WHITE PAPER

Crear confianza en identidades de usuario con Tecnologías de autenticación sólida

Cómo alcanzar el nivel de comprobación de identidad que necesita conveniente y accesible

Resumen ejecutivo

Es un desafío constante tener que satisfacer las distintas necesidades de acceso de todos los usuarios y, al mismo tiempo, resguardar los recursos para protegerlos de amenazas.

Para asegurarse de que los usuarios son quienes dicen ser y gestionar eficazmente su acceso a los recursos, usted necesita una solución completa de comprobación de identidad, cuya base es una autenticación sólida.

Sin embargo, la emisión y la constante gestión de identidades de usuario en los distintos tipos de dispositivo (desde tarjetas inteligentes hasta teléfonos móviles) que se deben emitir para todas las aplicaciones y todos los recursos a los que los usuarios quieran acceder pueden presentar sus propios problemas. En consecuencia, usted necesita una sólida solución de autenticación que le facilite la emisión y la gestión de identidades con el fin de proporcionar distintos niveles de seguridad para distintos niveles de acceso en formas que sean convenientes para el usuario. De lo contrario, se perderá la eficacia de toda la solución.

La necesidad de una autenticación sólida en las empresas de hoy

Día a día, los usuarios están más distribuidos, utilizan más dispositivos móviles y son más dinámicos. En consecuencia, las empresas deben adoptar nuevos mecanismos de confianza en la identidad del usuario y controlar su acceso de forma acorde. En el pasado, se le daba más importancia a las defensas perimetrales mediante controles para determinar quién podía ingresar al edificio (con sistemas de acceso físico) y quién podía entrar a la red (con firewalls y VPN). Sin embargo, una vez adentro, los usuarios podían tener acceso, casi sin obstáculos, a todos los sistemas, aplicaciones y a todos los recursos de estas instalaciones y sus redes.

En la actualidad, tras reconocer que las amenazas provienen de usuarios “de este lado del muro” (el 81 % de las organizaciones han sufrido filtraciones de datos por parte de usuarios o empleados internos que actúan con negligencia o malicia) y ver caer los muros debido a la naturaleza dinámica y global de la actividad comercial moderna, muchas empresas están revaluando sus métodos para el acceso.

Si su empresa es como la mayoría, está luchando por satisfacer las distintas necesidades de todos los usuarios y, al mismo tiempo, minimizar los riesgos que su acceso puede representar para la organización, lo cual es complicado debido al ecosistema de amenazas y a la población de usuarios que cambia día a día. Los ataques continúan evolucionando y son cada vez más sofisticados, como demuestra el incremento de amenazas persistentes avanzadas (APT) que emplean malware personalizado para realizar ataques específicos y a largo plazo a una organización. Al mismo tiempo, los usuarios, que necesitan tener acceso a información y recursos, ya no son solo empleados: abarcan una amplia variedad de asesores, contratistas, proveedores, socios, distribuidores y clientes.

Todos estos usuarios quieren tener acceso a lo que necesitan desde cualquier lugar y con cualquier dispositivo, desde sus teléfonos personales hasta computadoras portátiles y tabletas (BYOD). Si no se tiene cuidado, estas variables pueden aumentar los riesgos en su entorno. Lo que hace falta es una manera de confiar en la identidad de todos estos usuarios diferentes y, a continuación, controlar correctamente su acceso mientras navegan por la organización.
Una de las formas más eficaces de proporcionar la productividad que su empresa necesita y reducir los riesgos en su organización es emplear autenticaciones sólidas en cada aplicación. Si protege cada aplicación empresarial o en la nube asi como sus respectivas bases de datos, podrá gestionar el acceso y asegurar los recursos de información con eficacia, tanto si se encuentran en una computadora portátil o un teléfono móvil.

Definir una autenticación sólida para enfrentar los desafíos de las soluciones tradicionales

La autenticación sólida, también llamada autenticación avanzada (AA) o autenticación de doble factor, va más allá del uso de una sola contraseña para autenticarse. Requiere factores adicionales para establecer si el usuario es quien dice ser. Puede ser algo que el usuario conoce, como una contraseña única o un número de identificación personal (PIN); algo que tiene, como una tarjeta inteligente, un token o un teléfono móvil; o, incluso, algo que recolecta el sistema de autenticación, como inteligencia sobre el comportamiento o fraudes, que se usa para que la autenticación tenga un nivel de seguridad superior.

