IBM Forum

El valor de la gestión de Identidades

MORSE

02 de Marzo de 2006

Agenda

- Los tópicos en gestión de identidades revisados
- Caso práctico real
- Un paso atrás, para tener más perspectiva
- Visión global integrada

I'll take you there

El valor de la gestión de identidades, los tópicos: REVISED ….

La problemática de la gestión de seguridad

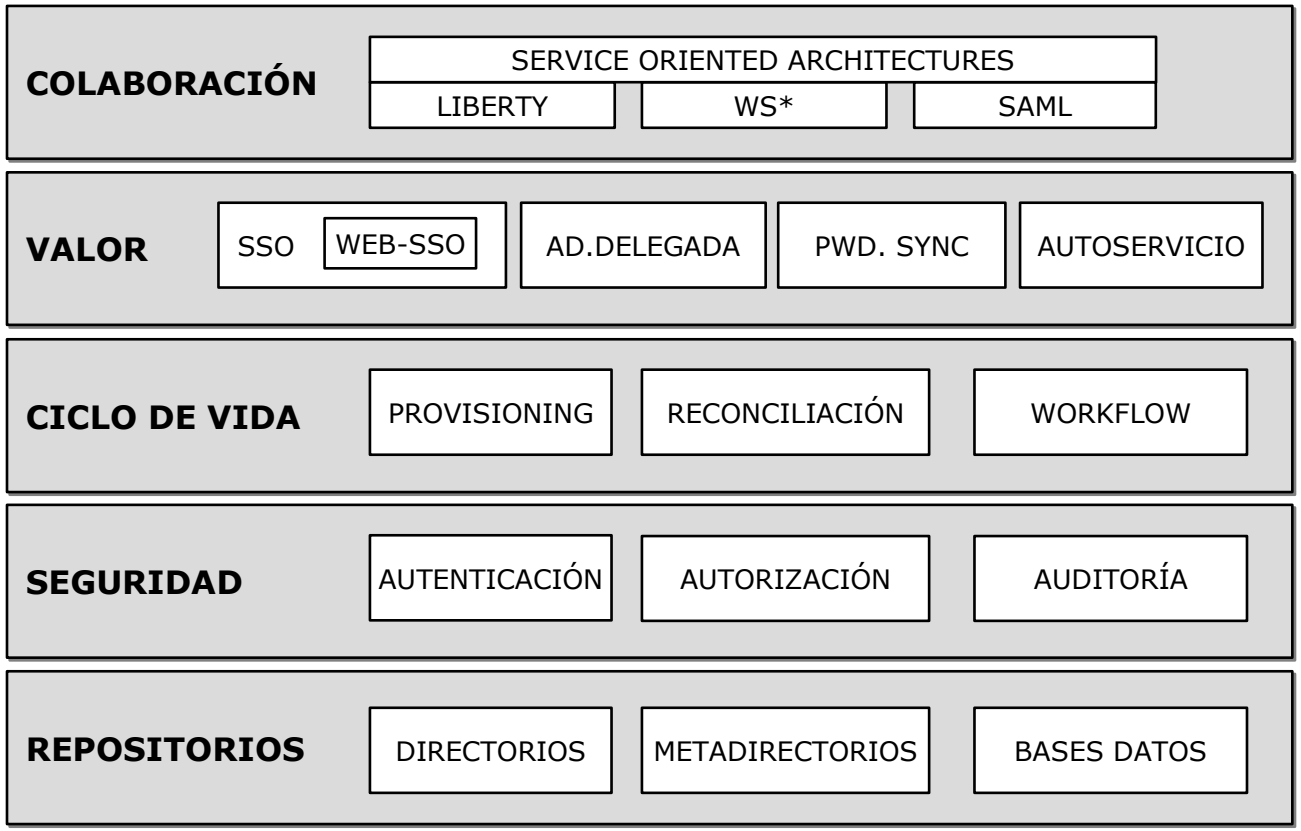
1. Costes elevados en la administración de seguridad
2. Falta de información sobre qué usuarios pueden acceder a qué recursos, y si la realidad está alineada con las políticas establecidas
3. Los usuarios tardan mucho en estar habilitados en los diferentes entornos
4. Gestión de contraseñas es cada vez más difícil a medida que incrementa la complejidad del entorno
5. La seguridad de las aplicaciones propietarias es inadecuada y cara
6. Es necesario limitar el acceso a información de carácter personal en los sistemas, para poder cumplir con la LOPD
7. Es necesario un mayor control para poder cumplir con las auditorías de seguridad
8. La información sobre identidades está repartida en muchos repositorios y no es coherente
9. Existen muchas fuentes de alertas de seguridad que no aportan información útil y manejable

El coste de una gestión de Identidad deficiente

Gestionar Identidades en una empresa es un proceso complejo y de gran carga para los administradores

Nuevo usuario establecido	Habilitar nuevo usuario	Usuario productivo	Desplegar nuevas iniciativas	Deshabilitar usuarios/ iniciativas
29% de compañias ven el despliegue e-business a los clientes como la preocupación número 1	Tiempo necesario hasta 12 dias	Help Desk cuesta 20$ por llamada para pw resets	Hasta el 20% del tiempo de desarrollo en app. para control de acceso	30-60% de cuentas existentes son inválidas
• **Proceso aprobación manual** • **Habilitación manual de cada cuenta de usuario**	• **Multiple logins** • **Multiple Help Desk calls for password resets and account updates**	• **Código de seguridad escrito en cada aplicación** • **Habilitación manual y actualización de derechos en cada recurso**	• **Cada cuenta de usuario gestionada manualmente**	
• **Mas tiempo para que el usuario sea productivo** • **Costes administrativos mas altos**	• **Productividad y satisfacción mas bajos de los usuarios** • **Costes de Help-desk mas altos**	• **Costes de desarrollo mas altos** • **Mas tiempo en desarrollo**	• **Muchos incidentes de cuentas huerfanas** • **Costes administrativos mas altos**	

