR 2900 o ISR 3900, ofrecen conectividad WAN para sucursales y oficinas domésticas, y conectividad para la infraestructura por cable y WLAN en sucursales. Además, los ISR pueden ofrecer conectividad directa a servicios en la nube e Internet, servicios de optimización WAN y aplicaciones, y pueden utilizarse además como puntos de terminación para conexiones VPN con dispositivos móviles.

Gracias a la función de aprovisionamiento seguro de dispositivos (SDP) del ISR, pueden utilizarse como autoridad de certificados (CA), lo que resulta muy útil para implementaciones de menor tamaño.

Puntos de acceso de LAN inalámbrica de Cisco

Los puntos de acceso de LAN inalámbrica (WLAN) de Cisco, como el AP3500 y el AP3600, ofrecen conectividad Wi-Fi para la red corporativa y gestión de las solicitudes de autenticación de acceso a la red a través de 802.1x. Además, la WLAN cuenta con funciones fundamentales para obtener una conectividad de los dispositivos móviles fiable y de alto rendimiento.

Controlador de LAN inalámbrica de Cisco

El controlador Cisco Wireless LAN Controller (WLC) se utiliza para automatizar la configuración inalámbrica y las funciones de gestión, así como para ofrecer visibilidad y control de la WLAN. El WLC es capaz de interactuar con Identity Services Engine (ISE) para aplicar políticas de autorización y autenticación en todos los terminales.

Dispositivo de seguridad adaptable Cisco Adaptive Security Appliance

El dispositivo de seguridad adaptable Cisco Adaptive Security Appliance (ASA) proporciona funciones de seguridad tradicionales, como firewall y el sistema de prevención de intrusiones (IPS), así como un importante punto de terminación VPN seguro (AnyConnect) para la conexión de dispositivos móviles a través de Internet, incluidas zonas Wi-Fi públicas y redes móviles 3G/4G.

Cliente Cisco AnyConnect

El cliente Cisco AnyConnect™ ofrece capacidad de suplicante 802.1x en redes de confianza y conectividad VPN para dispositivos que accedan a la red corporativa desde redes que no son de confianza, incluidas las redes públicas de Internet, zonas Wi-Fi públicas y redes móviles 3G/4G. La implementación y gestión de un único cliente suplicante tiene ventajas operativas y proporciona una experiencia y un procedimiento comunes para todos los usuarios.

Por otro lado, el cliente AnyConnect puede utilizarse para la evaluación del estado de los dispositivos en el dispositivo BYOD, además de como un nivel de aplicación de políticas y para aplicar políticas de uso.

Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) es un componente central de la arquitectura de la solución BYOD de Cisco y ofrece diversos servicios, entre los que se incluyen los siguientes:

- Portales de registro e inscripción de autoservicio
- Autenticación
- Autorización
- Definición de perfiles de dispositivos
- Registro y aprovisionamiento de dispositivos

- Inscripción de certificados
- Evaluación de estado
- Definición de políticas
- Interfaz para la identificación de almacenes (por ejemplo, Active Directory® [AD])
- Notificación e inclusión en lista negra de dispositivos perdidos o robados

Una de las funciones más importantes que ofrece Cisco ISE es la capacidad de tener una única ubicación para el registro de los dispositivos. La primera vez que se conectan los dispositivos a la red, pueden redirigirse a un portal de registro de autoservicio (o intervención de TI), donde los usuarios pueden registrarlos, inscribirlos y recibir autoaprovisionamiento en ellos. Este es un servicio esencial para aligerar la carga que debe abordar el departamento de TI al tener que manipular y preaprovisionar cada dispositivo de la red, además de proporcionarle visibilidad sobre los dispositivos que acceden a la red.

Además de las funciones centrales, como la autenticación y la autorización, Cisco ISE ofrece información acerca de los dispositivos que se conectan a la red mediante la creación de perfiles. La creación de perfiles de los dispositivos puede resultar de utilidad para detectar, localizar y determinar el tipo y la funcionalidad de los terminales que se conectan a la red y para rechazar o aplicar reglas de autorización específicas.

