


Seguridad

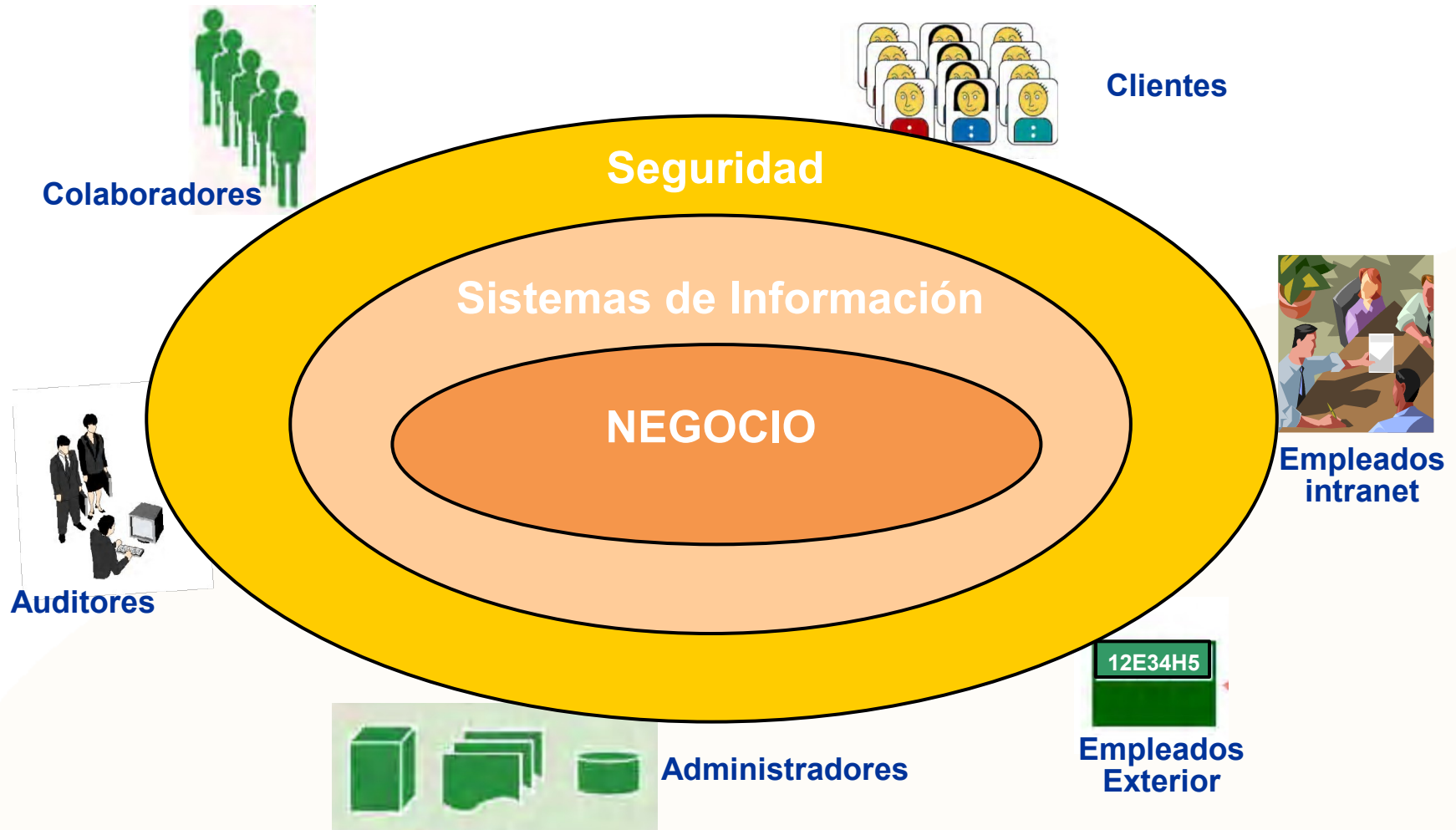
Un caso real sobre Gestión de identidades