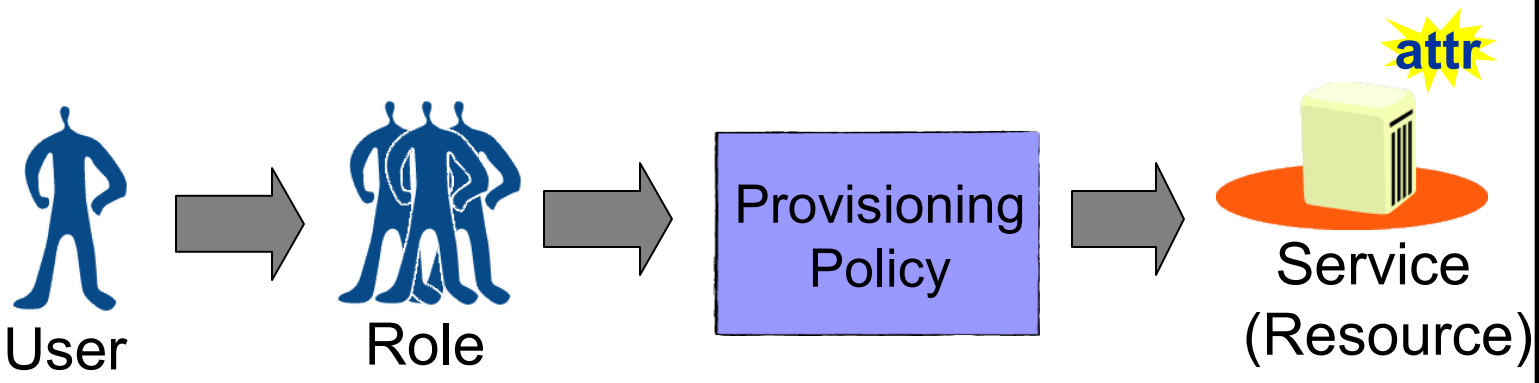
Arquitectura de la gestión de identidades



I'll take you there

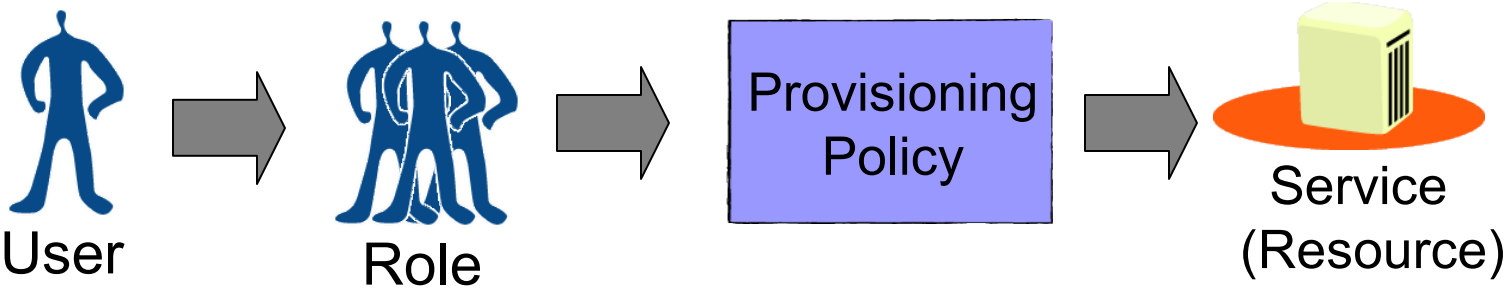
MORSE

El modelo de provisionamiento



- Un role es una colección de usuarios con una responsabilidad común
- Los roles pueden ser estáticos o dinámicos
- Los roles dinámicos están definidos sobre atributos LDAP
- El provisionamiento está basado en la pertencia a un role
- Las Provisioning Policy gestionan a los miembros de un role y pueden llegar a definir atributos de un usuario

La Reconciliación compara "Qué es" con "Qué debería ser"



- La reconciliación es un proceso de comprobación de las políticas definidas (p.e. atributos en un servicio)
  - IM puede hacer "roll back" de cambios no autorizados
- La reconciliación identifica cuentas huérfanas
  - Adopted, suspended, restored or de-provisioned

Identity Manager

- Reconocido por los analistas como una solución líder.
- Fácil configuración y adaptación a entornos existentes.
- Amplio soporte de aplicaciones y plataformas.
- Add-ons propios y de terceros, enorme aportación de valor.
- Entorno seguro y escalable.
- Experiencia en instalaciones a nivel mundial.

I'll take you there

El valor de la gestió de identidades, caso práctico:
Valor demostrado …..

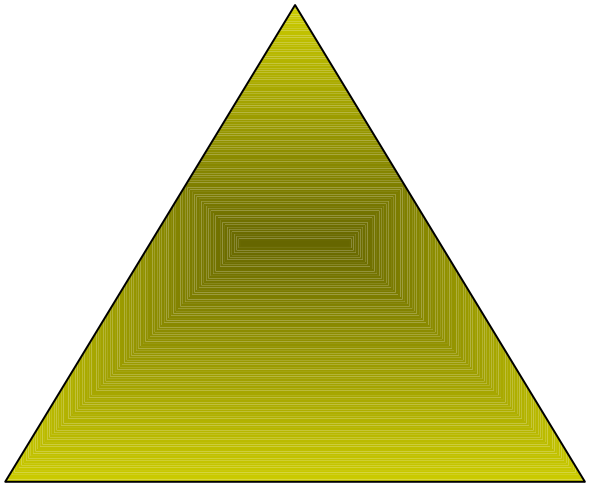
Fases del proyecto

- Fase 1: Análisis
- Fase 2: Diseño
- Fase 3: Implementación
- Fase 4: A día de hoy
- Fase 5: El futuro

