Acceso móvil, lo que usted necesita saber

Parte 1

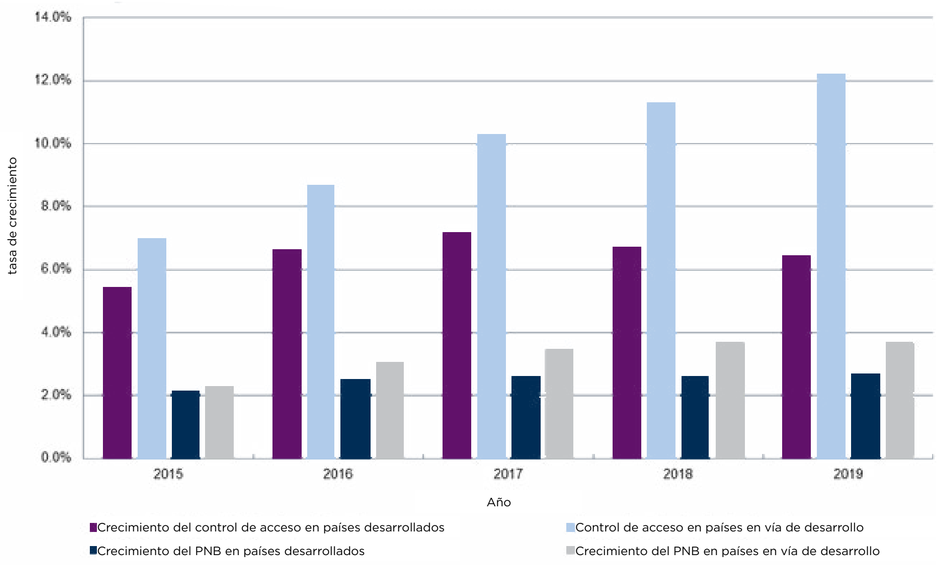
1 ¿Por qué considerar el acceso móvil?

A pesar de la muy justificada atención que se presta a los delitos informáticos y a las filtraciones electrónicas de información, el control de acceso físico —restringir quién puede ingresar al espacio de las oficinas y a los centros de datos, entre otros lugares— sigue siendo una primera línea de defensa fundamental para organizaciones de todos los sectores y tamaños. Las tarjetas inteligentes, los dispositivos de seguridad y muchas otras tecnologías de acceso son comunes en muchos entornos de oficina, y lo han sido desde hace algún tiempo.

Los dispositivos móviles también son omnipresentes en el entorno actual de oficinas. Por lo general, estos dispositivos pueden llevarse en el bolsillo y sirven varios propósitos para sus usuarios: les permiten comunicarse de varias formas, les proporcionan acceso a datos y aplicaciones que antes requerían dispositivos más engorrosos, los ayudan en la navegación, les permiten controlar otros dispositivos como televisores e incluso les permiten abordar aviones.

En vista de estos avances, usar un dispositivo inteligente para controlar el acceso físico (una práctica que en la industria se denomina “control de acceso móvil”) es un paso lógico tanto para los empleados como para las empresas. El presente libro digital se centrará en los beneficios del control de acceso móvil en un nuevo mundo que da prioridad a la experiencia móvil de los usuarios, ayudará a los lectores a comprender las tecnologías disponibles en el mercado y analizará qué deben tener en cuenta las organizaciones al implementar una solución de control de acceso móvil.

El aumento de las identificaciones móviles en relación con el control de acceso global y el crecimiento del PNB



IHS Technology, Identifying growth in the access control industry, junio 2 de 2015

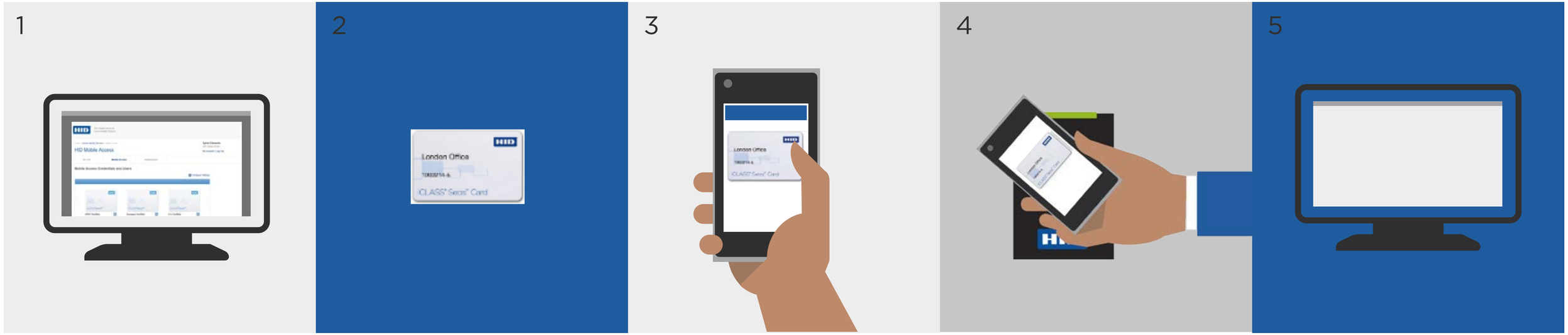
2 Los dispositivos inteligentes están en todas partes

