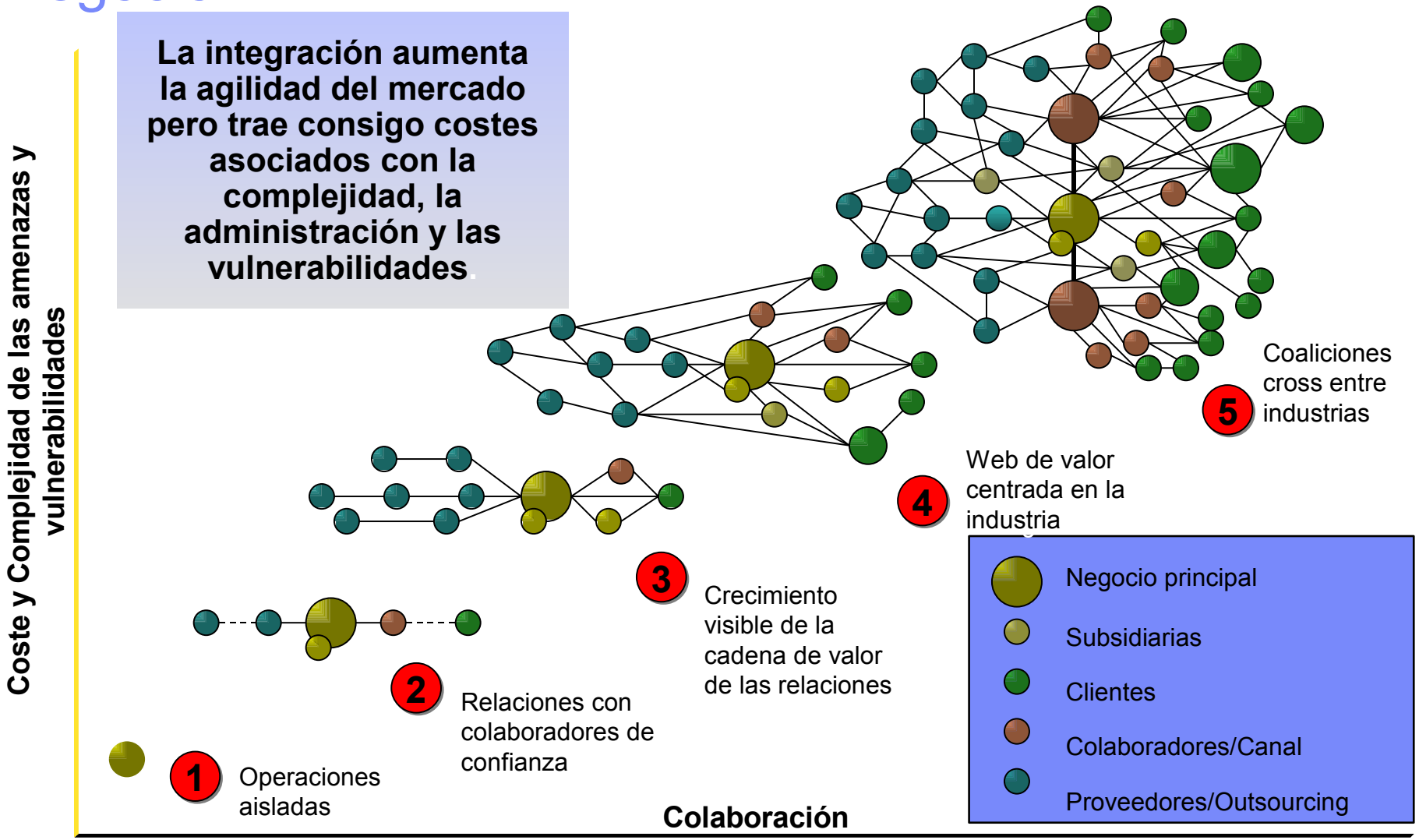
Hacia la madurez de la gestión de seguridad. Accesos, Identidades e Intrusismo

Rosa Escribano

El Ecosistema de Integración Incrementa los Retos de Negocio

La integración aumenta la agilidad del mercado pero trae consigo costes asociados con la complejidad, la administración y las vulnerabilidades.