I'll take you there

FASE 1 – ANÁLISIS
Algunos factores a tener en cuenta…

Legislación Nacional

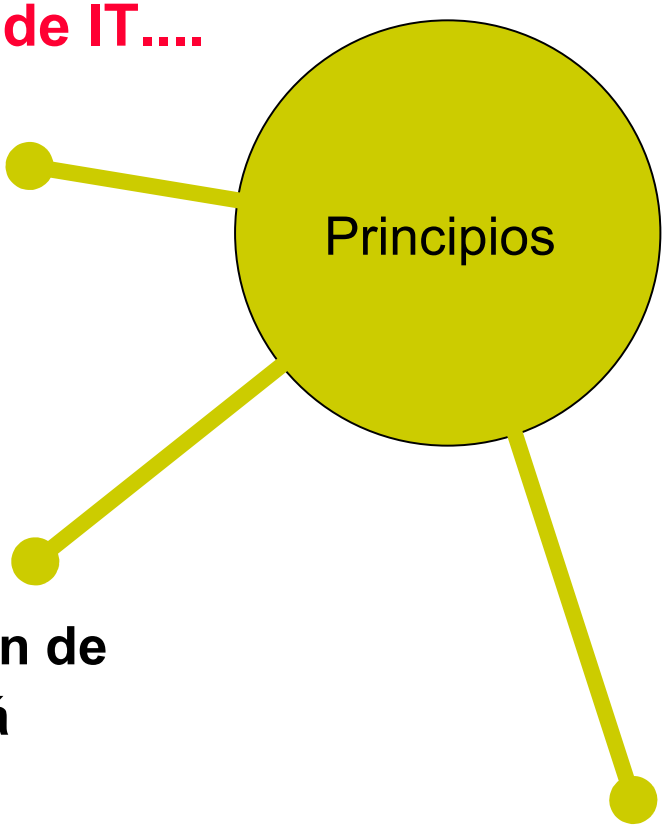


Políticas de Seguridad de IT

Situación Actual

FASE 1 – ANÁLISIS
Política de Seguridad de IT....

Cada departamento es responsable de definir y mantener su entorno de seguridad adecuado



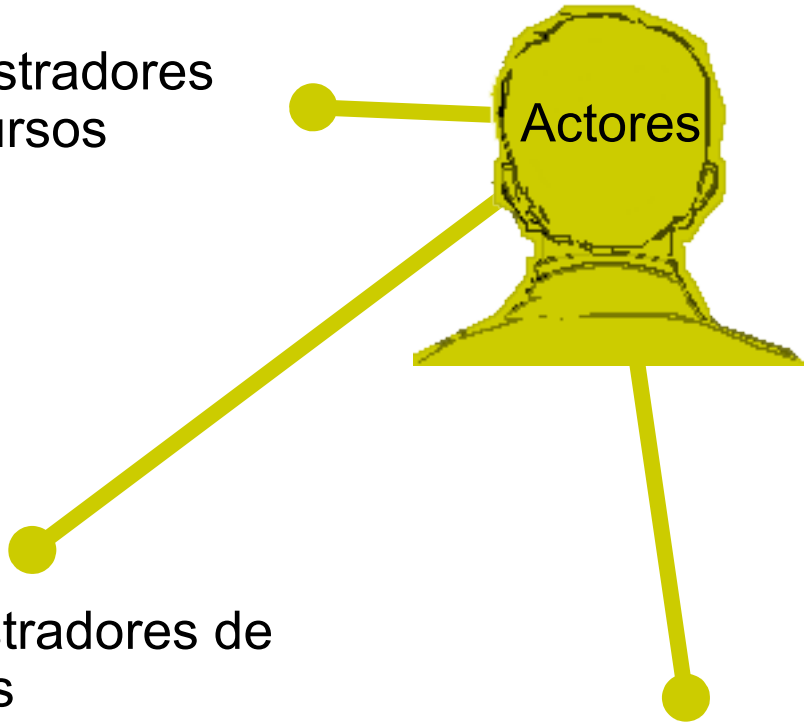
La administración de la seguridad está descentralizada