¿Por qué es importante? Los piratas informáticos siguen yendo contra las identidades de usuarios porque les brindan acceso a las instalaciones y a las redes. De esta forma, pueden “pasar desapercibidos” y moverse por la organización sin ser detectados. Según estudios recientes, casi la mitad de las filtraciones de datos se aprovechan de identidades robadas o débiles. Si consideramos esta estadística, es fácil ver que si fortalecemos los mecanismos que usan los usuarios para autenticarse, mejorará la seguridad global de la empresa.

La realidad es que el uso de contraseñas estáticas tradicionales, aunque sean convenientes, simplemente no son suficientes para protegerse de las amenazas dinámicas actuales. Las herramientas que registran las pulsaciones de teclas, los ataques de suplantación de identidad, los monitoreos informáticos y hasta "adivinar" serán suficientes para descifrarlas. Las contraseñas de un solo uso (OTP) y los tokens ofrecen mayor seguridad porque las contraseñas que generan solo sirven para una sesión o transacción; sin embargo, pueden crear otros problemas si no se implementan correctamente. Muchas soluciones anteriores no ofrecen control sobre la “llave” del token (el registro de semilla del token). En su lugar, los registros de la semilla de los tokens se almacenan en las bases de datos del proveedor. Esto significa que si el proveedor es víctima de un ataque, la seguridad de la empresa podría verse amenazada.

Además, las soluciones anteriormente descritas, que consideran que todo estará bien después del ingreso, simplemente no son lo suficientemente completas o versátiles para considerar el rol del usuario, su ubicación y el tipo de dispositivo usado para acceder, que son necesarios para establecer la confianza y otorgar acceso en una amplia gama de aplicaciones empresariales o en la nube. No es suficiente el usar una autenticación sólida solo cuando se ingresa por primera vez al edificio o a la red. Como se mencionó antes, los perímetros de defensa ya no sirven. Es necesario que la autenticación sólida se extienda a toda la organización para que incluya al acceso a computadoras de escritorio, servidores, teléfonos móviles, datos, aplicaciones empresariales y en la nube de una manera que le permita aumentar realmente la seguridad total de su empresa.

Sin embargo, la emisión y la gestión constantes de identidades de usuario en todos los distintos tipos de dispositivos (desde tarjetas inteligentes hasta teléfonos móviles) para todas las

aplicaciones y todos los recursos a los que se quiera acceder puede ser un proceso manual y lento. Es aún más complicado cuando se trabaja con varios tipos de identificación, para accesos físicos y en línea, y distintos sistemas de identificación y autenticación. Se necesita un proceso único con un sistema consolidado de gestión de identidades de usuario capaz de emitir y gestionar identidades de seguridad para que todos los usuarios puedan tener un acceso adecuado a todo lo que necesiten, desde edificios hasta aplicaciones en la nube, en varios formatos, desde tarjetas inteligentes hasta teléfonos móviles.

Descripción general de la versatilidad del dispositivo ActivID:

- **Dispositivos compatibles:** teléfonos inteligentes, tabletas, computadoras portátiles, etc.
- **Métodos de autenticación**: tokens OTP de hardware y de software, tarjetas inteligentes, ID de dispositivos, autenticación adaptable, mecanismos de detección de fraude o mecanismos OTP fuera de banda (SMS o correo electrónico) para autenticaciones a nivel de transacción.
- **Aplicaciones:** empresariales, de nube, etc. (como Windows, Salesforce.com, SAP, Oracle, Google Apps, etc.).

