accenture

High performance. Delivered.

Oportunidades y riesgos en la implantación de soluciones de Gestión de Identidad y Acceso

Seminario IBM sobre Soluciones de Gestión de la Seguridad

Madrid, 2 de Marzo de 2006

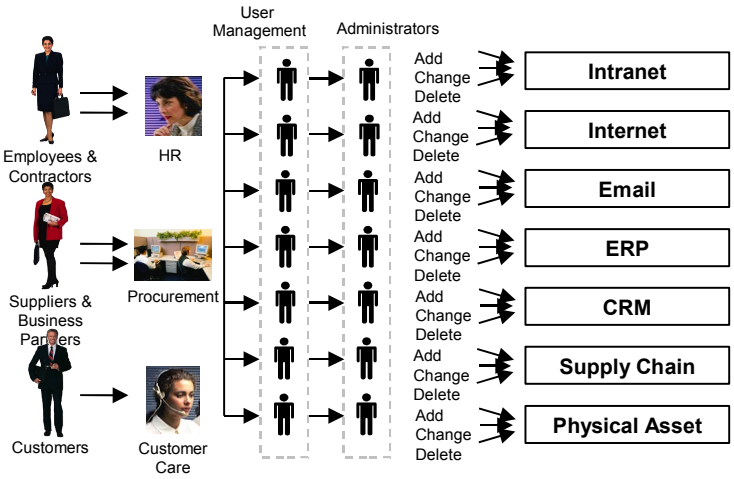
Las soluciones de Gestión de Identidad y Acceso se orientan a resolver algunos de los retos clave en la gestión de la Seguridad IT

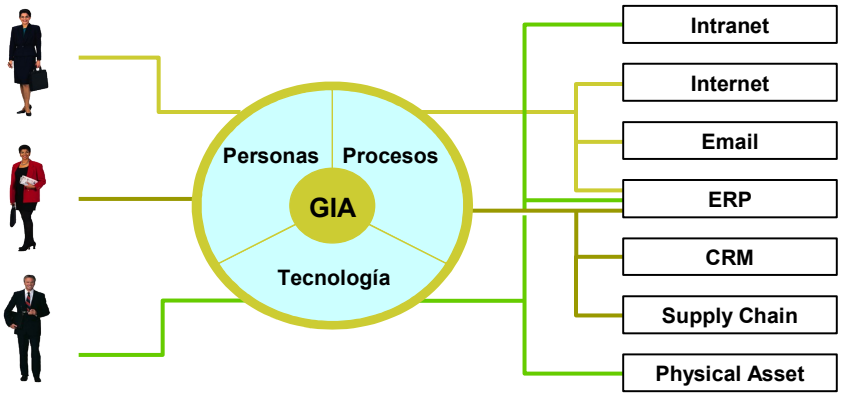
Retos clave

- Variedad de usuarios con acceso a aplicaciones y datos, incluyendo empleados, socios de negocio, clientes, proveedores, etc.
- Incremento en el número de aplicaciones de misión crítica
- Diferentes clases de usuarios con diferentes requerimientos de seguridad y control
- Insuficiencia de las medidas de seguridad periférica
- **¿Cómo mantener el control?**

Soluciones

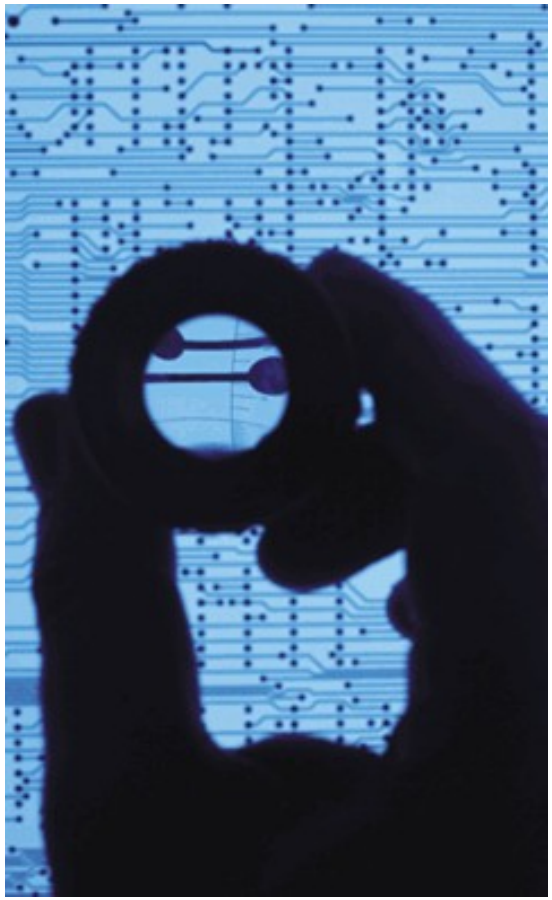
- Alinear organización, procesos y tecnología en la consolidación e integración de servicios de Gestión de Identidad y Acceso
- Proporcionar a los usuarios privilegios individualizados de acceso a partir de su identidad
- Implantar soluciones pragmáticas basadas en mejores prácticas