Con el lanzamiento del iPhone en 2007, Apple dio inicio al boom de los teléfonos inteligentes —el uso de un dispositivo móvil como una computadora conectada—. Hoy, Samsung y Apple lideran el mercado. En conjunto, estas dos compañías vendieron más de 500 millones de teléfonos inteligentes en 2014[1]. El sistema operativo Android de Google es actualmente el más ampliamente utilizado, seguido de iOS de Apple. Muy rezagado, con menos del 5 por ciento de cuota de mercado, se encuentra el sistema operativo Windows.

Una nueva clase de dispositivos denominados “prendas electrónicas inteligentes” aumentará aún más el número de dispositivos móviles en el mercado. Entre estas nuevas incorporaciones al universo de dispositivos inteligentes se encuentran gafas, relojes y aparatos médicos y para el bienestar físico. IDC prevé que habrá 155.7 prendas o accesorios electrónicos inteligentes en uso para 2019[2]. La comodidad de uso de este tipo de dispositivos, de naturaleza verdaderamente móvil, que están siempre conectados, los convierte en candidatos aún más obvios para emplear en las aplicaciones de control de acceso.

1. Gartner, noticia: Gartner Says Demand for Enterprise Mobile Apps Willl Outstrip Available Development Capacity Five to One, junio 16 de 2015 (Informe: The Enterprise App Explosion: Scaling One to 100 Mobile Apps)
2. CompTIA, Building digital organizations, junio de 2015

3 ¿Cuáles son las etapas del acceso móvil?



El administrador de los usuarios finales gestiona los usuarios y las identificaciones móviles a través del portal Secure Identity Services

La identificación móvil es transferida al teléfono de forma inalámbrica

El lector es activado mediante un “toque” a una corta distancia o, a una distancia mayor, mediante la tecnología de reconocimiento de gestos twist and go (girar e ingresar)

El lector envía los datos de la credencial al panel

El cliente accede al sistema de control

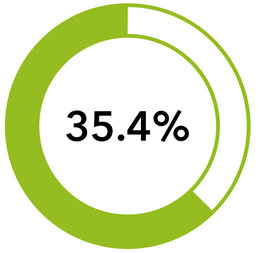
4 Las empresas esperan un mundo que prioriza la experiencia móvil de los usuarios

Movidas por la comodidad y la eficiencia operativa, las empresas están buscando cada vez más aprovechar el potencial de un mundo que da prioridad a la experiencia móvil. El aprovechamiento de la revolución móvil para el control de acceso físico terminará por fusionar las necesidades de acceso a las redes y otras necesidades de acceso seguro, generando un entorno más conectado.

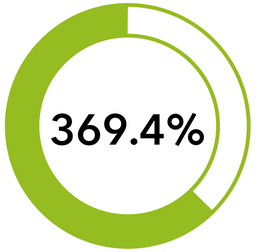
Sin embargo, la movilidad empresarial no está exenta de desafíos. La tendencia que permite a los empleados usar sus propios dispositivos (BYOD, por sus siglas en inglés) se desarrolló rápidamente y tomó por sorpresa a algunas compañías. Pero poco a poco se ha ido haciendo frente a los desafíos que plantea esta tendencia con métodos más prácticos de implementación de los dispositivos móviles en la organización. En lugar de tener una población desconocida de dispositivos que son propiedad de los empleados, los cuales podrían no ser compatibles, las organizaciones están otorgando permiso a ciertos dispositivos personales para acceder a los sistemas corporativos[3]. Varias opciones, incluida la estrategia que permite a los empleados elegir su propio dispositivo (CYOD, por sus siglas en inglés), —en la cual las organizaciones ofrecen una lista de aplicaciones y dispositivos permitidos para roles específicos— están haciendo frente a estos desafíos[4].