Por ejemplo, la combinación de la creación de perfiles de los dispositivos, la evaluación del estado y la aplicación de políticas puede utilizarse para hacer cumplir las políticas de BYOD, como las siguientes:

- Permitir el acceso a la red a iPads® propiedad de los empleados, pero solo para el tráfico HTTP
- Prohibir el acceso a la red de iPhones ® si están liberados
- Si el dispositivo Android™ es propiedad de la empresa, permitir el acceso total

Cisco Prime

Cisco Prime™ ofrece funciones de control y administración de redes, como la visibilidad de dispositivos y usuarios clave, además del aprovisionamiento de dispositivos de la red.

Cisco ScanSafe Cloud Web Security

Cisco ScanSafe amplía las capacidades de seguridad que tienen en sus instalaciones la mayoría de los clientes empresariales a través de una solución gestionada en la nube con el fin de proteger a los clientes que utilizan BYOD cuando se encuentran fuera del trabajo. Al indicar a los clientes que utilizan BYOD que accedan a Internet a través de la nube Scan Safe, se realiza un análisis de seguridad para filtrar el acceso web, detectar malware, identificar comportamientos anómalos y ofrecer a las empresas comentarios en tiempo real. Ampliar la protección de dispositivos BYOD es fundamental cuando el dispositivo abandona la red empresarial para evitar vectores de ataques de seguridad y riesgos cuando el dispositivo vuelve a conectarse a la red empresarial de las instalaciones.

Cisco Jabber

Cisco Jabber amplía la colaboración a dispositivos BYOD al integrar el dispositivo en el conjunto de productos de Comunicaciones Unificadas. El usuario puede utilizar fácilmente comunicaciones de voz y vídeo, acceder a mensajes de voz y comunicarse por mensajería instantánea. Los clientes de Jabber también participan en Presence, además de tener acceso a las mismas aplicaciones de teleconferencia y uso compartido de escritorio que desde ordenadores de empleados más tradicionales, como Cisco WebEx.

Imagen 8. *Cisco Jabber en iPads de Apple.*

Componentes de soluciones de terceros

En las siguientes secciones se describen los diferentes componentes de terceros (proveedores ajenos a Cisco) que forman parte de la arquitectura de la solución y la función que desempeñan.

RSA SecurID

El servidor de autenticación y los tokens RSA SecurID se utilizan para proporcionar servicios de autenticación en dos pasos (PIN secreto y código de contraseña único) para obtener mayor seguridad en las conexiones a través de VPN.

Gestor de dispositivos móviles

El gestor de dispositivos móviles (MDM) permite la gestión centralizada de terminales para varios sistemas operativos de dispositivos BYOD. La funcionalidad y el nivel de soporte dependen de los diferentes proveedores de MDM. No obstante, la funcionalidad típica incluye la configuración de los dispositivos, el cifrado en el dispositivo, la aplicación de contraseñas y el autoaprovisionamiento.

Aparte de las funciones relacionadas con el acceso a la red que se han descrito, el MDM también actúa como un importante servicio de seguridad en el dispositivo final, por lo que ofrece también servicios de autenticación de las aplicaciones.

La arquitectura de la solución BYOD de Cisco puede funcionar con diversas opciones de MDM como un componente opcional.

Autoridad de certificados

La autoridad de certificados (CA) se utiliza para emitir certificados digitales para los dispositivos con el fin de que se les permita el acceso a la red mediante la implementación de una infraestructura de clave pública (PKI). Existen diversas implementaciones de CA estándar que pueden utilizarse como parte de la solución BYOD. A efectos de este documento, la solución se validó con dos tipos de CA: servicios de CA de Microsoft® y el servicio de aprovisionamiento seguro de dispositivos (SDP) de Cisco IOS alojados en un ISR (consulte Routers de servicios integrados de Cisco).