Componentes clave de una solución de Gestión de Identidad y Acceso

- ✓ **Gestión de identidad**
- ✓ **Control de acceso**
- ✓ **Aprovisionamiento**
- ✓ **Repositorios de datos de identidad y autorización**



Las soluciones de Gestión de Identidad y Acceso ofrecen oportunidades desde diferentes puntos de vista

Oportunidades de negocio

Oportunidades tecnoló

Oportunidades de Seguridad

Oportunidades de Negocio

Las soluciones integradas de gestión de identidad y acceso suponen un paso natural en la consolidación de los sistemas de seguridad mediante la centralización de la identidad de usuario y las políticas de seguridad aplicables a todos los niveles de la compañía, lo que redunda en la consecución de los siguientes beneficios clave de negocio:

- **Incremento de la productividad** mediante:
  - Reducción del tiempo necesario en los procesos de acceso a los recursos de negocio
  - Reducción del tiempo de pérdida de servicio provocado por ataques e infecciones de virus
- **Mejor identificación de usuarios** integrando los diferentes usuarios a nivel de infraestructura y de aplicación en una única identidad
- **Flexibilidad en la introducción de nuevos servicios y modelos de negocio, así como en la integración con entidades externas,** gracias a la mayor agilidad en el aprovisionamiento y a la posibilidad de federación de identidades

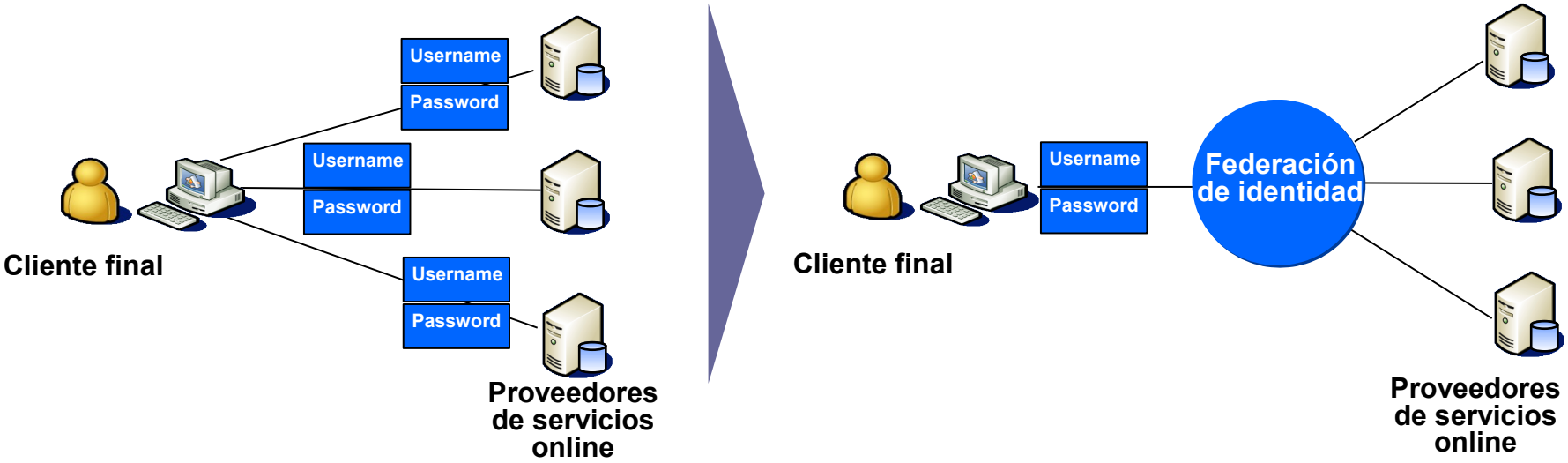
Ejemplo – Identidad federada en el acceso de clientes finales

Situación sin identidad federada

- Necesidad de registro independiente
- Cada proveedor online debe crear y gestionar credenciales separadas para el usuario