La ampliación del control de acceso físico a los dispositivos móviles aumenta la eficiencia de las empresas al automatizar y eliminar una serie de tareas manuales. Solo piense en cómo esta ampliación cambia situaciones que se repiten en los edificios de todo el mundo cada día.

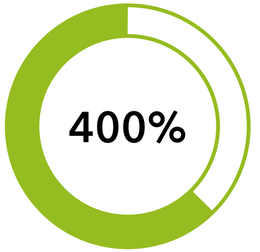
3 CompTIA, Building digital organizations, junio de 2015, www.comptia.org/resources/building-digital-organizations
4 Forrester Research, Demystifying BYOD In Europe, diciembre 18 de 2013, www.forrester.com/Demystifying+BYOD+In+Europe/fulltext/-/E-RES104603



Crecimiento TCAC (tasa de crecimiento anual compuesto) global de los servicios de movilidad empresarial para el período 2015-2019: 35.4%



Crecimiento global del mercado de la movilidad empresarial y de la tendencia BYOD para el período 2013-2019: de 72 mil millones de dólares a 266 mil millones de dólares



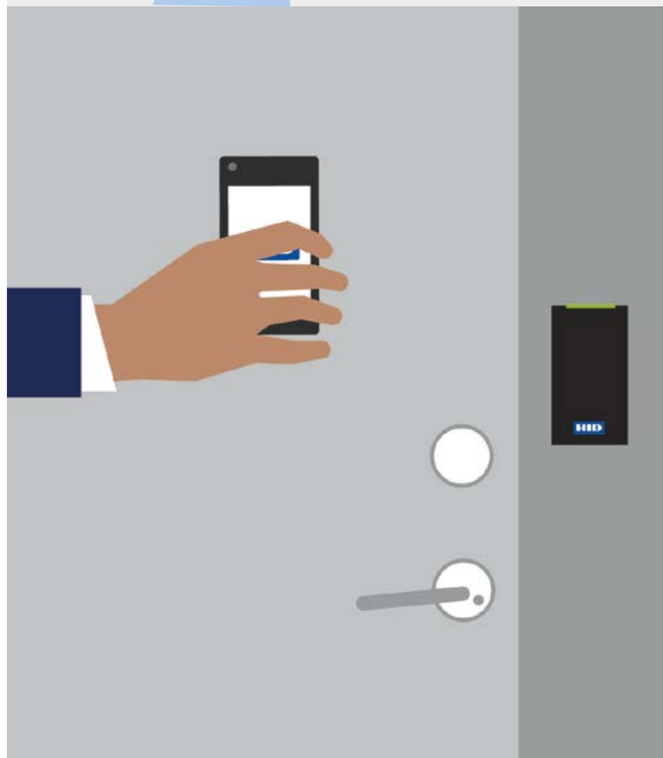
En el período 2014-2016 se cuadruplicaron las aplicaciones empresariales móviles

5 Los beneficios del acceso móvil

Una experiencia mejor y más cómoda para los usuarios finales

La libertad de trasladar el control de acceso a teléfonos, tabletas, pulseras, relojes y otras prendas electrónicas brinda opciones y comodidad a los usuarios finales, junto con nuevas y más prácticas maneras de abrir puertas y portones.

- El dispositivo móvil inteligente siempre está a la mano. Los usuarios no tienen que mantener ni llevar consigo varias tarjetas.
- El acceso mediante un dispositivo móvil puede brindar una experiencia más rápida y sin complicaciones. Por ejemplo, en los estacionamientos, o en los portones de acceso, el mayor alcance del estándar de comunicaciones Bluetooth Smart permite conducir hasta el portón sin tener que bajar la ventanilla del automóvil ni extender la mano para activar un lector.
- Los sensores de los dispositivos inteligentes, especialmente el giroscopio y el acelerómetro, permiten el reconocimiento de gestos. Esto representa un beneficio adicional para el control de acceso: la posibilidad de abrir puertas a distancia mediante gestos intuitivos. Por ejemplo, la tecnología patentada de reconocimiento de gestos twist and go (girar e ingresar) de HID Global permite a los usuarios abrir puertas o portones rotando sus teléfonos inteligentes de una manera similar a como se gira una llave. Esto también proporciona un nivel adicional de autenticación para mayor seguridad.



El acceso móvil puede gestionarse con mayor eficiencia

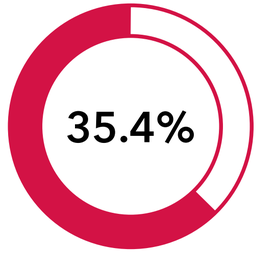
Los dispositivos móviles conectados introducen nuevas formas de gestionar las identificaciones móviles en tiempo casi real.