Madrid, Marzo de 2.006

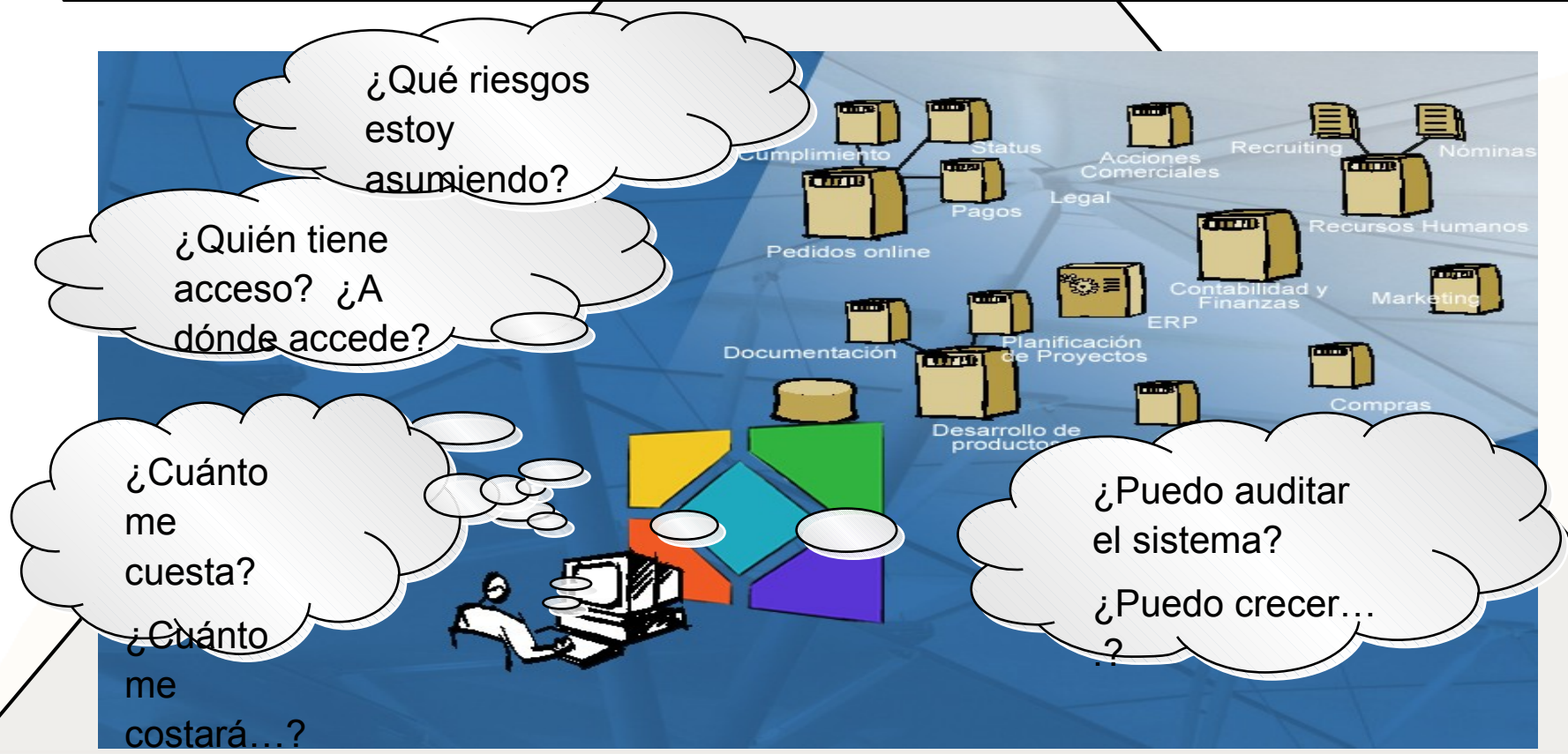


Juan Ignacio Gordon
www.es.capgemini.com

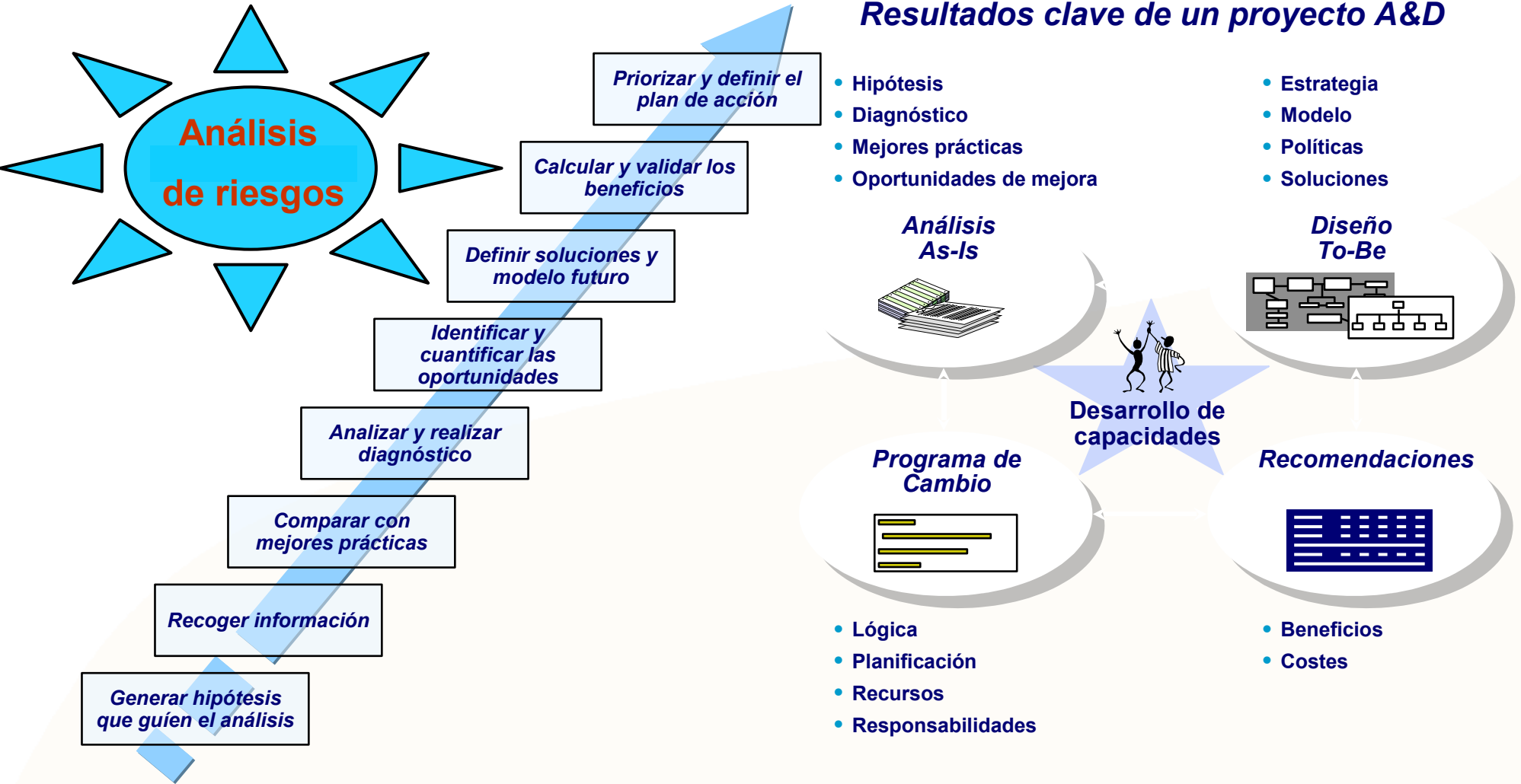
Contexto



¿Cómo está mi gestión de identidades?



Metodología: Dónde y cómo pueden mejorar. Qué puedo esperar del cambio



Situación de partida: Resumen

Fortalezas

- Existen políticas de seguridad correctas y extendidas*
- Se han desarrollado normas, procedimientos y órdenes de trabajo adecuadas y de obligado cumplimiento*
- Se cumple con la legalidad LOPD*
- Existen controles*

Debilidades

- Existe gran dificultad para implantar y aplicar las políticas*
- Es muy difícil y costoso ejercer la actividad de control*
- Se actúa siempre a reacción*
- No es posible hacer previsiones realista*
- La gestión es muy costosa e ineficiente*
- El mantenimiento (técnico y legal) es más difícil cada día y no guarda proporción con los resultados obtenidos*

Debilidades encontradas

Gestión

- Distintos puntos de entrada de la información sin interrelacionar
- Distintos usuarios y contraseñas para un mismo recurso
- Diferentes interfaces de administración según sistema
- Entrada de datos manual.
- Repetición de operaciones por error
- Incumplimiento de Políticas (atributos sin normalizar)
- Alto volumen de cuentas y atributos
- Alto porcentaje de cuentas sin conciliar (huérfanas)
- Sincronización de la información muy compleja (scripts).