Beneficios de la federación

- Mejor experiencia para el usuario
- Adquisición simplificada de usuarios
- Mejoras en la seguridad



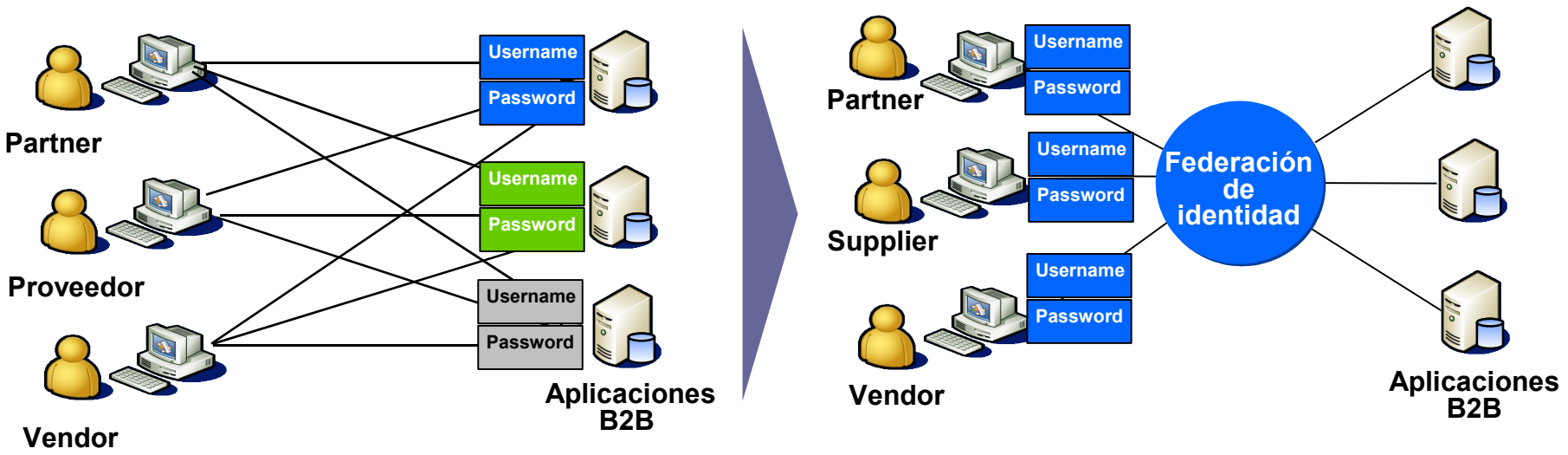
Ejemplo – Identidad federada en la relación entre negocios

Situación sin identidad federada

- Las entidades involucradas deben mantener las identidades de los socios y entidades externas con las que se relacionan
- Los proveedores deben mantener información sobre sus empleados en numerosos sistemas de clientes

Beneficios de la federación

- Reducción de coste administrativo
- Mejora de productividad
- Flexibilidad y rapidez en la integración con entidades externas, con menor coste de integración



Oportunidades tecnológicas

Las soluciones integradas de gestión de identidad y acceso proporcionan un gran abanico de funcionalidades para mejorar el acceso a los servicios de negocio:

- **Reducción del tiempo de activación de usuarios y de los errores administrativos** mediante la automatización de tareas rutinarias de administración de red
- **Delegación de la administración de las decisiones en materia de seguridad de red** a los responsables de negocio en lugar de a la organización de IT
- **Mejora de la experiencia del usuario** gracias a la reducción del número de identificadores y contraseñas
- **Automatización de los procesos** asociados a la gestión del cambio de usuarios de red y aplicación de políticas de seguridad
- **Reducción de los costes de desarrollo y mantenimiento** gracias a la automatización de las tareas de administración