Política de control de acceso discrecional y basada en Roles

I'll take you there

FASE 1 – ANÁLISIS
Política de seguridad IT

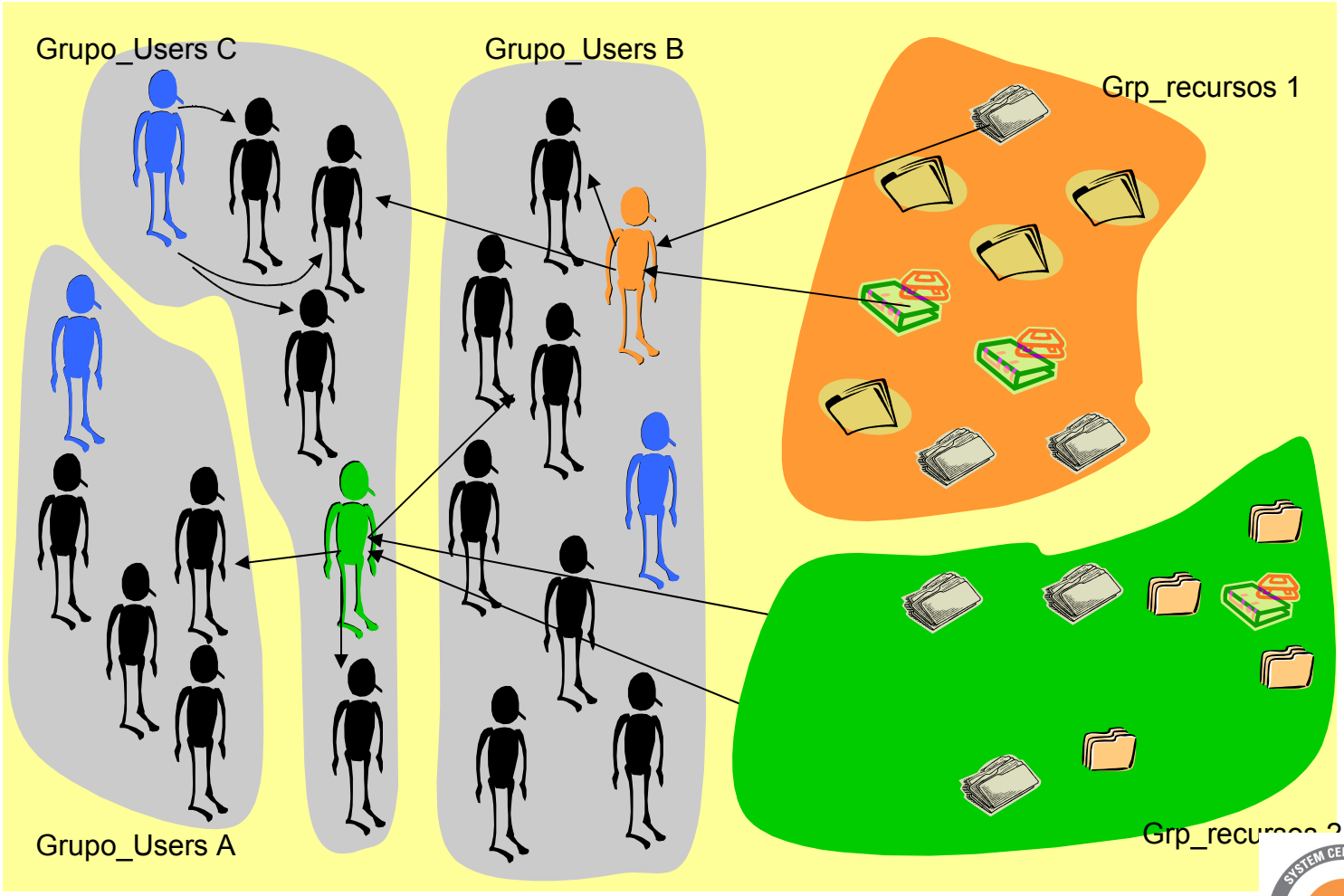
Administradores de recursos



Administradores de usuarios

Administrador del Sistema de Seguridad

FASE 1 – ANÁLISIS
Todo junto …



I'll take you there

FASE 1 – ANÁLISIS
"Situación de partida"

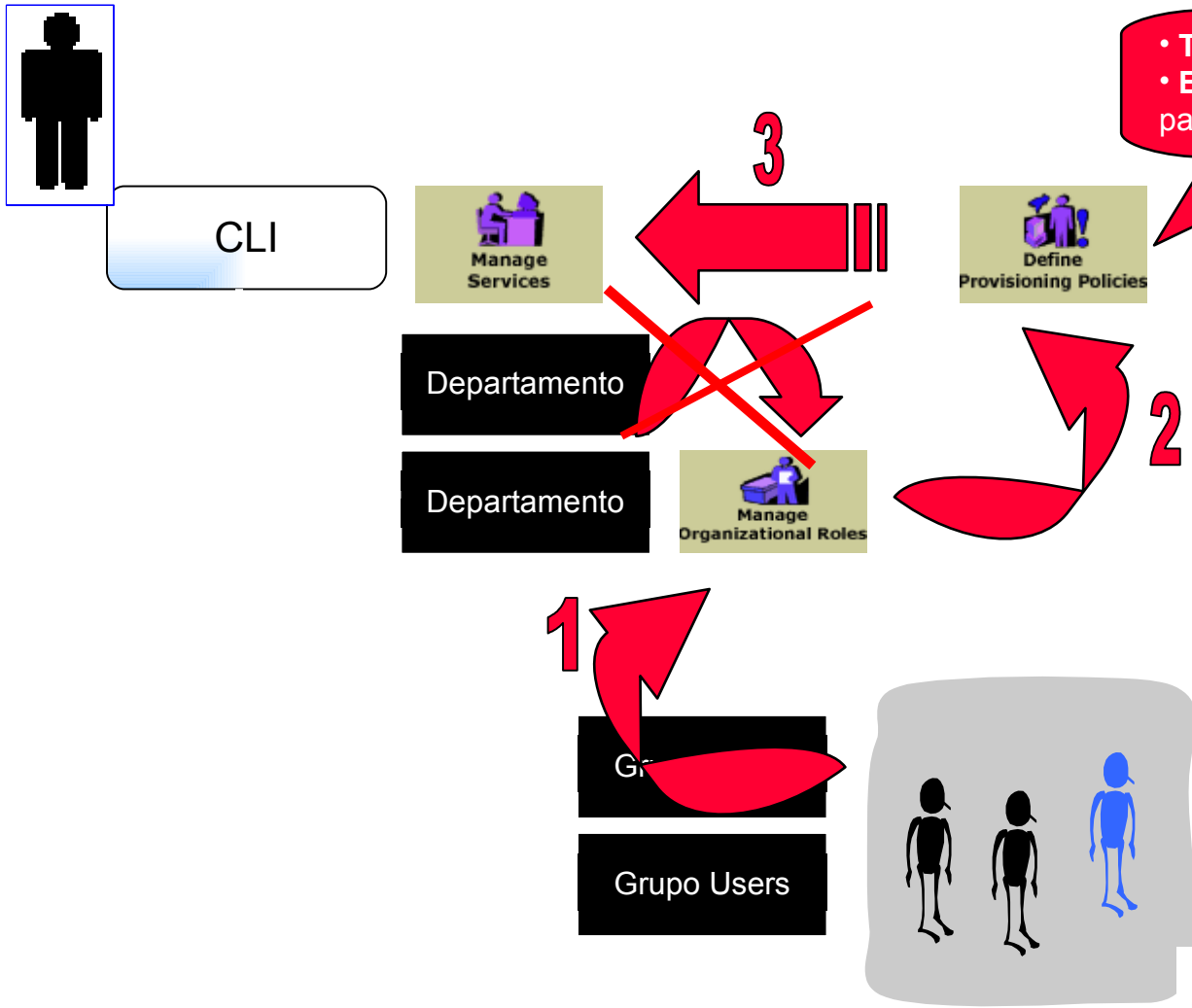
- **La política está totalmente implementada en su sistema z/OS mediante una aplicación desarrollada internamente.**
- **Los departamentos están acostumbrados a:**
  - Gestionar y controlar sus cuentas de usuarios.
  - Gestionar y controlar sus recursos de IT.
- **El departamento de auditoria interna está acostumbrado a:**
  - Acceder a toda esta información.
  - Auditar las actividades de administración de la seguridad.