Requisitos para una autenticación sólida y eficaz, sin riesgos

Una solución eficaz de autenticación sólida debe ser capaz de agregar seguridad sin incrementar los costos ni la complejidad. En los entornos empresariales actuales, solo una solución de autenticación sólida que sea fácil de gestionar será capaz de funcionar con la amplia variedad de usuarios que su organización debe atender si desea estar protegida contra la abundante cantidad de ataques actuales y futuros. Usted necesita una solución que proporcione lo siguiente:

Autenticación sólida:

- **Autenticación de doble factor o más:** aumente la confianza en las identidades de sus usuarios para que pueda otorgarles el acceso adecuado.
- **Distintos niveles de acceso:** según los riesgos asociados a distintos tipos de usuarios y transacciones. Debe ser capaz de proporcionar soluciones de seguridad transparentes y en capas para aumentar la seguridad de forma significativa sin afectar la experiencia del usuario (por lo menos de usuarios que se conecten desde dispositivos y ubicaciones confiables).
- **Detección avanzada de fraudes:** tenga en cuenta factores como la ubicación geográfica y la información del dispositivo cuando realice la autenticación de usuarios para limitar el acceso a dispositivos confiables en países y localidades confiables.

Otra alternativa es solicitarle al usuario que utilice métodos de autenticación suplementarios o más seguros, como contraseñas de un solo uso enviadas por SMS, cuando se conecten desde dispositivos o ubicaciones que no estén en la lista de lugares o dispositivos seguros.

- **Análisis constante de comportamiento :** para autenticaciones continua y capacidades forenses mejoradas mediante el uso de análisis de comportamiento de las interacciones del

usuario con las aplicaciones. La actividad de los usuarios se monitorea y analiza constantemente para conocer el comportamiento de un usuario específico de modo que las desviaciones de comportamiento se puedan detectar y alertar sin afectar la facilidad de uso del usuario ni poner en riesgo la privacidad.

Si ocurre una desviación (p. ej., otra persona usa la computadora), la aplicación puede volver a solicitar la autenticación del usuario o agregar el evento a una base de datos de auditoría para estudios forenses posteriores. Este método se puede usar para disminuir la cantidad de veces que el usuario necesite autenticarse en el sistema y mejorar la experiencia del usuario.

Gestión simplificada:

- **Rápida de implementar y gestionar**: la puesta en marcha de la solución debe ser simple y no debe agregar complejidad ni costos innecesarios. De ser posible, debe permitirle tener un panorama consolidado para simplificar la emisión de identidades y la gestión constante de sus soluciones de comprobación de identidad con el objetivo de garantizar que sean compatibles con su política sobre la seguridad (por ejemplo, la identificación y suspensión de identidades debe ser sencilla, de modo que no existan identidades y perfiles para empleados que ya no trabajan en la empresa).
- **Integral:** un único sistema de gestión de identidades capaz de gestionar las identidades de sus usuarios en varios dispositivos, como tarjetas inteligentes y teléfonos móviles, y el ciclo de vida actual de dichos dispositivos e identidades. De ser posible, debe habilitar el acceso a sus recursos físicos (edificios) y en línea (aplicaciones y recursos empresariales y basados en la nube), y proporcionar una única vista simplificada de todos sus sistemas de comprobación de identidad.
- **Simple de integrar:** la solución debe ser capaz de integrarse con las actuales herramientas de gestión que utiliza normalmente para crear una interfaz consolidada y uniforme de identidades de seguridad del usuario y gestión de la autenticación.

Comodidad del usuario:

- **Fácil de usar:** no debe interrumpir los flujos de trabajo. De ser posible, debe aprovechar las tarjetas de identificación, las tarjetas inteligentes y los teléfonos móviles que ya utilicen los usuarios para ampliar el acceso seguro a los recursos físicos y digitales que requieran.
- **Dinámica:** no debe causar demoras innecesarias en las aplicaciones empresariales y en la nube que los usuarios necesitan para realizar sus tareas.

El método de una solución de autenticación sólida capaz de proporcionar el acceso seguro que necesitan los usuarios

La familia de productos de ActivID™ se puede usar para emitir y gestionar identificaciones y perfiles de una amplia variedad de usuarios que necesiten acceder a la red. También les permite usar cualquier dispositivo para autenticarse, y obtener los recursos necesarios de forma conveniente y segura. Esta solución poderosa consta de las credenciales unificadas ActivID, el dispositivo ActivID con servidor de autenticación y el sistema de gestión de identidades (CMS) ActivID:

Identidades unificadas

La cartera de productos de ActivID ofrece identidades unificadas, que son únicas en la industria, y que se pueden usar en sistemas lógicos y físicos. De esta forma, los usuarios pueden autenticarse

para entrar a un edificio, conectarse a la red, y obtener un acceso seguro a las aplicaciones y a otros sistemas que necesiten. También pueden usar las identidades unificadas para obtener acceso remoto a redes seguras; en consecuencia, no se necesitan tokens de contraseñas de uso único (OTP) o tokens de hardware.