Ejemplo – Gestión de Identidad y Acceso a nivel de infraestructura

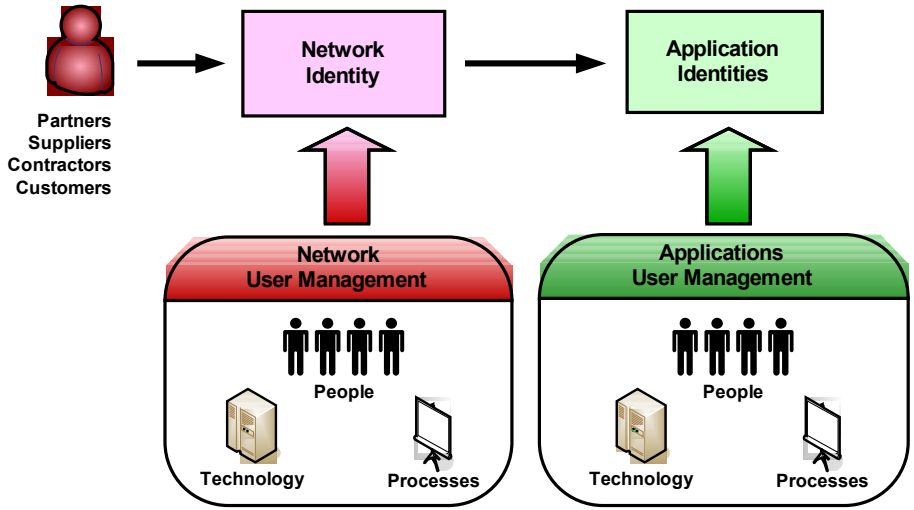
Con el paso del tiempo las infraestructuras de red han pasado de ser un elemento meramente de comunicaciones a una plataforma integradora de servicios.

- El actual modelo de negocio necesita el **acceso a los servicios independientemente de la localización** y la infraestructura que los soporta
- La infraestructura de red ya no sólo se limita al ámbito interno de las empresas, si no cada vez con más frecuencia se habilita el **acceso externo a los servicios**:
  - Acceso a clientes y proveedores desde plataformas no siempre suficientemente securizadas
  - Acceso a empleados (acceso a servicios más críticos, aunque normalmente desde plataformas más protegidas)
- La red, como elemento integrador, tiene el reto de resolver la **Identificación y autorización en el acceso a los recursos y servicios de la empresa**, consolidando la información de usuario (identidad) a lo largo de todas las capas de la infraestructura tecnológica

Ejemplo – Gestión de Identidad y Acceso a nivel de infraestructura

Retos

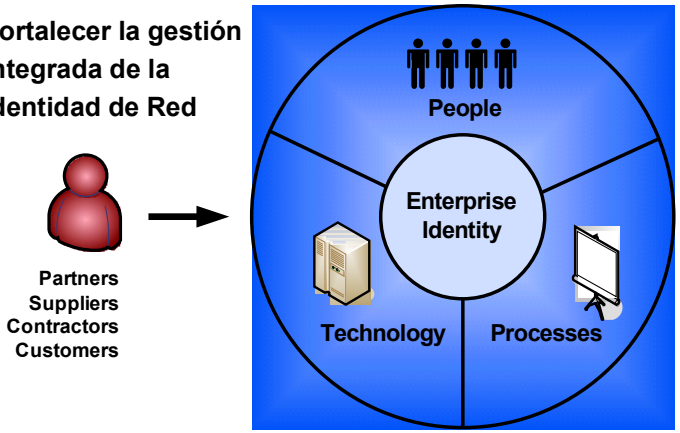
- Existencia de múltiples modelos organizativos, procesos y tecnologías para la gestión de usuarios tanto en el acceso a recursos de red como en el acceso a servicios y aplicaciones
- Creciente número de usuarios móviles con acceso a los recursos de red (como es el caso de socios de negocio, clientes, proveedores) y diferentes requerimientos
- Aumento de servicios críticos de negocio a los que se proporciona acceso desde fuera del perímetro de seguridad de la empresa
- Dependencia de políticas estáticas para el control de la seguridad perimetral de la red



Soluciones

- Apalancamiento de las inversiones realizadas en procesos, organización y tecnologías en los servicios de gestión de Identidad y Acceso (I&AM: Identity and Access Management)
- Integración y consolidación de los sistemas de gestión y control de Identidad mediante IBNP (Identity Based Network Provisioning)
- Habilitación y dotación de mayor inteligencia en la infraestructura de red a los sistemas de autentificación
- Accesibilidad individualizada a los servicios de red basada en el control de Identidad mediante la aplicación de políticas de control de contenido

Fortalecer la gestión integrada de la Identidad de Red



Oportunidades de Seguridad

La implementación de estas soluciones mejora la seguridad de la red corporativa mediante la correcta asignación de permisos y niveles de autorización a usuarios y recursos y a través de la imposición de políticas de seguridad en cada acceso

- **Asegurar el cumplimiento de los requerimientos de seguridad tanto a nivel de infraestructura como de aplicación**
- **Actualización inmediata de los niveles de seguridad de los usuarios** en función de cambios organizativos (cambio de departamento, abandono de la compañía, etc.)
- **Mantener el control** del ciclo de vida de las cuentas de usuario y políticas de seguridad ayudándose de herramientas de auditoria
- Gestionar y automatizar de forma **consistente y centralizada un entorno seguro** a lo largo de la red, sistemas y aplicaciones
  - Disponer de un foto completa de los privilegios de acceso de los usuarios
  - Facilitar la definición y aplicación de las políticas de seguridad
- Facilitar la **obtención y análisis de información de eventos de seguridad** para dar rápida respuesta a peticiones de auditorias y normativas.