I'll take you there

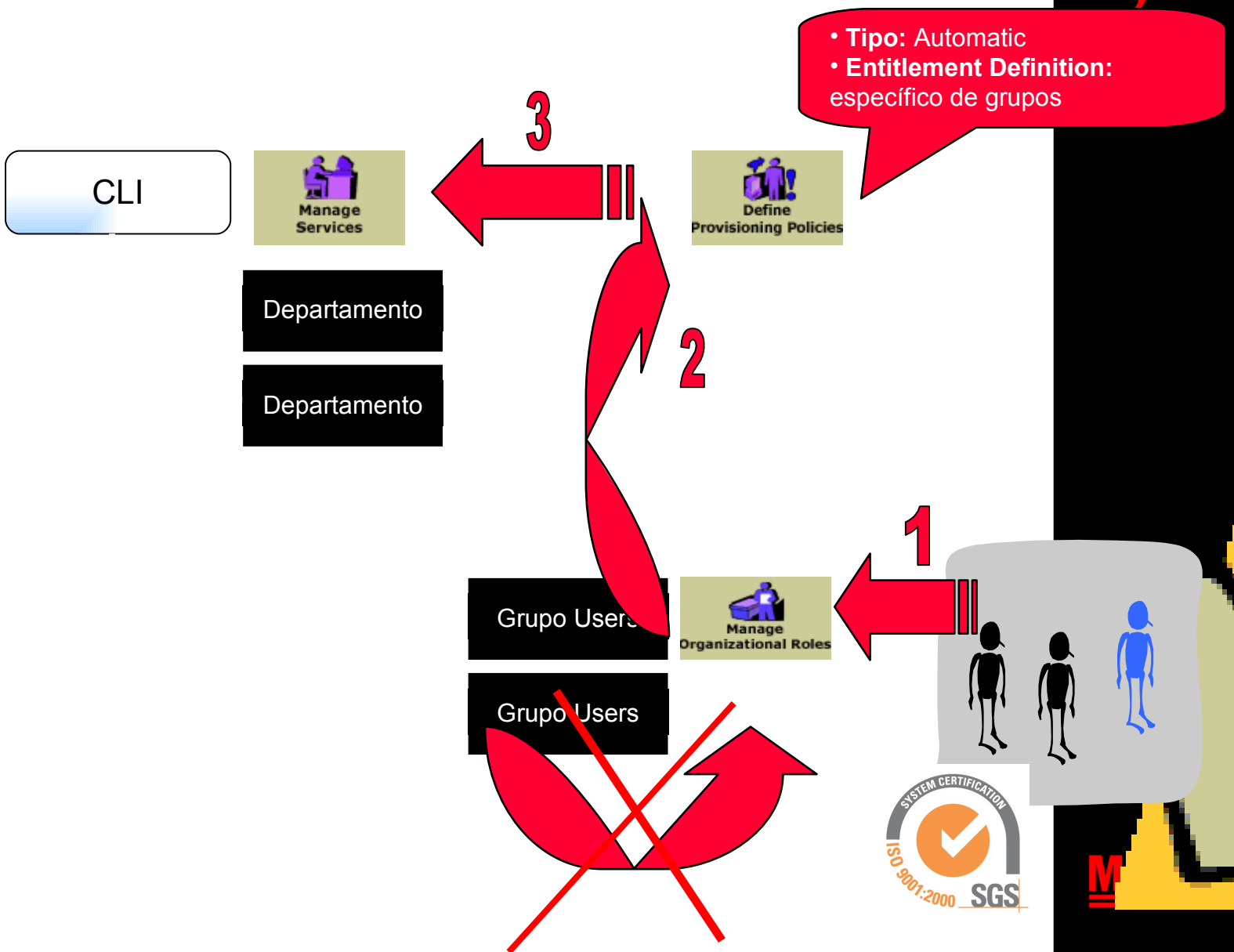
FASE 2 - DISEÑO

- **Objetivo principal**
  - Delegar la administración de las cuentas de los usuarios de los administradores de sistemas a los administradores de usuarios.
    - Provisioning: add/delete, suspend/restore and change password.
    - Granting/Revoking authorization.
    - Auditing.
- **Puntos clave**
  - Traducción de los conceptos de los administradores de usuarios y de recursos a TIM, punto de vista de administración.
  - Los usuarios finales de TIM no van a ser personal técnico.

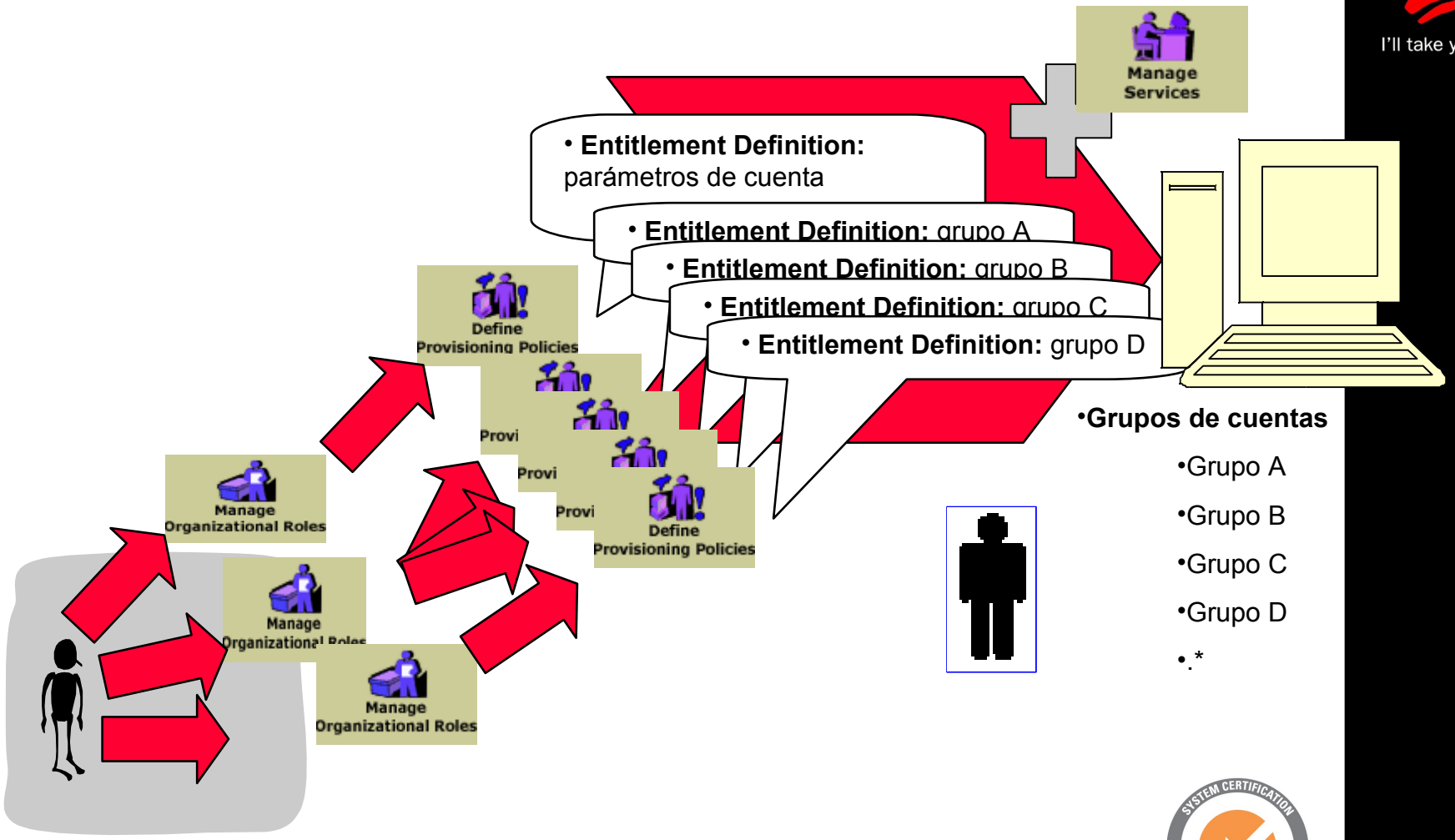
FASE 3 – IMPLEMENTACIÓN
Aprovisionamiento