Retos de la Seguridad TI

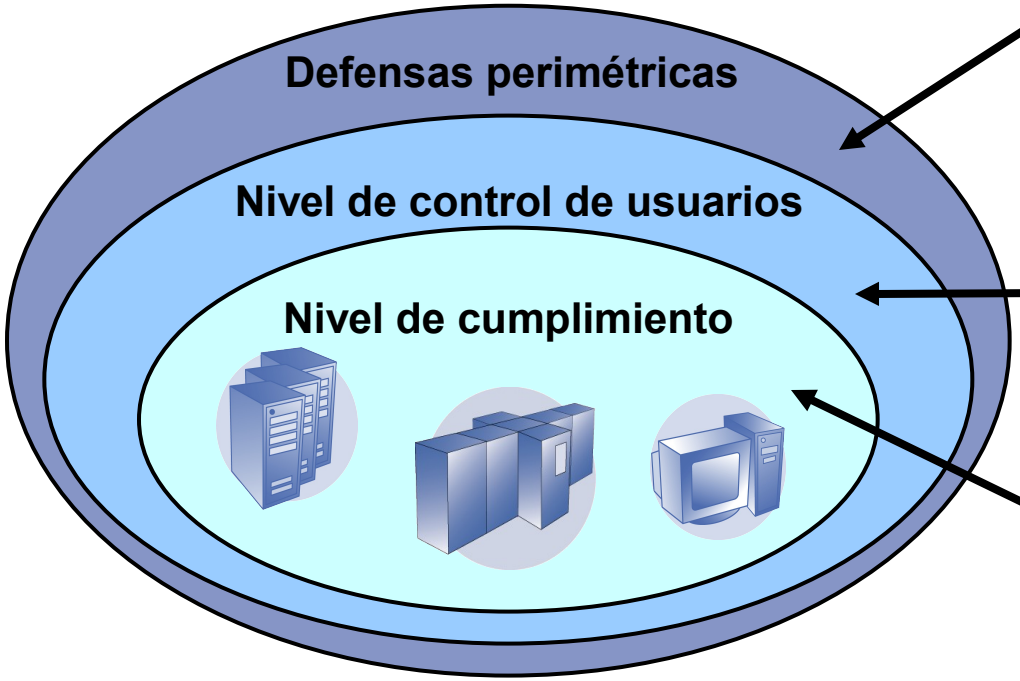
Mantener las innovaciones de Negocio y crecer de cara al riesgo

- Incremento de la complejidad de los eventos de seguridad en el entorno actual
- Elevados costes de Administración y Soporte
- Establecer relaciones de confianza con clientes, colaboradores y empleados
- Limitar y controlar los accesos a datos y activos sensibles o privados
- Datos de las identidades dispersos en múltiples repositorios
- Necesidad de proteger la información confidencial frente a incursiones de seguridad y riesgos
- Cumplimiento con las regulaciones y requerimientos de auditoría

Impacto de los problemas de seguridad sobre el negocio

Cuestiones de Seguridad	***Impacto***
▪ Dificiltad para proteger información sensible sobre empleados, clientes, colaboradores	▪ Deterioro de las relaciones entre empleados y colaboradores; pérdida de clientes; compromiso de la reputación; exposición ante requerimientos legales
▪ Los usuarios no pueden manejar tantas contraseñas. Constantes llamadas a los Centros de Asistencia de Usuarios por pérdidas de contraseñas	▪ Disminución de la productividad de los usuarios y de su satisfacción; altos costes de soporte
▪ Dificultades para cumplir con las regulaciones de seguridad y auditorias	▪ Exposiciones legales y financieras; sobrecarga para el personal encargado del cumplimiento
▪ Las brechas de seguridad afectan a los sitios Web; a los usuarios, a las redes… ▪ Hackers, empleados disgustados, gusanos/virus, denegaciones de servicio…	▪ Discontinuidad de los procesos de negocio ▪ Pérdidas en ventas, usuarios desocupados, reputación dañada
▪ Multiples inconsistencias, procesos de seguridad manuales ▪ Cada nueva aplicación requiere un nuevo proceso de seguridad y acceso.	▪ Falta de flexibilidad y rapidez en los negocios, lenta respuesta a los requerimientos del mercado ▪ Aumento del coste y complejidad del ciclo de desarrollo de aplicaciones

Las organizaciones necesitan algo más que defensas perimétricas



Defensas perimétricas
Previenen entradas no deseadas
- Firewalls
- Antivirus
- Detección de intrusismo, etc.