Ineficacia / costes

- No se utilizan las posibilidades tecnológicas en la automatización e información de los procesos (Workflows, e-mail, mensajes, web, ...)
- Coste alto de Administración
- Número alto de incidencias en CAU
- Imposibilidad de aplicar diferentes políticas
- Imprescindible presencia física de administradores o responsables para la realización de las funciones
- Mucho tiempo de espera en las altas y descontrol en las bajas
- Incapacidad de ejercer control de acceso y Auditoría
- Evolución difícil (cuantos más servicios mayor complejidad y coste exponencial)

Gran complejidad

Procesos actuales de sincronización

- 36 procesos de carga más de la mitad con 2 o 3 subprocesos
- Aproximadamente 100 atributos / campos para un esquema global
- Una media de 20 atributos por proceso
- Necesidad de desarrollar aplicación web con diversos interfaces
- Estimación esfuerzo inicial 32 meses hombre a realizar en 8 meses

Requisitos

Gestión

- Un solo punto de entrada, una interfaz única y basada en Web*
- Usuarios personales*
- Unificación y sincronización de la información automática*
- Minimizar las entradas manuales potenciando los valores por defecto*
- Normalización de atributos y nombres*
- Procedimientos automáticos de conciliación de cuentas*
- Posibilitar la delegación de funciones*
- Conciliación de cuentas*