Las identidades unificadas son más convenientes para los usuarios ya que eliminan la necesidad de contar con varios dispositivos o solicitar continuamente contraseñas de uso único. También ofrecen seguridad mejorada porque habilitan la autenticación sólida en toda la infraestructura informática de sistemas clave, recursos empresariales y aplicaciones basadas en la nube, y no solamente en el perímetro.

Descripción general del dispositivo CMS ActivID:

Usted puede gestionar:

- **Sus dispositivos de autenticación**: desde tarjetas inteligentes y tokens USB hasta teléfonos móviles
- **Sus datos**: contraseñas estáticas, elementos biométricos y datos demográficos;
- **Sus applets**: aplicaciones de contraseñas de uso único y applets de verificación de identidad personal (PIV)
- **Sus identidades digitales**: como certificados de infraestructura de clave pública (PKI) durante todo su ciclo de vida.

Dispositivo ActivID con servidor de autenticación

El dispositivo ActivID con servidor de autenticación ofrece la versatilidad requerida para autenticar y asegurar el acceso de los usuarios a aplicaciones necesarias para realizar su trabajo, de forma conveniente y rentable. Soportando una amplia variedad de dispositivos y más de 15 métodos de autenticación, usted tendrá todo lo necesario para confiar en la identidad del usuario, y otorgarle acceso a todas las aplicaciones empresariales y en la nube.

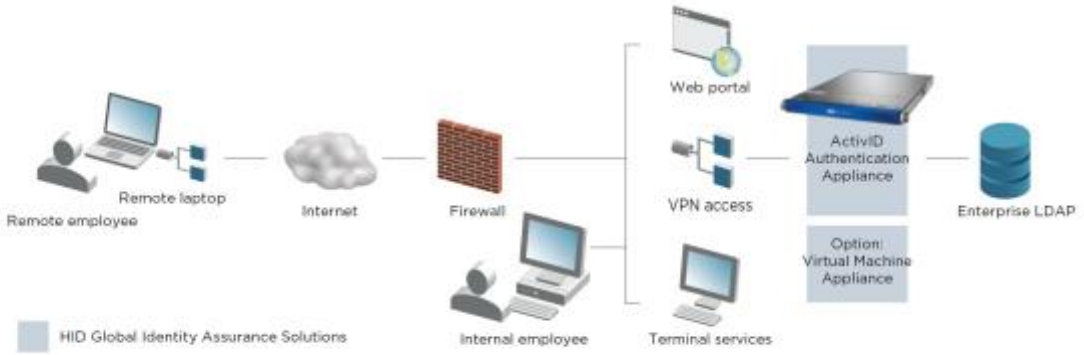
El dispositivo ActivID ofrece la seguridad que necesita sin complejidad. Las plantillas sencillas y las políticas de seguridad fáciles de definir le permiten implementar rápidamente la solución de autenticación que más se adapte a sus necesidades. El servicio de detección de fraude en el dispositivo ActivID, único en la industria, le permite personalizar la solución para satisfacer las necesidades específicas de su entorno. Se puede usar para identificar información del acceso (como las computadoras que usan los usuarios para conectarse, el navegador que emplean y si ya usaron estos elementos anteriormente) con el objetivo de determinar si es necesaria una autenticación simple o una de doble factor en un momento determinado, según el conjunto de reglas que se haya definido previamente. Esto le permite fácilmente añadir seguridad, siendo esta invisible para los usuarios.