Nivel de control de usuarios
- Qué usuarios acceden
- Qué pueden ver y hacer
- Soporte de sus preferencias
- Protección de su privacidad

Nivel de cumplimiento
- Cumplir con regulaciones
- Generación de informes
- Riesgos / vulnerabilidades
- Respuesta ante eventos

¿Donde nos centramos?

Mientras la seguridad tradicional mantiene a los intrusos fuera…

- **Firewalls, VPN, Anti-Virus, Detección de Intrusión**

… IBM se centra en controlar a las personas invitadas a entrar

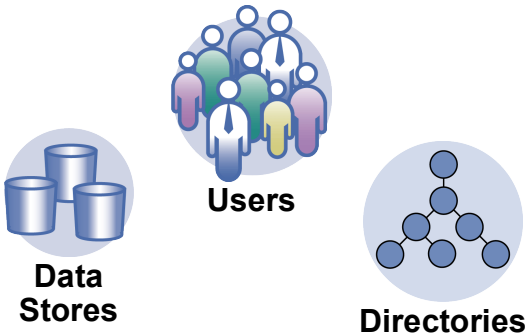
La identidad es la base del nivel de control

Actualmente, los datos de identidad estan fragmentados e incompletos
Pero, los datos de identidad son claves para:

- **Decisiones de acceso**
- **Autoservicio**
- **Asignación de autorizaciones**
- **Personalizacion**