- **Ahorro de tiempo:** El uso de un portal en la nube para gestionar de forma centralizada las identificaciones móviles, en lugar de gestionar las credenciales físicas, libera tiempo al personal. Incluso es posible inscribir a muchos usuarios a la vez importando un archivo CSV o Excel (carga por lotes). Las invitaciones y el aprovisionamiento a los usuarios finales también se pueden gestionar por correo electrónico.

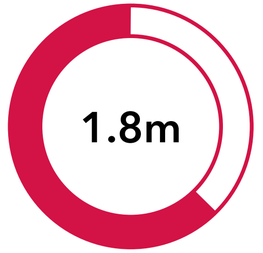
- **Proceso de inscripción fácil para los usuarios finales:** un usuario final recibe la invitación por correo electrónico, descarga la aplicación y se inscribe. La identificación móvil se aprovisiona directamente al dispositivo inteligente del usuario final.

- **Gestión de varias sedes:** Muchas organizaciones tienen oficinas en todo el mundo con diferentes sistemas de control de acceso. Los empleados que están de visita en una de estas oficinas deben, por lo general, obtener una tarjeta de visitante. Con una solución de acceso móvil que brinde soporte a varias identificaciones en cada dispositivo móvil, solo es necesario que un empleado reciba, antes de salir o a su llegada, una identificación móvil adicional en su teléfono.

Dada la importancia cada vez mayor que tienen las soluciones de control de acceso en la nube, los portales de control de acceso móvil también proporcionarán grandes beneficios al modelo de negocio del control de acceso como servicio (ACaaS, por sus siglas en inglés). El modelo ACaaS proporciona funciones básicas del sistema de control de acceso a los usuarios finales por una cuota de suscripción mensual. Por lo general, el software reside en un servidor en el centro de datos del proveedor de servicios y se puede acceder a él a través de un navegador web.



Crecimiento esperado del mercado global de ACaaS: 2018; 530 millones de dólares, 2025; 1.800 millones de dólares



ACaaS controlará 1.8 millones de puertas en el continente americano para 2018

El control de acceso móvil puede ser más seguro

El acceso móvil es un complemento a las soluciones existentes de control de acceso, ya que permite el uso de un dispositivo inteligente como una alternativa a los formatos más tradicionales. Los teléfonos inteligentes u otros dispositivos inteligentes presentan una serie de beneficios de seguridad con respecto a las tarjetas inteligentes o a los dispositivos de seguridad:

- Los números PIN utilizados por los sistemas con teclado se pueden compartir fácilmente. Los sistemas preexistentes, que emplean tecnologías anteriores, como las tarjetas de banda magnética y las tarjetas de proximidad con baja frecuencia, son vulnerables a la clonación (registro y repetición).
- En soluciones de acceso móvil de alta calidad, las credenciales digitales o las identificaciones móviles se almacenan y protegen de forma segura, utilizando las funciones de seguridad del sistema operativo móvil (por ejemplo, aislamiento de procesos o pines) y una encriptación robusta.
- La comunicación entre el dispositivo y el lector transmite datos de forma inalámbrica mediante protocolos de comunicación seguros y servicios de procesamiento de datos confiables, independientemente de las tecnologías de comunicación como NFC (comunicación de campo cercano) o bluetooth.
- Gracias a que los dispositivos inteligentes pueden comunicarse con los lectores a distancias más largas, los lectores pueden montarse en el lado seguro de una puerta, minimizando el riesgo de robo, ataques físicos u observación.
- Las tarjetas y las credenciales se extravían con mucha mayor facilidad que los teléfonos inteligentes. Los teléfonos móviles rara vez se comparten o son hurtados en un ambiente de trabajo, algo que ocurre más fácilmente con las tarjetas.
- En el caso de que un dispositivo móvil se pierda, sea hurtado o violentado, es posible revocar fácilmente todos los derechos de acceso de las identificaciones móviles, de forma remota a través del portal de gestión.
- Los dispositivos inteligentes también son compatibles con la autenticación de varios factores, la identificación biométrica y otras funciones de seguridad avanzadas que van mucho más allá de las prestaciones que ofrecen las tarjetas con tecnologías anteriores.

El acceso móvil permite un entorno más conectado

Las organizaciones actuales están empezando a ver los beneficios de fusionar el acceso físico y el acceso lógico. La gestión simplificada, la reducción de gastos de mantenimiento de varios sistemas, una mayor seguridad y una mejor experiencia para los usuarios son todos factores que están impulsando esta tendencia.