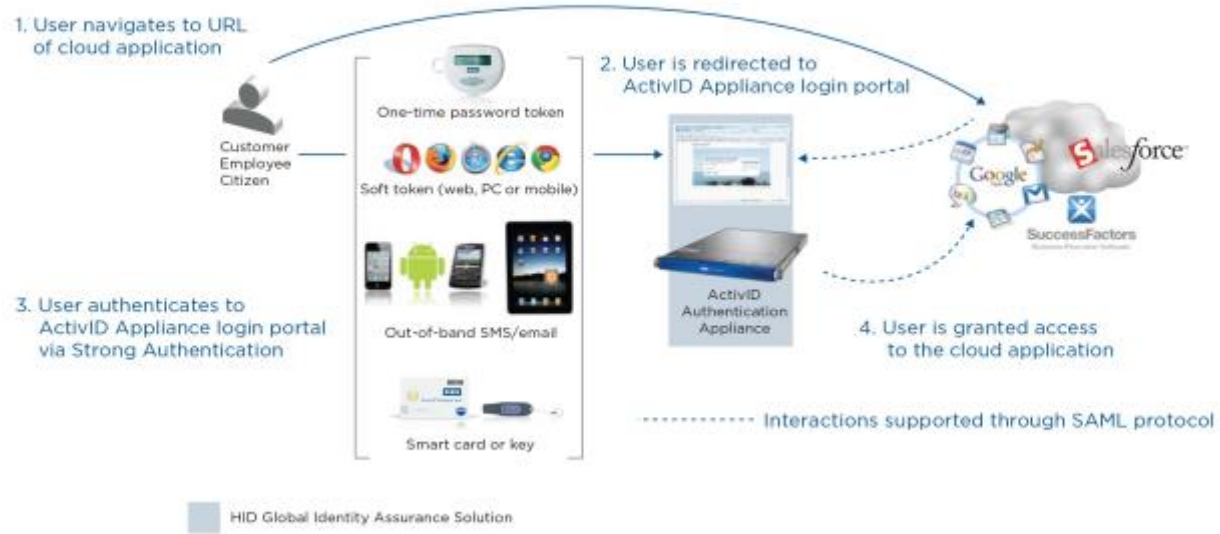
Puede usar el nivel de especificidad que desee: puede limitar el acceso a ciertos dispositivos de un área específica o puede tener en cuenta el rol del usuario (si es el presidente ejecutivo o el gerente de marketing, por ejemplo), y determinar la identificación y permisos que se otorgarán y la forma que se gestionará su acceso. También puede aprovechar la inteligencia recopilada por miles de otros clientes para identificar si el cambio de panorama (p. ej., si las computadoras de un área determinada están teniendo problemas) debe hacer que usted cambie sus requisitos de autenticación (limitar el acceso o solicitar autenticación adicional).

Como resultado, ActivID lo ayuda a mantenerse al frente de los requisitos de seguridad que cambian día a día: podrá proporcionar seguridad de forma tal que se integre al flujo de trabajo de sus usuarios para garantizar una protección dinámica adicional en sus recursos críticos. No olvide que los tokens de ActivID duran hasta ocho años. Puede gestionar sus propios registros de semilla para controlar completamente la protección de las claves criptográficas y estar más tranquilo.

Los servicios profesionales de HID Global también están disponibles para ayudarlo a redefinir la implementación y configuración del servicio de detección de amenazas ActivID si desea utilizarlo. Pueden ayudarlo a crear las mejores políticas para su entorno que tome en cuenta cualquiera de los más de 20 parámetros disponibles, como el rol de las personas, la hora de inicio de sesión o el tipo de dispositivo utilizado, etc. para que la puesta en marcha sea fácil y rápida.