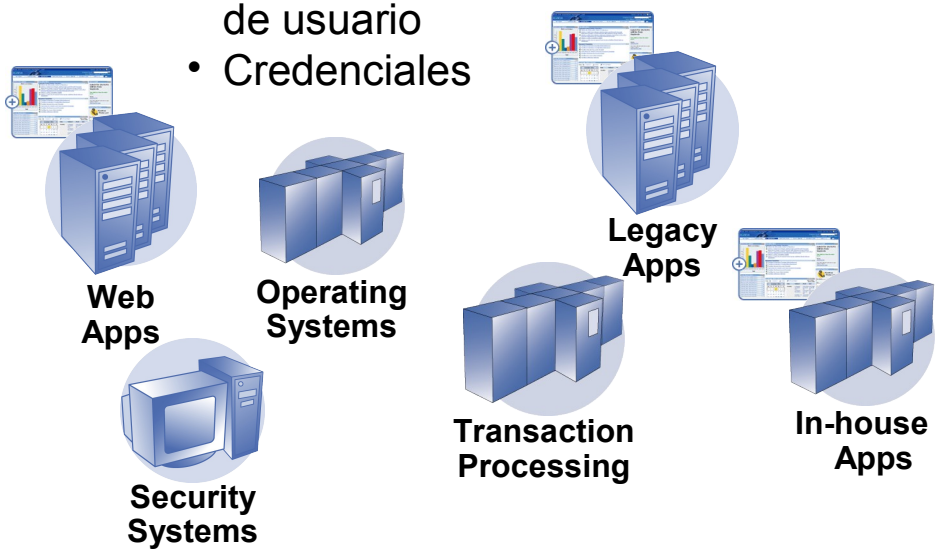
Informacion sobre las personas

- Empleados
- Colaboradores
- Subcontratados
- Clientes

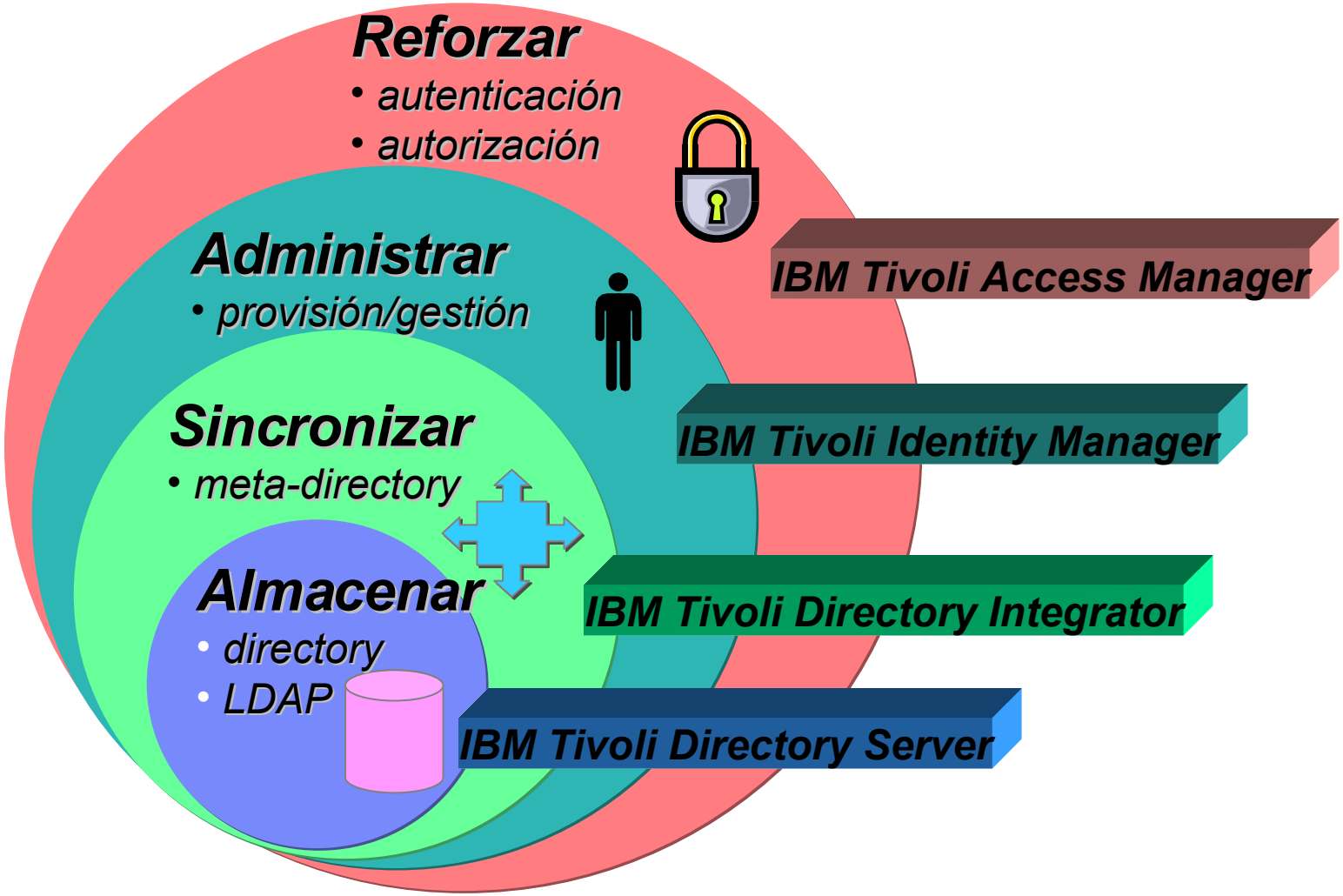


Informacion sobre los accesos

- Privilegios de las cuentas de usuario
- Credenciales

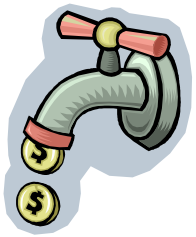


El Ecosistema de la Gestión de Identidades



Los retos de la Gestión de Identidades

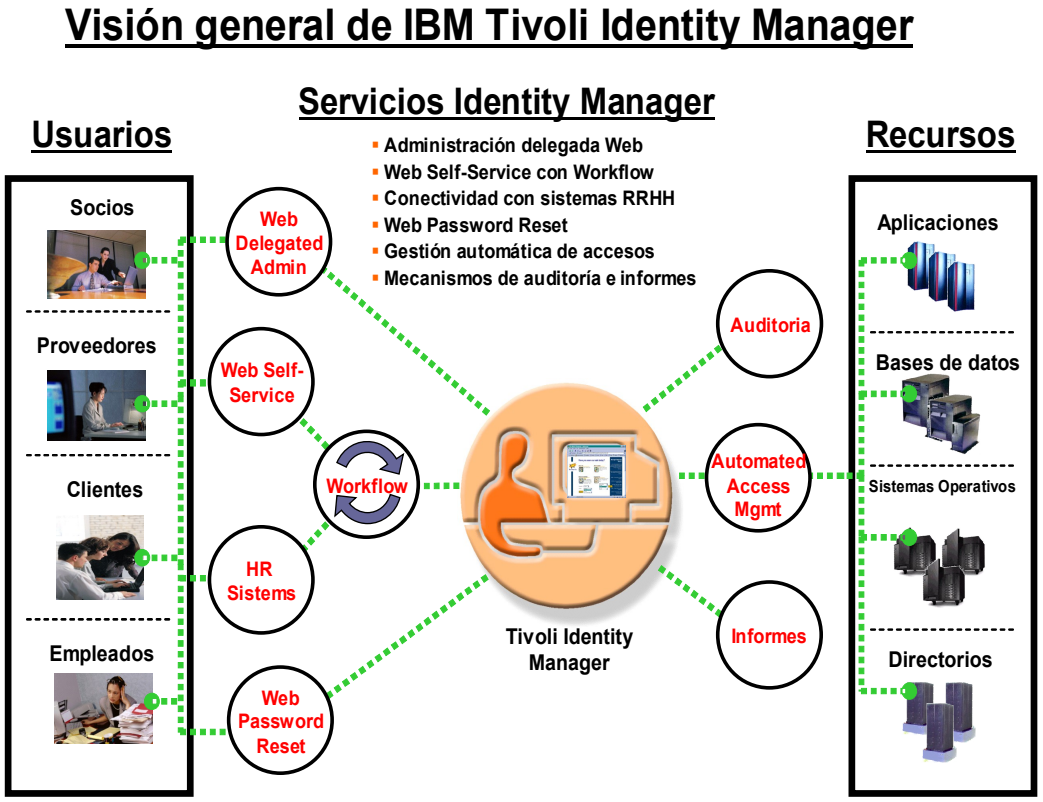
- ¿Cuanto tiempo se pierde con los cambios rutinarios de contraseñas?
  - ✓ **Trés o cuatro veces al año, por usuario y con un coste estimado de 24€ por llamada**
- ¿Cuanto tiempo tarda un nuevo empleado/subcontratado en ser productivo?
  - ✓ **Hasta 12 dias por usuario hasta tener disponibles todas las cuentas y accesos que necesita**
- ¿Cuantos antiguos empleados/subcontratados tienen todavía acceso a datos sensibles?
  - ✓ **Del 30% al 60% de las cuentas son huerfanas (riesgo potencial de seguridad)**