FASE 3 – IMPLEMENTACIÓN
Granting/Revoking Authorization



FASE 3 – IMPLEMENTACIÓN:
Aprovisionamiento + Autorización.



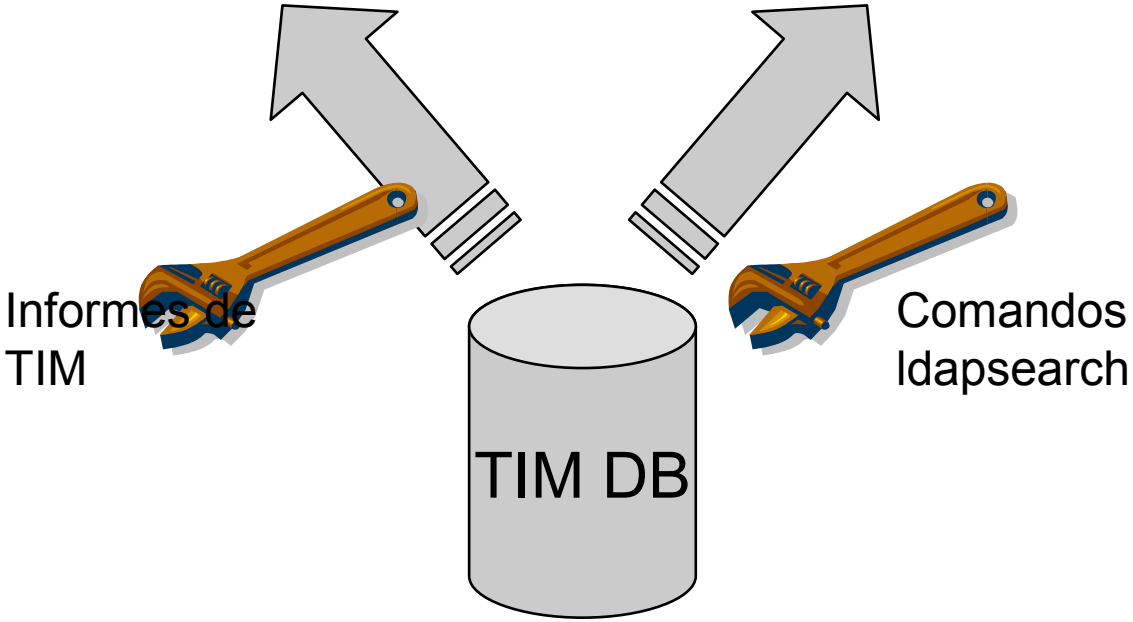
FASE 3: IMPLEMENTACIÓN
Informes y Auditoria

AUDITORIA

- Operaciones de cambio de password.
- Autorizaciones sobre recursos Grant/Revoke?

INFORMES / REPORTING

- Recursos a los que un usuario tiene acceso.
- Usuarios gestionados por un AU.
- Diferencias entre TIM y las plataformas nativas



FASE 3: IMPLEMENTACIÓN

- **Alcance**
  - 2800 personas.
  - 3900 cuentas Windows sobre 1 Active Directory.
  - 3150 buzones de Exchange repartidos en 2 sites.
  - 1800 cuentas UNIX/DCE en 30 servidores.
  - 1300 cuentas Oracle en 32 instancias.

I'll take you there

Fase 4: A día de hoy

- **En producción:**
  - 100 % de las unidades de negocio.
- **Siguientes pasos:**
  - Crecimiento de los recursos gestionados.
  - Definición de Roles funcionales, nuevos tipos de Roles, Jerarquía.
  - Aumentar el tipo de sistemas gestionados:
    - Windows 2003, ya está hecho.
    - Exchange 2003.
    - SQL Server.
    - Paso de DCE a Kerberos, con IDI.
  - Set up de nuevas funcionalidades de TIM
    - Workflows para aprobaciones y autorizaciones.
    - Integración de TIM y TAM.

I'll take you there

MORSE

Lo que dicen nuestros clientes

- **Se redujo el tiempo para dar de alta usuarios desde más de dos días hasta menos de dos horas.**
- **La modificación de permisos a usuarios existentes se realiza en 15 minutos.**
- **El personal de TI cualificado puede utilizar su tiempo en actividades mucho más importantes y estratégicas, y no en los problemas de gestión del día a día. La gestión de usuarios puede ser realizada por personal técnico de nivel medio.**
- **Se emplea un 40% menos de tiempo en reseteo de contraseñas.**
- **La tasa de error ha descendido desde un 10% a prácticamente un 0%, y los administradores de seguridad son capaces de localizar las cuentas huérfanas.**
- **Los informes son mucho más sencillos al disponer de información consolidada en un repositorio.**
- **Se tiene la seguridad de que sólo las personas autorizadas tienen acceso a datos y sistemas sensibles.**

FASE 5: Después de TIM …… y el futuro

- **Mejora continua del sistema de gestión de identidades**
- **Otras soluciones de seguridad TIVOLI implementadas:**
  - IBM Tivoli Risk Manager
  - IBM Tivoli Access Manager for e-Business
  - IBM Tivoli Access Manager for Business Integrator?
  - IBM Tivoli Access Manager for Operating Systems?