Dispositivo ActivID de autenticación: cómo funciona

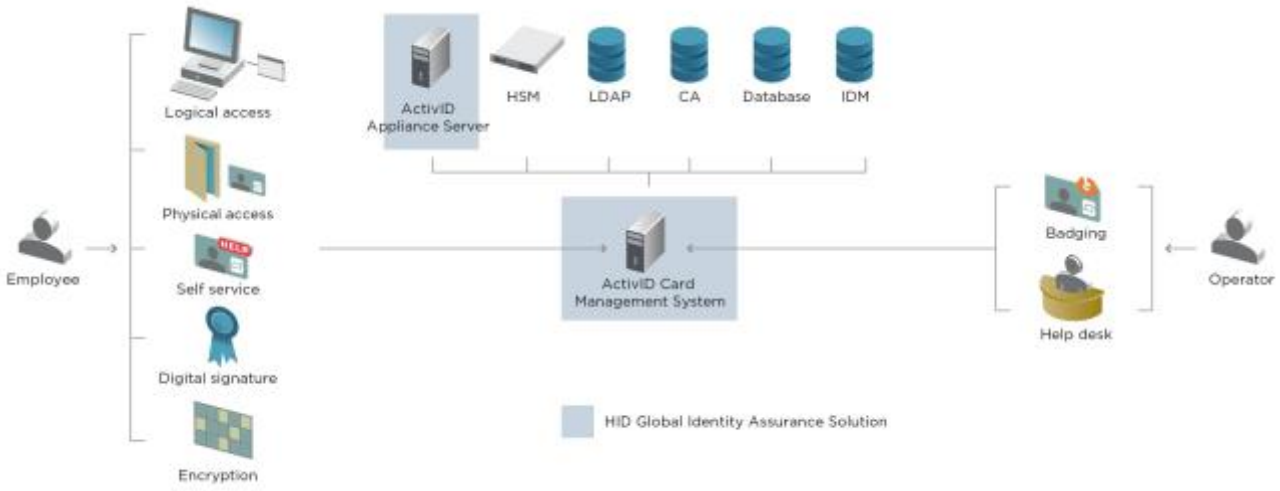




Sistema de gestión de identidades (CMS) de ActivID

El CMS de ActivID proporciona una solución completa y flexible que le permite gestionar fácilmente la emisión y requisitos de administración para una correcta implementación de autenticación. Puede emitir y gestionar tarjetas inteligentes, tokens USB inteligentes y tokens digitales de teléfonos móviles que se pueden usar en varias aplicaciones de escritorio, de seguridad de red y de productividad. Esto le permite configurar políticas y flujos de trabajo personalizados que se adapten fácilmente a todos los entornos y escenarios de implementación. Ofrece funcionalidades completas de auditoría a prueba de alteraciones que registran todas las actividades de eventos para realizar reportes con capacidades de actualización únicas, patentadas y postemisión. De esta forma, su solución de autenticación siempre estará vigente. El autoservicio basado en la web y la administración del centro de ayuda disminuyen los costos operativos asociados a la gestión y al mantenimiento constantes de la solución.

Sistema de gestión de identificaciones (CMS) de ActivID: cómo funciona



Aprovechar los beneficios de una solución eficaz de autenticación sólida

Toda la solución de autenticación sólida que ofrece ActivID lo ayuda a aumentar la seguridad y, al mismo tiempo, a satisfacer las necesidades de usuarios distribuidos, dinámicos y que utilizan dispositivos móviles. La flexibilidad de la solución le permite equilibrar los costos y requisitos de seguridad para poder brindar la seguridad que buscan los usuarios y disminuir los riesgos presentes en un ecosistema de amenazas que cambia día a día. La solución de ActivID proporciona lo siguiente:

Autenticación sólida:

- **Menos riesgos:** permita que los usuarios se conecten con seguridad a aplicaciones mediante autenticaciones de dos o más factores para eliminar violaciones de seguridad.

- **Detección de fraudes y análisis de comportamientos:** establezca factores adicionales que el proceso de autenticación debe considerar para aumentar la confianza en la identidad y el acceso de los usuarios, y mejorar la experiencia del usuario.
- **Estrategia de autenticación adaptable:** puede determinar distintos niveles de acceso ya que es posible definir la identificación de autenticación (dispositivo) necesaria y el tipo de acceso que requiere la persona.