Microsoft Active Directory

Microsoft Active Directory (AD) proporciona una base de datos central de identidades y grupos que muchas empresas utilizan habitualmente para la gestión centralizada de identidades. En lugar de duplicar un almacén de identidades, la arquitectura de la solución BYOD se validó utilizando AD como fuente de identidades externa para Cisco ISE.

Dispositivos admitidos

La solución BYOD de Cisco admite una amplia gama de dispositivos, pero su funcionalidad y capacidades pueden variar en función del dispositivo o del sistema operativo. Consulte las especificaciones de cada modelo para conocer la funcionalidad y las limitaciones de cada tipo de dispositivo. Tabla 1 muestra los tipos de dispositivo actualmente validados con la solución.

Tabla 1 Dispositivos admitidos

Dispositivo	Por cable	Red Wi-Fi corporativa	Red Wi-Fi pública	3G/4G móvil
Smartphones y tablets Android[1]		Sí	Sí	Sí
Apple® OS X® Mac®	Sí	Sí	Sí	
Apple iOS™ iPhone		Sí	Sí	Sí
Apple iOS iPad/iPad2		Sí	Sí	Sí
Cisco Cius (Android)	Sí	Sí	Sí	Sí
Samsung™ Galaxy™ (Android)		Sí	Sí	Sí
Microsoft Windows® XP PC	Sí	Sí	Sí	
Portátiles con Microsoft Windows 7	Sí	Sí	Sí	

Normalmente, la compatibilidad de los dispositivos depende del nivel de compatibilidad de Cisco AnyConnect y del gestor de dispositivos móviles (MDM) que se utilice. Pueden utilizarse mayoría de dispositivos que pueden conectarse de forma segura a Wi-Fi.

Principales ventajas de la solución BYOD de Cisco

La solución BYOD de Cisco integra productos de Cisco, productos de terceros y dispositivos descritos anteriormente en un enfoque completo de BYOD que se integra en toda la infraestructura de la red. Ofrece un conjunto único de ventajas con respecto a otras soluciones.

1 La compatibilidad con dispositivos Android depende de la versión del sistema operativo y de la compatibilidad con el mismo.

Acceso seguro para cualquier dispositivo

Gracias a la combinación de certificados digitales X.509, la autenticación en dos pasos, el cliente Cisco AnyConnect y 802.1x, es posible usar una amplia variedad de dispositivos que pueden acceder a la red de forma segura.

Autoservicio en la incorporación

El enfoque integrado permite que los dispositivos puedan incorporarse sin intervención adicional la primera vez que se conectan a la red. A cada dispositivo se le asigna un código único para poder identificarlo en los siguientes intentos de acceso a la red.

Aplicación centralizada de las políticas de uso de la empresa

Cisco Identity Services Engine (ISE) proporciona una fuente única y centralizada de políticas para la empresa que pueden aplicarse para diferentes tipos de acceso a la red.

Servicios y acceso diferenciados

La solución BYOD de Cisco ofrece un medio de identificación de dispositivos y usuarios, así como servicios diferenciados basados en opciones de política personalizadas. Por ejemplo, los empleados que utilizan dispositivos propiedad de la empresa y gestionados por ella pueden recibir un tratamiento distinto a los empleados que utilizan sus propios dispositivos no gestionados para sus tareas profesionales. Igualmente, los empleados temporales, partners, invitados, clientes, estudiantes y demás clasificaciones importantes para la empresa o entidad se identificarán y tratarán en conformidad con las políticas empresariales, restringiendo su acceso a un conjunto determinado de servicios y permitiéndoles acceder a aquellos servicios para los que han sido autorizados.