Ejemplo – Modelo de control de acceso basado en perfiles (RBAC)

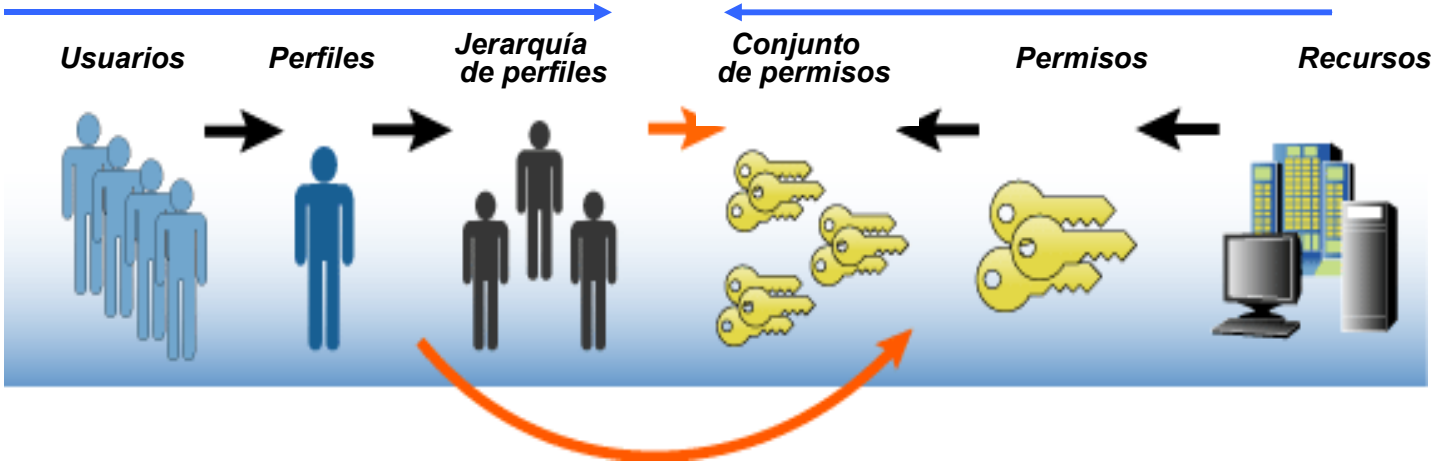
La implantación de un modelo de control de acceso basado en perfiles facilita la implantación de políticas de seguridad, pero exige un equilibrio entre la visión de negocio y tecnológica

