

# Nueve consejos para realizar la implantación de proyectos de gestión de identidades y de accesos



**\_betasystems**

Libro blanco

## Introducción

Cada vez con más frecuencia las incidencias de seguridad de TI afectan a las empresas, independientemente de su sector, volumen o actividad. Acceso no autorizado, usurpación de identidad, fuga de datos... las empresas ya no se pueden permitir pasar por alto el riesgo de los ciberataques ni suponer que los atacantes nunca podrán penetrar en el sistema de información.

Por este motivo, los analistas más destacados (KuppingerCole, Pierre Audouin Conseil, Gartner...) hacen hincapié en la necesidad de implantar un sistema IAM (gestión de identidades y accesos) para completar el arsenal de medidas de seguridad del sistema de información de la empresa. Los proyectos IAM ahora son una prioridad real para quien desee reforzar su ciberseguridad.

No obstante, resulta evidente que numerosas iniciativas están obstaculizadas por los errores con los que se han encontrado otras empresas. Por lo tanto, es esencial preparar correctamente la implantación del proyecto, tanto en sus aspectos técnicos como empresariales. A continuación le presentamos algunos métodos más recomendables para llevar a cabo correctamente un proyecto IAM.

### 1. Creación de un equipo de proyecto combinado de TI y empresarial

Un proyecto IAM es un proyecto transversal que requiere la participación de numerosas partes interesadas de la empresa, normalmente el departamento de TI, pero también los responsables de recursos humanos y empresariales. Subestimar la necesidad de implicarlos puede ser suficiente para que el proyecto no salga adelante. Además, su proyecto no se puede enfocar únicamente desde un punto de vista técnico. Es necesario obtener el apoyo y la colaboración de los departamentos empresariales para movilizar a las partes pertinentes en torno al proyecto y poder partir de su conocimiento de los procesos de negocio y de la estructura organizativa de la empresa.

### 2. Definición de la administración y de los objetivos del proyecto

Un proyecto IAM con un proceso de administración deficiente tiene muy pocas posibilidades de tener éxito. En primer lugar, se deben determinar los roles y las responsabilidades de cada participante, así como los distintos pasos de la implantación. La consecución de los objetivos conlleva una supervisión rigurosa y una colaboración estrecha entre el equipo del proyecto y los consultores de IAM del proveedor. Compruebe que las especificaciones y los objetivos se entienden y se documentan de común acuerdo antes del inicio de la implantación. Los cambios posteriores aumentarán desproporcionadamente el tiempo y el coste de implantación del proyecto.

### 3. Reducción de la personalización al mínimo

Al elegir una solución, el software IAM estándar y preconfigurado constituye la mejor estrategia, especialmente porque con este planteamiento se aprovechan las implantaciones de IAM que se han realizado en otros clientes. Además, simplifica considerablemente la integración de nuevas funciones a medida que se lanzan versiones de software nuevas. El abandono de la oferta estándar por un sistema más personalizado debe ser un hecho excepcional. Los productos estándar del proveedor reducen los costes de implantación y de mantenimiento, además de acelerar el proceso.

### 4. Implantación por fases

Sea pragmático: la implantación de la solución IAM con un ámbito técnico y funcional amplio puede retrasar el proyecto. Dé prioridad a un planteamiento rápido, con una implantación paso a paso e hitos

asequibles. Si limita voluntariamente el ámbito inicial a un número reducido de sistemas, usuarios y funciones de destino, obtendrá resultados más rápidamente, incluso en pocos meses. Este retorno anticipado de la inversión le ayudará a reforzar la aceptación de la empresa para obtener presupuestos adicionales y, de este modo, ampliar el ámbito del proyecto.

## **5. Conexión de los sistemas de recursos humanos**

Los movimientos de personal (nuevas incorporaciones, abandonos, movilidad,...) se pueden comunicar al departamento de TI o de recursos humanos con algo de retardo o, incluso, no comunicarse. Estas complicaciones pueden aumentar cuando las tareas de administración del personal se llevan a cabo manualmente o de un modo descentralizado. Por lo tanto, inicialmente, la fuente de datos de RR. HH. principal debe estar conectada con el sistema IAM de un modo automático, lo que ofrece ventajas rápidamente cuantificables: acceso simplificado, mayor productividad, satisfacción de los usuarios...

## **6. Limpieza de los datos**

La calidad de los datos es esencial para cualquier proyecto IAM de éxito. Pero, con demasiada frecuencia, no se realiza el mantenimiento de la información de los permisos de acceso y puede convertirse en un desastre. El resultado es que se pierden los vínculos entre las cuentas y los usuarios, algunas cuentas se quedan sin propietario y otras son erróneas. Por este motivo, todo proyecto IAM debe empezar necesariamente por la consolidación de las identidades de usuario. En este paso, las cuentas de usuario se asignan a las personas correspondientes del conjunto de identidades. De forma inmediata, la limpieza de los datos muestra una primera ventaja: la consolidación de los identificadores de usuario muestra las cuentas que no tienen propietario.