LAN inalámbrica de alto rendimiento y fiabilidad

La solución BYOD de Cisco incluye las principales tecnologías de WLAN que hacen posible un rendimiento y una fiabilidad óptimos para los clientes inalámbricos. Las tecnologías que incluyen Cisco CleanAir™, ClientLink y diseño de antena 4x4 básicamente mejoran el rendimiento de RF. El roaming rápido seguro, VideoStream y la calidad de servicio inalámbrico mejoran la experiencia de las aplicaciones. Ninguna otra solución del sector cuenta con una oferta de productos tan amplia como la familia WLAN de Cisco.

Enfoque unificado para el acceso por cable, inalámbrico, remoto y móvil

La estrategia de la solución BYOD de Cisco consiste en proporcionar un enfoque común independientemente del tipo de conexión a la red de los dispositivos, ya sea por cable, Wi-Fi, Wi-Fi pública o móvil 3G/4G o de si la conectividad tiene lugar en el campus principal o en sucursales, oficinas domésticas o ubicaciones de teletrabajo móviles.

Experiencia unificada para los usuarios finales

El enfoque unificado para todas las ubicaciones y tipos de acceso a la red, así como el uso del cliente Cisco AnyConnect, proporciona una experiencia uniforme para los usuarios, tanto si se conectan en la oficina de la empresa mediante Wi-Fi o de forma remota a través de proveedores de redes móviles 3G/4G.

Visibilidad y gestión de dispositivos unificadas

Cisco ISE y Cisco Prime ofrecen una única fuente y visibilidad para usuarios y dispositivos, por lo que facilita las tareas de resolución de problemas y auditoría.

Comunicaciones Unificadas

Cisco UC y Cisco Jabber amplían la colaboración a los dispositivos BYOD, integrando a los usuarios con sistemas de comunicaciones corporativas como voz, vídeo y teleconferencia, lo que aumenta aún más su productividad.

Arquitectura de soluciones validada

Por último, Cisco se encarga de garantizar que los componentes de la arquitectura de la solución BYOD se integran unos con otros perfectamente y ofrece directrices y mejores prácticas de diseño validado para reducir los riesgos de la implementación. Además, la solución BYOD puede validarse con las arquitecturas de otras soluciones de Cisco.

Introducción a BYOD

Implementación de una solución completa BYOD de Cisco

Como ya se ha tratado anteriormente, la solución BYOD de Cisco es una solución completa que responde a los principales requisitos y desafíos tanto de las organizaciones de TI como de los usuarios. Se han tratado los principales aspectos que han de tenerse en cuenta a la hora de planificar cualquier implementación.

Cisco ofrece diseños validados y mejores prácticas para minimizar los riesgos de la implementación. Para obtener más información, consulte la zona dedicada al diseño de Cisco en: http://www.cisco.com/go/designzone.

Servicios de evaluación e implementación

Las implementaciones de BYOD de gran tamaño y complejas pueden suponer un desafío. A modo de ayuda, Cisco ofrece un completo conjunto de servicios de evaluación, diseño e implementación para garantizar que las implantaciones están bien planificadas y se llevan a cabo sin problemas.

Para obtener más información

- Zona dedicada al diseño de Cisco: http://www.cisco.com/go/designzone
- Dispositivos de seguridad Cisco Adaptive Security Appliances (ASA): http://www.cisco.com/go/asa
- Cisco AnyConnect: http://www.cisco.com/en/US/netsol/ns1049/index.html
- Cisco Identity Services Engine (ISE): http://www.cisco.com/go/ise
- Cisco Jabber: http://www.cisco.com/go/jabber
- Cisco WebEx: http://www.cisco.com/go/webex
- Cisco ScanSafe: http://www.cisco.com/go/scansafe
- Cisco Unified/Converged Acces: http://www.cisco.com/en/US/partner/prod/collateral/switches/ps5718/ps12686/white_paper_c11-726107.htm
- Cisco TrustSec: http://www.cisco.com/go/trustsec
- Cisco Unified Access: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns815/landing_unified_access.html
- Productos Cisco Wireless: http://www.cisco.com/go/wireless