I'll take you there

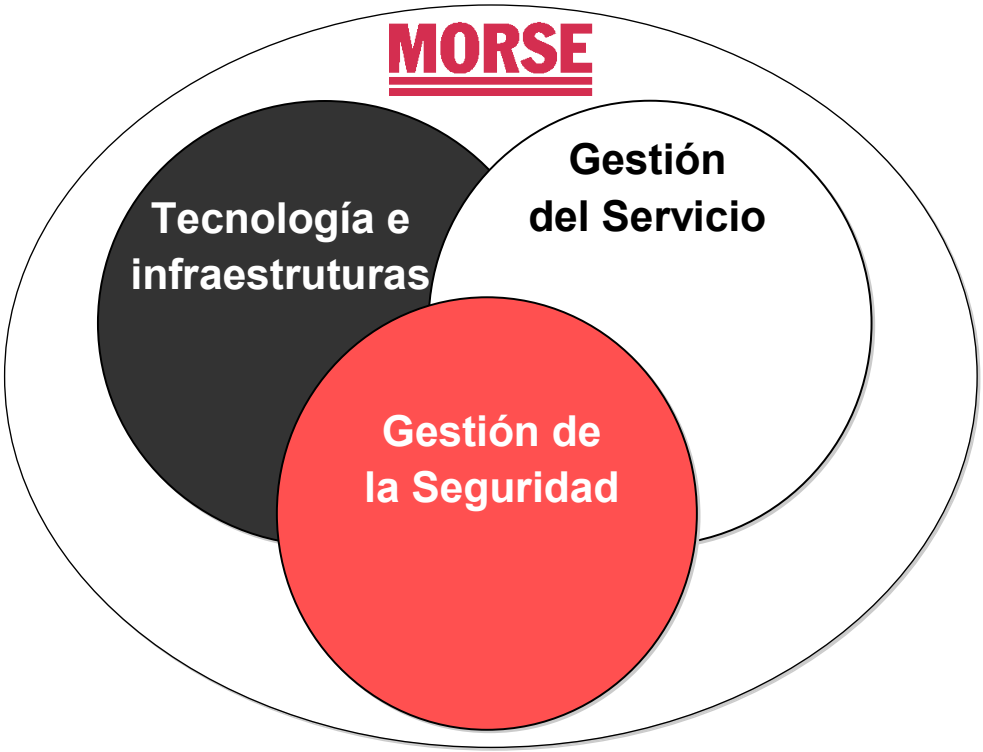
I'll take you there

Un paso atrás, perspectiva y visión global integrada:
El valor no evidente que aparece….

MORSE

MORSE en España integra los aspectos clave de la seguridad IT

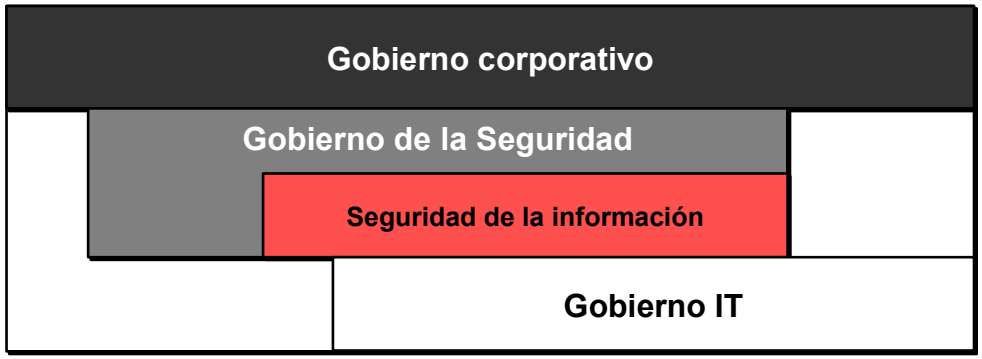
"Sólo una visión integral de la seguridad, del servicio y de la tecnología puede producir soluciones de seguridad adaptada al negocio"



I'll take you there

La gestión de la seguridad de la información es un componente del gobierno corporativo

- **El gobierno corporativo (governance) es el proceso que establece la dirección para asegurar el logro de dos objetivos:**
  - Uso eficiente de activos en el negocio actual
  - Disponibilidad de activos para nuevos negocios que maximicen el retorno
- **Aspectos clave de buen gobierno:**
  - Obtención de valor y gestión del riesgo
  - Asignación de responsables y medición de resultados
- **No existe un solo marco global aplicable, sino complementarios**



El buen gobierno está cambiando de un enfoque de mejores prácticas a un enfoque normativo y legal

La gestión del servicio respecto a la seguridad, es una vulnerabilidad

take you there

Objetivos

- **Preservar la seguridad de la información**
- **Garantizar la continuidad del negocio**
- **Proporcionar un entorno de confianza**
  - Seguridad de los procesos de negocio
  - Confianza de clientes, empleados y socios
  - Identificación de nuevas oportunidades de negocio
- **Cumplir el marco legal**

Retos

- **Gestionar y planificar recursos de seguridad en términos de rentabilidad y eficiencia**
- **Dar respuestas al negocio**
- **Cambiar visiones obsoletas**
  - La seguridad es un problema tecnológico
  - La seguridad es un problema de otro
  - La seguridad es un añadido en el diseño de sistemas y procesos