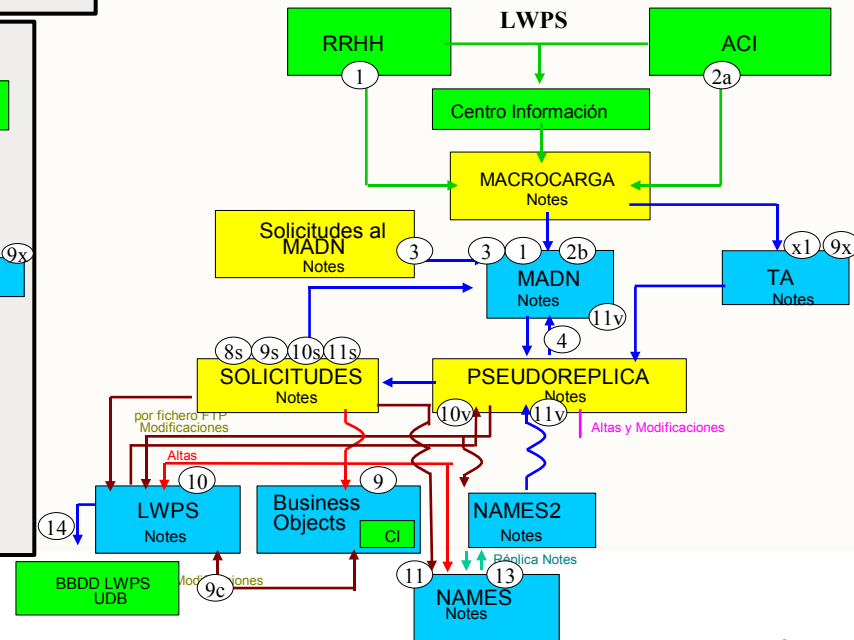
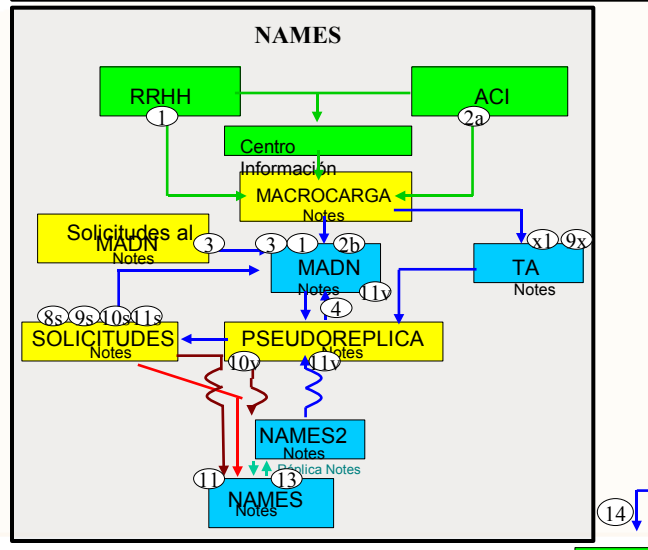
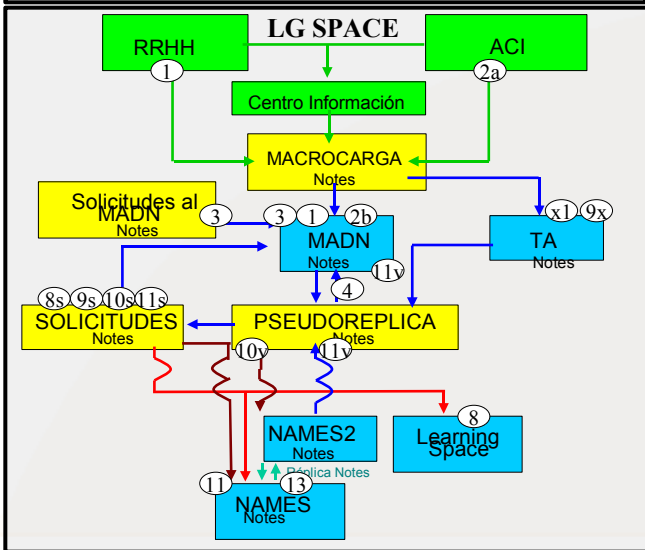
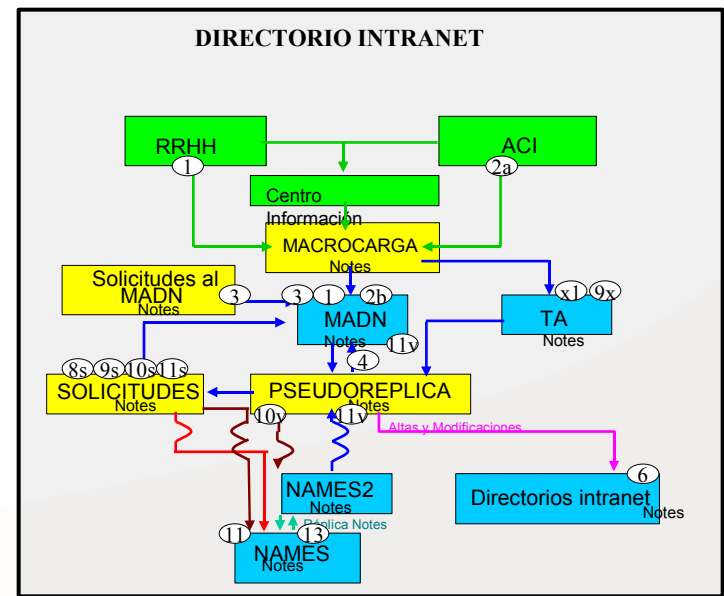
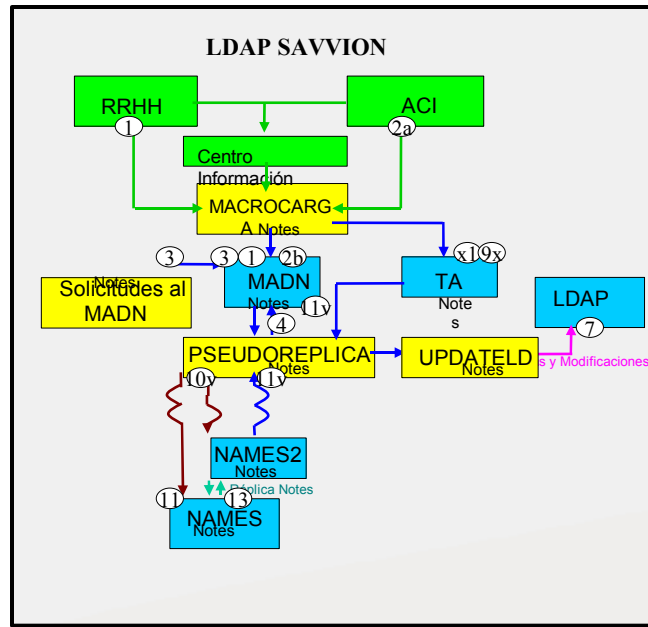
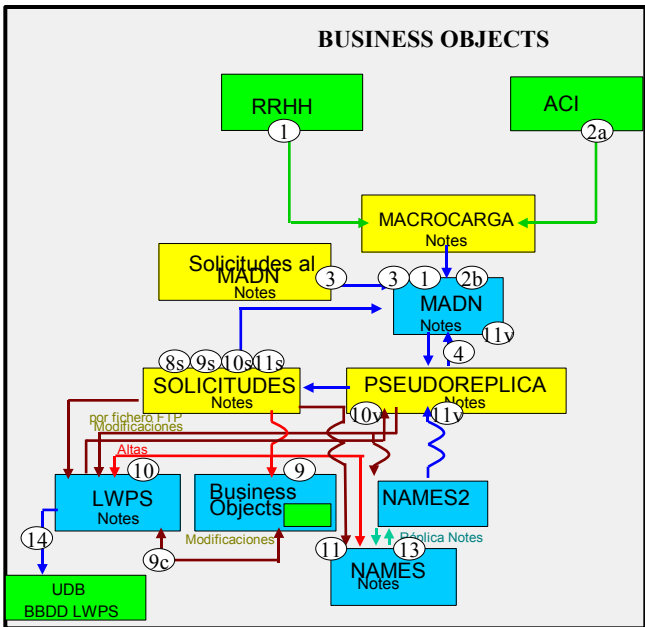
Eficacia