## **7. Implantación de roles**

Un rol es un conjunto de permisos de accesos individuales que son necesarios para una determinada función o tarea de la empresa. Está vinculado estrechamente con los procesos empresariales específicos de la empresa. Los «grupos» de permisos de acceso, denominados «roles», reducen considerablemente las tareas de administración. Son esenciales para automatizar los procesos y para implantar reglas que impidan la acumulación de determinados permisos (segregación de obligaciones). Pero la implantación de roles requiere algo más que la simple definición de grupos de permisos de acceso. Los roles son objetos vivos. Se debe hacer una actualización y un mantenimiento de ellos de forma continuada. Es importante designar a un «propietario» para cada rol. Será el responsable de la evolución posterior del rol. Por lo tanto, los roles se deben revisar periódicamente para que se adapten a los cambios de la empresa o de los sistemas de TI.

## **8. Incorporación de la valoración de riesgos**

Los sistemas IAM proporcionan una considerable cantidad de datos que se deben procesar para detectar los elementos más arriesgados. La identificación y la valoración de estos riesgos es una herramienta potente para ordenar los datos de acceso, como los usuarios, los roles y las cuentas, según el nivel de los riesgos potenciales. No obstante, la implantación de una evaluación de riesgos de toda la estructura de permisos de acceso requiere tiempo y recursos. El uso de un planteamiento descendente (de arriba abajo) puede ofrecerle un primer análisis rápido de los riesgos, ordenarlos por categoría y valorarlos. La duración del proyecto ofrece la ventaja de que el ámbito de estas evaluaciones se expandirá gradualmente.

## 9. Incorporación de las características principales que necesita cada departamento

Recuerde que, incluso si los sistemas IAM están impulsados por auditores y responsables de TI, los departamentos empresariales también están interesados. Presentar rápidamente los primeros resultados concretos a la junta le servirá para ganarse el apoyo de toda la empresa. Por este motivo, en las primeras fases del proyecto céntrese en las características empresariales que facilitarán las tareas a los usuarios finales: por ejemplo, un portal web para volver a certificar los permisos de algunos usuarios o un proceso para automatizar la aprobación de las solicitudes de permisos. La satisfacción de los usuarios empresariales es un indicador clave para demostrar el éxito de su proyecto IAM.

Apoyándose en sus 20 años de experiencia en el campo de IAM, Beta Systems ofrece una suite completa para la gestión de acceso a los recursos TI basada en las identidades y roles de los usuarios.

**SAM Enterprise Identity Manager:** Automatización de la gestión de identidades y del acceso a los recursos TI. Centralización, mantenimiento de consistencia y utilización de los datos.

**SAM Business Process Workflow:** Automatización de los procesos de negocio que implican derechos de acceso con un motor potente y una interfaz de usuario sencilla.

**Garancy Data Access Governance:** Control de acceso seguro a los datos almacenados en formato desestructurado.

**Garancy Recertification Center:** Ejecución de campañas de revisión de los derechos de acceso de los usuarios basado en niveles de riesgo.

**Garancy Access Intelligence Manager:** Análisis multidimensional de los derechos de acceso y evaluación de los riesgos asociados: Business Intelligence dedicada a la seguridad de los accesos.

**SAM Password Management:** Acceso seguro y simplificado a las aplicaciones.



## Información sobre Beta Systems

Beta Systems es un proveedor de soluciones de software independiente de tamaño medio de Europa. La empresa, que se fundó en 1983, desarrolla software que protege el procesamiento de datos en centros de TI grandes, así como una gama de soluciones IAM/IAG (gestión de identidades y de accesos). La oferta de Beta Systems en el área de los centros de datos y la ciberseguridad garantiza que sus 1300 clientes en todo el mundo optimizan sus procesos de TI, protegen sus sistemas de información y cumplen los requisitos de gobernanza, gestión de riesgos y cumplimiento de normativas (GRC). Los clientes de Beta Systems son líderes de mercado de los sectores de banca y seguros, finanzas, industria, transporte y atención sanitaria. La sede de la empresa se encuentra en Berlín (Alemania). Beta Systems cotiza en bolsa desde 1997 y emplea a cerca de 300 personas. La empresa, junto con sus 16 filiales en propiedad y sus numerosas empresas asociadas, tiene una fuerte orientación nacional e internacional.

Beta Systems está presente en España con su propia filial local desde 1998. Para obtener más información, visite [www.betasystems.es](http://www.betasystems.es).



## Contacto

[marketing-f@betasystems.com](mailto:marketing-f@betasystems.com)

+34 9 13 07 76 75

*Libro blanco - Mayo de 2015*  
*Beta Systems Software España, S.L.*