Los dispositivos inteligentes pueden ofrecer opciones de seguridad adicionales para acceder a redes de datos al permitir la autenticación de varios factores. Pueden generar otras prestaciones de seguridad, como las contraseñas de uso único que se requieren para acceder a la red o a las aplicaciones web.

Los empleados tienen la comodidad de poder utilizar el mismo dispositivo para acceder a un edificio, autenticarse en una red virtual privada (VPN) y acceder a redes inalámbricas, así como para iniciar sesión en la intranet corporativa, el servidor de correo electrónico, las aplicaciones en la nube, los clientes de autenticación única y otros recursos informáticos.

Una plataforma de identificación móvil compartida tanto para el acceso físico como para el acceso lógico reporta varios beneficios. Facilita a los encargados de la seguridad la gestión de los derechos de acceso, reduce los errores ocasionados por una sincronización incorrecta entre dos sistemas de gestión independientes y ofrece mayor comodidad a los empleados para que se autentiquen en diferentes servicios.

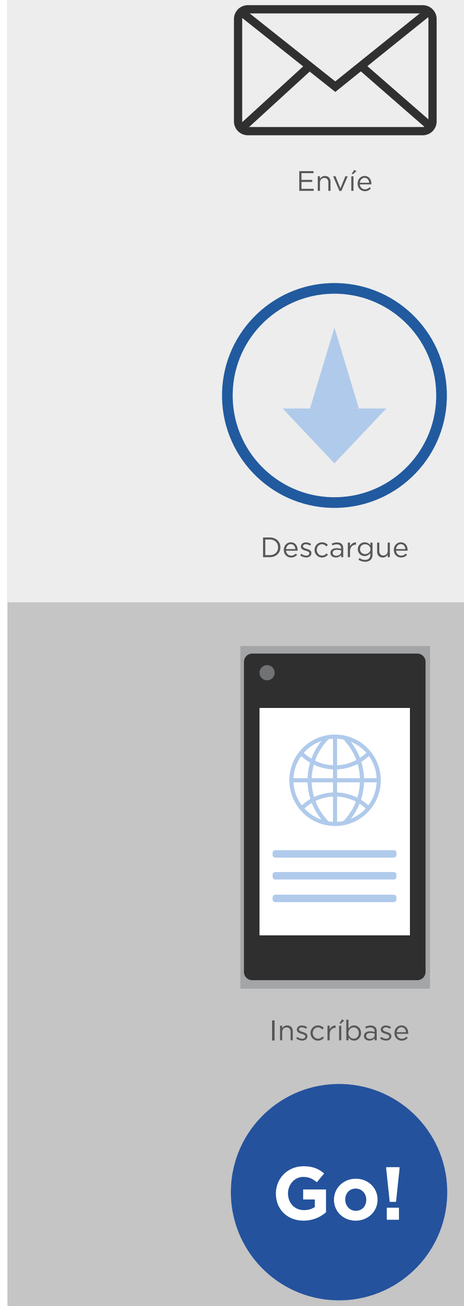
6 Conclusión

Los dispositivos móviles están cambiando la forma en que los trabajadores realizan su labor, así como la manera en que las empresas conciben sus operaciones, redes y seguridad. El siguiente paso lógico para muchas organizaciones es reemplazar los sistemas preexistentes, basados en tecnologías anteriores, por soluciones flexibles de control de acceso físico, que se adapten a los desarrollos futuros y que brinden soporte al acceso móvil.

- Poner a funcionar los dispositivos móviles como herramientas para el acceso seguro es más cómodo para los usuarios.
- Es más fácil de gestionar para las empresas; más seguro que las tecnologías de generaciones anteriores.
- Genera oportunidades para la convergencia de la seguridad de las redes y la seguridad física que no es posible obtener con herramientas de acceso que funcionan con tecnologías anteriores.

Si desea conocer más sobre el acceso móvil y sobre HID Global, por favor visítenos en: hidglobal.com/solutions/mobile-access.

Lisez la suite dans la deuxième partie 2:
Ce qu'il faut savoir pour déployer l'accès mobile avec succès



Norteamérica: +1 512 776 9000 • Línea gratuita: 1 800 237 7769
Europa, Medio Oriente, África: +44 1440 714 850
Asia Pacífico: +852 3160 9800 • América Latina: +52 55 5081 1650

2017-05-31-hid-global-mobile-access-eb-enterprise-part-1-es PLT-03351

An ASSA ABLOY Group brand