- Utilizar la tecnología actual para facilitar la comunicación*
- Liberar de actividad rutinaria a perfiles de administración por la utilización de interfaces únicas de Gestión*
- Reducir drásticamente las incidencias debidas a cambios de contraseñas. Incremento del autoservicio*
- Potenciar la aplicación extensiva de las políticas y el control de aplicación*
- Desarrollo al máximo de la Gestión basada en WorkFlow (ciclo de validación)*
- Altas inmediatas para los valores estándar. Bajas automáticas*
- Facilitar los nuevos desarrollos en el marco común*

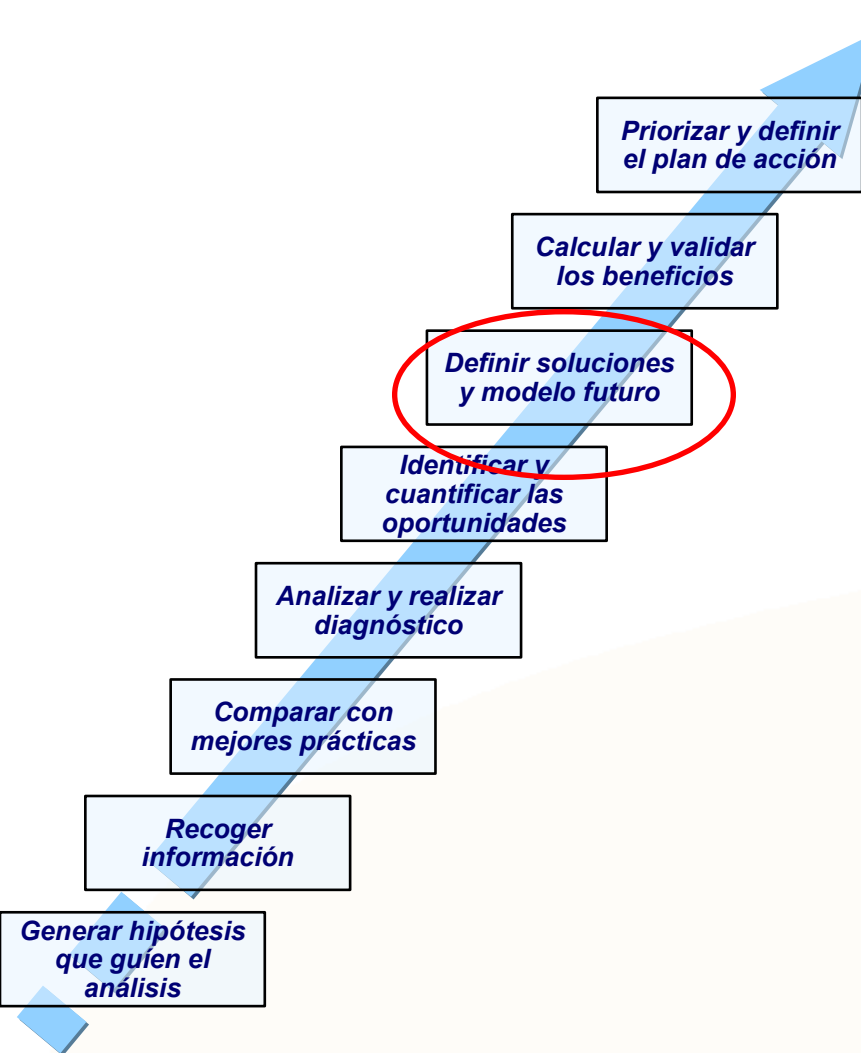
Cumplimiento legal

- Obtención de las listas de usuarios y permisos*
- Automatizar los cambios periódicos de contraseñas*
- Asegurar la correcta definición de las cuentas según política de seguridad*
- Asegurar el acceso correcto a los datos según perfiles profesionales*
- Controlar el acceso a los sistemas y registro*
- Controlar el uso adecuado de los identificadores*
- Amplio control de acceso y Auditoría*