ENFOQUE TOP DOWN

- Visión de negocio
- Estructura organizativa y procesos de negocio

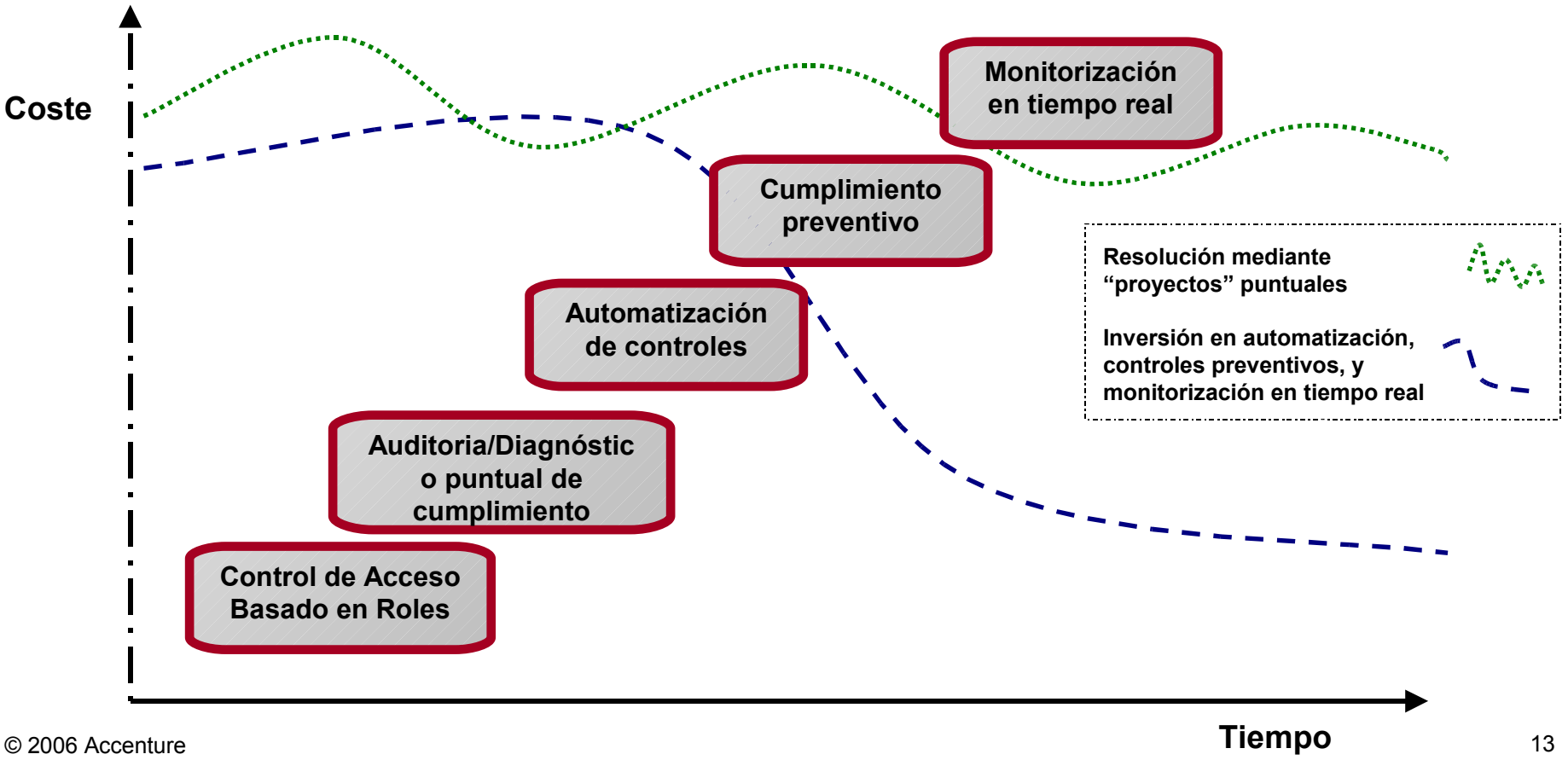
ENFOQUE BOTTOM UP

- Visión tecnológica
- Modelo de permisos en las aplicaciones y recursos de TI



Evolución de la arquitectura de controles y autorizaciones de usuario

De forma general se implantan soluciones limitadas que de forma reactiva "arreglan" los posibles fallos o situaciones de riesgo. Sería necesario disponer de un plan que establezca el mapa de ruta que permita alcanzar soluciones avanzadas de control preventivo y monitorización en tiempo real



Factores clave en la consecución de beneficios

El análisis coste-beneficio de estas soluciones debe tener en cuenta los factores clave de los que dependen las mejoras esperadas: factores de negocio, complejidad del modelo de autorización y acceso, volumen de usuarios, volumen de tareas administrativas y su complejidad

Costes

Coste en Software
En función del número de usuarios y dispositivos de acceso

Coste en Hardware
Servidores, equipos de comunicaciones, etc.

Servicios Profesionales
Análisis, planificación, diseño, construcción, pruebas y puesta en producción

Beneficios

Mayor eficiencia administrativa
Reducción de recursos de IT derivados de la mejora de la eficiencia en los procesos diarios de provisión de recursos de red; eliminación de aplicaciones de administración de seguridad de red obsoletas y con alto coste de mantenimiento

Mejora de la Productividad
Mejora de la productividad gracias a la eficiente provisión de recursos de red necesarios para el trabajo de usuarios, clientes y proveedores

Aprovechamiento de Recursos
Reducción de costes asociados a la utilización de recursos ya no disponibles para los usuarios (por ejemplo cuentas de correo)