SYSTEM CERTIFICATION ISO 9001:2000 SGS

MORSE

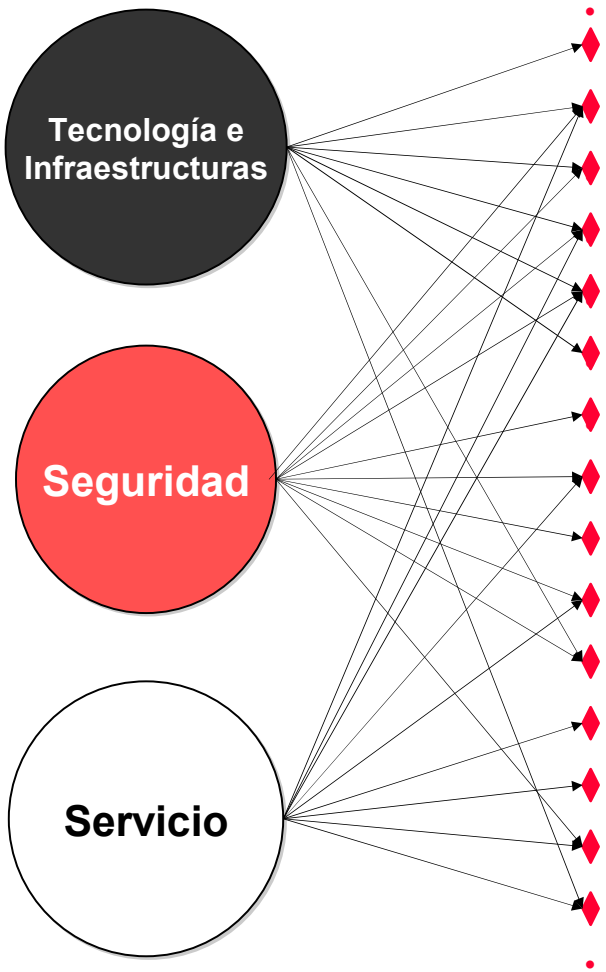
Mejor seguridad requiere integrar y desplegar los componentes de la plataforma de seguridad

Componentes
Gestión de la seguridad de la información (ISO 17799)
Gestión de Identidades y Control de Acceso
Protección y Contramedidas
Gestión de Incidentes y Recuperación
Infraestructura segura

Soluciones
• Evaluación, diagnóstico y auditoría de gestión
• Análisis y gestión de riesgos
• Planificación de la seguridad
• Implantación SGSI
• Asesoría y formación en seguridad y nuevas tecnologías
• Sistema de gestión de identidades
• Sistema de control de accesos
• Gestión de vulnerabilidades
• Anti-virus y Anti-spam
• Seguridad perimetral y cortafuegos de aplicaciones
• Sistemas de Detección de intrusiones
• Sistemas de Gestión de incidencias
• Sistemas de Gestión de políticas
• Continuidad y Sistemas BRS
• Disaster recovery
• Diseño de arquitecturas seguras
• Consolidación de servidores y almacenamiento
• Soluciones SBC
• Consolidación de soluciones de seguridad
• Auditorías técnicas (sistemas y red)

Es necesario un enfoque de mejora continua para desplegar tal variedad de componentes y soluciones

La visión coordinada genera entornos superiores desde el punto de vista de gestión

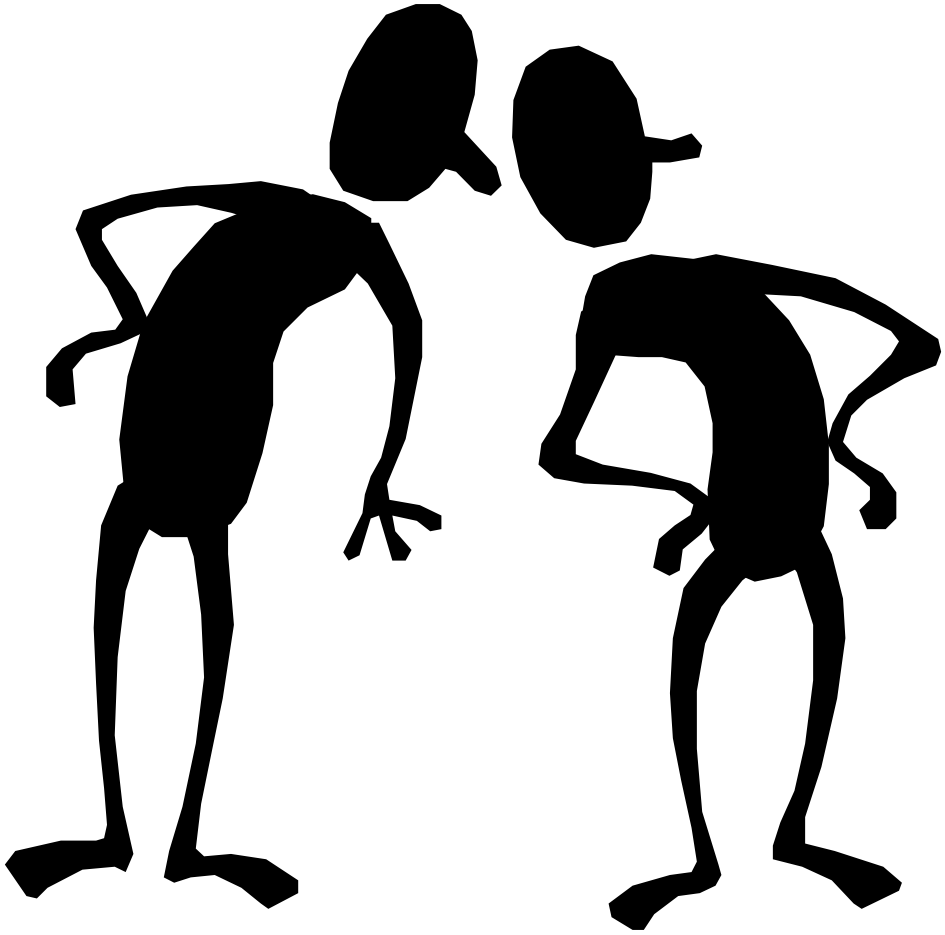


- Infraestructuras de almacenamiento, servidores y redes
- Consolidación de servidores y almacenamiento
- Soluciones Thin Client
- Gestión de datos
- Business Continuity
- Soluciones eBusiness
- Gestión de la seguridad de la información (ISO 17799)
- Gestión de Identidades y Control de Acceso
- Protección y Contramedidas
- Gestión de Incidentes y Recuperación
- Infraestructura segura
- Gestión del Servicio de TI (ITIL-BS 15000)
- Gestión de sistemas y redes
- Gestión de Incidentes y soporte del servicio
- Infraestructura Eficiente

I'll take you there

Muchas Gracias

Preguntas



I'll take you there

MORSE