Modelo de procesos candidatos muy complejos



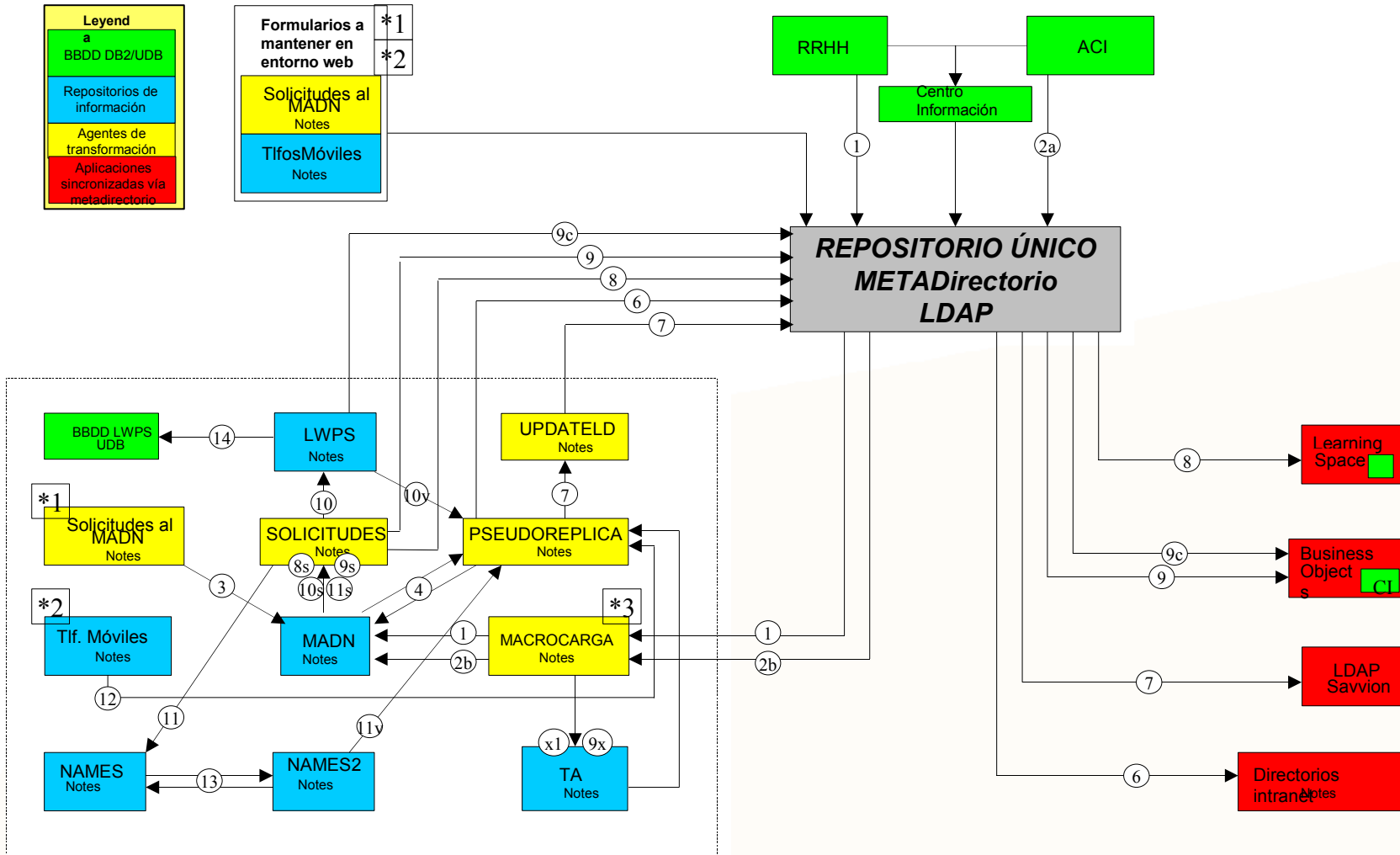
Estudio primera alternativa



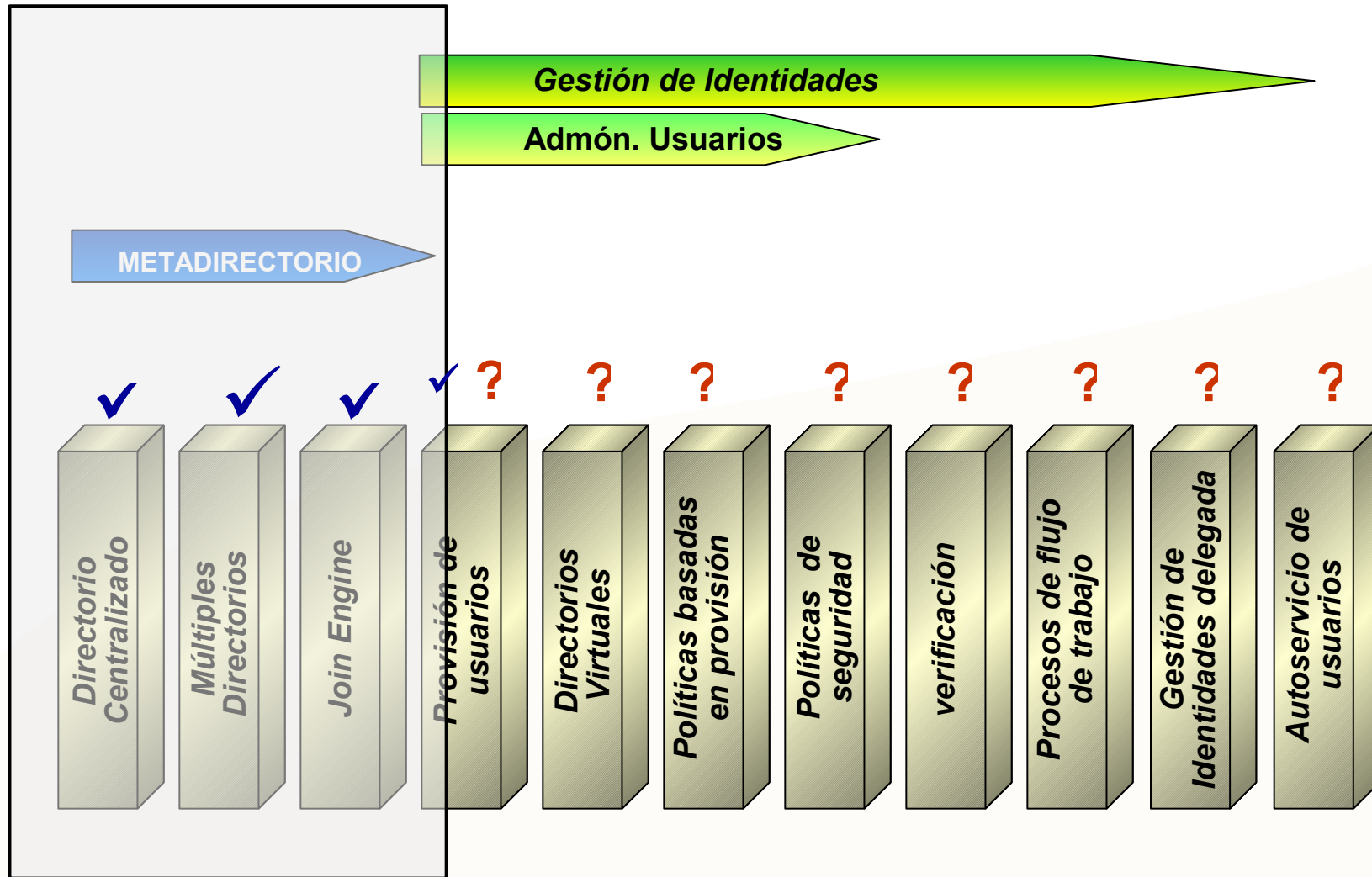
- **PROPUESTA: Alternativa 1. Inicio.**
- **Abstracción de orígenes de información para sincronización**
 - 1.1.- Altas de empleados y colaboradores externos desde las fuentes origen (RRHH,...)
 - 1.2.- Datos que han sido procesados por L.Notes
 - 1.3.- Desarrollo de formularios en entorno web para peticiones de altas o modificaciones.
- **Abstracción de destinos desde el repositorio central**
 - 1.- Procesos de salida desde repositorio central hacia al resto de fuentes
 - 2.- Resto de procesos (dentro del entorno Lotus Notes), se consideran internos al propio sistema Lotus Notes.