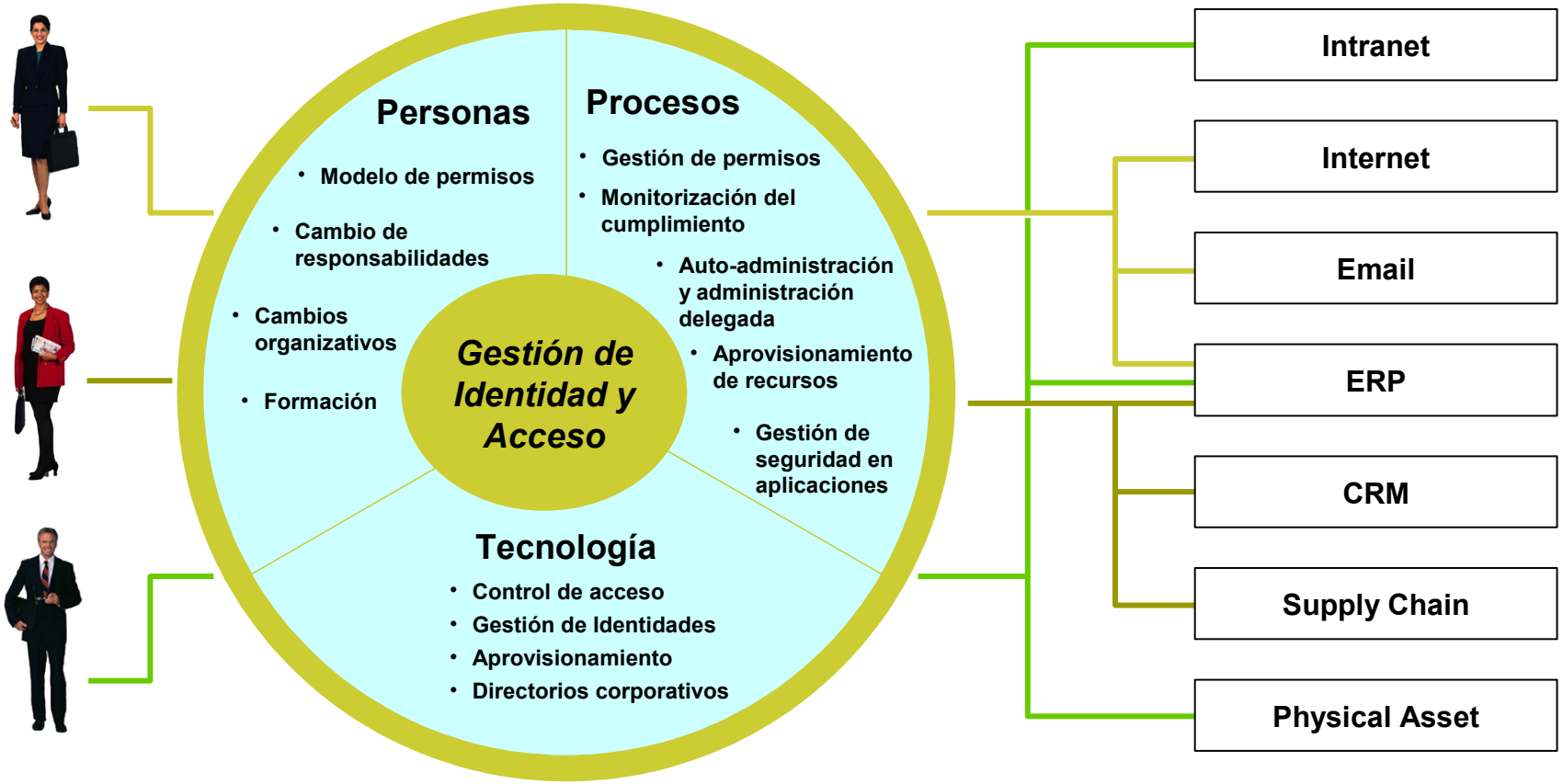
Oportunidades de negocio
Maximiza la contribución de empleados o socios de negocio a la base de la organización gracias a la posibilidad de acceder de forma rápida y segura a la infraestructura y contenido digital de la compañía

Reducción de Incidentes de Seguridad
Reducción del coste asociado a incidentes de seguridad a través de la aplicación eficiente de las políticas de seguridad