Gestión simplificada:

- **Rápida implementación y administración:** los usuarios pueden comenzar a trabajar rápidamente con autenticación de tokens para que sus aplicaciones sean seguras en toda la organización.
    - A medida que crezcan las necesidades de la organización, una simple actualización de la licencia le proporcionará a las organizaciones acceso al conjunto de métodos de autenticación más amplio de la industria, que incluye soluciones de certificados, soluciones basadas en el conocimiento y soluciones basadas en riesgos.
    - Incluye procesos empresariales y políticas de seguridad fáciles de definir para emitir y gestionar identidades y dispositivos digitales entre ilimitados grupos de usuarios finales en ubicaciones geográficamente dispersas.
- **Reducción de costos:** las identidades únicas y unificadas eliminan la necesidad de invertir en infraestructuras independientes de autenticaciones físicas y en línea. Simplifican los procesos, disminuyen el trabajo administrativo y permiten que la gestión general de su solución de comprobación de identidad sea fluida.
    - Amplíe las capacidades de las tarjetas/gafetes de los empleados y/o de sus teléfonos móviles, y con esto, se elimina la necesidad de contraseñas y de todos los procesos asociados al restablecimiento de contraseñas, entre otros.
    - Una plataforma de autenticación versátil y multicapa que le permite minimizar el tiempo y los costos asociados a la implementación y el mantenimiento de identidades digitales en forma de tarjetas inteligentes, tokens USB inteligentes y teléfonos móviles.
    - Le permite dirigir los gastos de seguridad a los usuarios y las aplicaciones que más lo necesiten.
- **Valor extendido:** una plataforma de gestión que se puede configurar y ampliar en gran medida para los gafetes multifunción de los empleados, identificaciones basadas en tarjetas inteligentes y tokens en teléfonos móviles.
    - Acceso seguro desde teléfonos inteligentes, dispositivos iPad, computadoras portátiles y PC sea seguro en VPN, portales web y aplicaciones en la nube.
    - Se integra fácilmente a una amplia variedad de sistemas operativos, directorios, sistemas de gestión y aprovisionamiento de identidades y de acceso a datos, autoridades de certificación y sistemas de control de acceso físico.
    - Emplea autenticación basada en el estándar de OATH, que permite ampliar las opciones de elección de dispositivos de autenticación.

Comodidad del usuario:

- **Facilidad de uso:** Se puede usar un solo gafete de identificación o, incluso, el teléfono móvil del usuario puede usarse para los accesos físicos y digitales (en línea). Sin la necesidad de llevar ningún elemento adicional o recordar ninguna clave, hace más fácil integrar la solución a los flujos de trabajo existentes.

Productividad mejorada:

- Las medidas de seguridad invisibles, como la detección de fraudes y el análisis de comportamientos, permiten que la solución sea fluida para el usuario y puedan disminuir realmente la cantidad de veces que el usuario debe autenticarse.

- Las políticas pueden aumentar las medidas de seguridad según el nivel de riesgo y exposición de la empresa. De esta forma, se garantiza la minimización de pasos adicionales, que solo se requerirán cuando sea necesario (a partir de distintos factores, como la ubicación, el tipo de dispositivo, el rol, la hora, los cambios de comportamiento, etc.).

La diferencia que marca ActivID: tranquilidad para los usuarios y las organizaciones

En los entornos dinámicos actuales, solo una solución de autenticación sólida que sea fácil de usar y gestionar será capaz satisfacer las necesidades de los usuarios y las organizaciones. La solución de ActivID le ofrece la flexibilidad que usted necesita para respaldar y asegurar a la amplia variedad de usuarios de su organización, quienes usan distintos dispositivos para acceder a una amplia gama de recursos y aplicaciones. Ya la utilizan muchas de las organizaciones que más importancia le dan a la seguridad, desde el Departamento de Defensa de EE. UU. (DoD) hasta instituciones financieras y de salud. Ofreciendo las únicas soluciones de acceso realmente unificadas del mercado, HID Global le brinda la solución de comprobación de identidad más completa, desde tarjetas de acceso para lectores de puertas hasta dispositivos y software de autenticación. Mediante su implementación, puede aumentar la confianza de la identidad de sus usuarios y proteger su organización contra los riesgos actuales y futuros de forma eficaz. En consecuencia, puede conectar usuarios desde cualquier ubicación con total seguridad a través de una variedad de dispositivos y métodos de autenticación. Así, podrá ayudarlos a obtener lo que necesiten de forma conveniente cuando deban llevar adelante sus actividades con seguridad.