Fuente: Capgemini Delivery

Primera alternativa

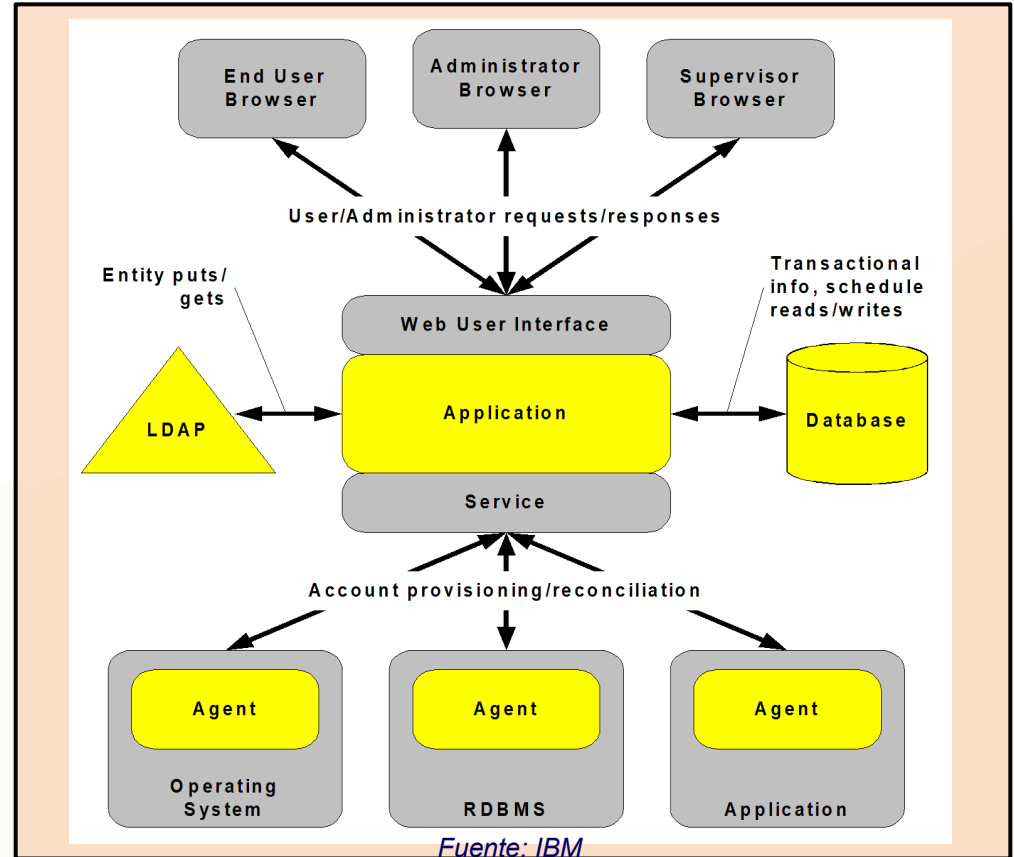


Insuficiente alcance respecto al modelo futuro



Propuesta ajustada al modelo: Nuestro objetivo

Fase I: Gestión de identidades con Tivoli Identity Manager (TIM)



Fase II: Web Single Sign On: Por decidir

Fase III: Single Sig On: Actualmente no contemplado

Muchas Gracias por su atención