Riesgos a tener en cuenta en la implantación

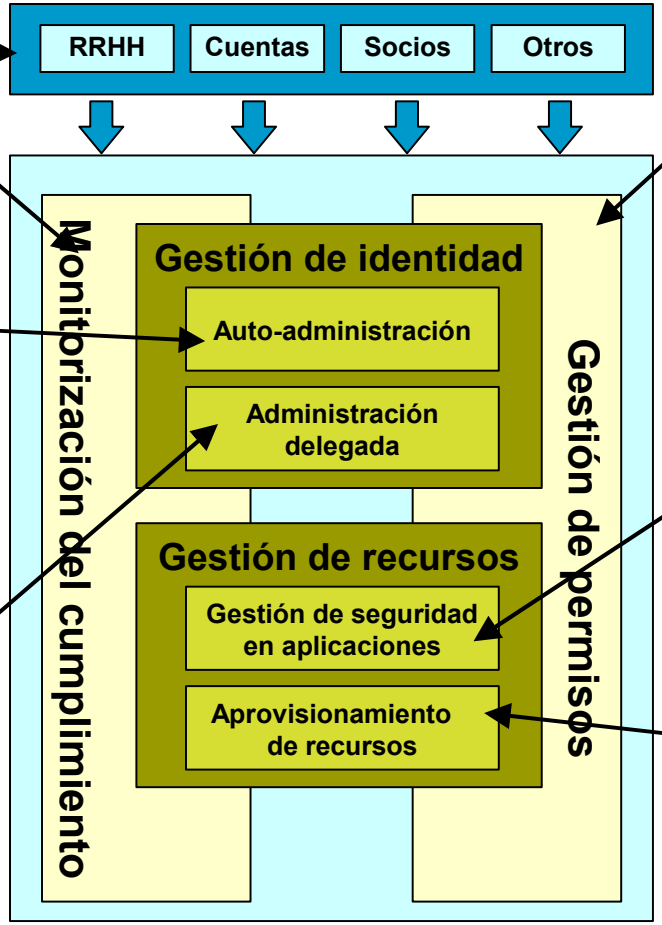
- **Incumplimiento de expectativas** de negocio o tecnológicas, con beneficios menores a los esperados o no materializados en los plazos esperados
- **Barreras organizativas** a la gestión integrada de identidades y acceso
- Incremento de complejidad en la **arquitectura global de seguridad**
- Elevado **coste de integración tecnológica** de la solución con aplicaciones existentes
- **Dificultad de evolución de la infraestructura tecnológica** si la solución elegida no ofrece garantías de evolución de acuerdo con los requerimientos tecnológicos globales

Comprender la naturaleza de la transformación que conllevan estas soluciones es crítico para su éxito:



Estas soluciones transforman los procesos existentes, automatizándolos y distribuyéndolos a los "propietarios" de negocio:

Procesos existentes que ofrecen entradas a los procesos de gestión de identidad y acceso



Monitorización

- ¿Cuales son las descripciones de roles?
- ¿Cómo se asignan los roles?
- ¿Quién aprueba las asignaciones?

Auto-administración

- Habilitar la auto-administración de los usuarios
- Registro de usuarios – auto-registro
- Cambio de contraseñas – permitiendo que los usuarios cambien sus contraseñas
- Gestión de perfiles de usuarios – permitiendo a los usuarios gestionar su perfil

Administración delegada

- Gestión de usuarios y grupos, delegando la administración por unidades, departamentos, etc.
- Procesos de aprobación por parte de los responsables de negocio

Gestión de permisos

- Entender las responsabilidades de empleados
- Correspondencia entre responsabilidades y roles
- Distinción de workflows de aplicación para diferentes roles
- Mantenimiento de roles y workflows de aprobación

Gestión de seg. en aplicaciones

- Registro de recursos
- Definición de controles de acceso – asignación de usuarios / roles a privilegios de acceso

Aprovisionamiento de recursos

- Automatización de la administración y gestión de recursos

La consideración del impacto en las personas es un factor clave de éxito en estas soluciones:

Modelo de permisos

- Definición de roles y modelo de privilegios
- Correspondencia entre roles y niveles de acceso a recursos

Responsabilidades

- Desplazamiento de responsabilidad a los usuarios finales mediante delegación y auto-administración
- Desplazamiento de responsabilidad a los “propietarios” de recursos
- Nuevas responsabilidades de administración de seguridad

Cambios organizativos

- Reducción de actividad en help-desk asociada a la gestión de usuarios, nuevas actividades de gestión de identidad y acceso
- Nueva función central de administración de la infraestructura de Gestión de Identidad y Acceso

Formación

- Formación en administración de seguridad según el nuevo modelo
- Formación a usuarios en nuevos procesos de registro y administración

Factores clave de éxito

- Definir con claridad la **visión organizativa** y los **resultados objetivo de negocio**
- Comenzar con un **plan estratégico** para el desarrollo del proyecto en fases alineadas con los requerimientos y el entorno de negocio
- **Alinear la solución** con el personal de la organización
- Definir la solución a partir de un **buen conocimiento de los procesos de negocio** y los procedimientos de gestión de usuarios
- Diseñar una solución integrada en la **arquitecturas global de seguridad**
- Hacer uso de componentes tecnológicos con **capacidades comprobadas de integración**
- **Apoyarse en estándares abiertos** para maximizar la interoperabilidad en el futuro

Preguntas

?