- ¿Estamos seguros de que sólo las personas adecuadas acceden a los datos de clientes?
  - ✓ **El 70% de los casos de fraude relacionados con datos de clientes se deben a ataques internos**
- ¿Cuanto tiempo lleva recopilar todos los informes necesarios para una auditoría?
  - ✓ **Puede llevar semanas y algunas compañías tienen personal a tiempo total dedicado a ello**



Sources: Gartner Group, Meta Group and IBM

Tivoli Identity Manager

- Aprovisionamiento
- Control de Acceso basado en Roles
- Workflow
- Autoservicio
- Consolidación de repositorios
- Integración de datos
- Meta-directorio
- Informes preconfigurados
- Gestión completa del ciclo de vida de una identidad

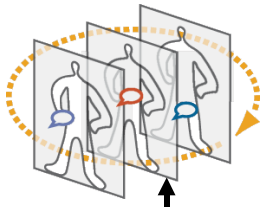


Tivoli Identity Manager - Aprovisionamiento

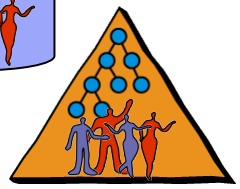
Cambio en personal(add/del/mod) → Evaluación de políticas → Circuito de aprobación → Actualización cuentas

Detecta y corrige privilegios establecidos localmente

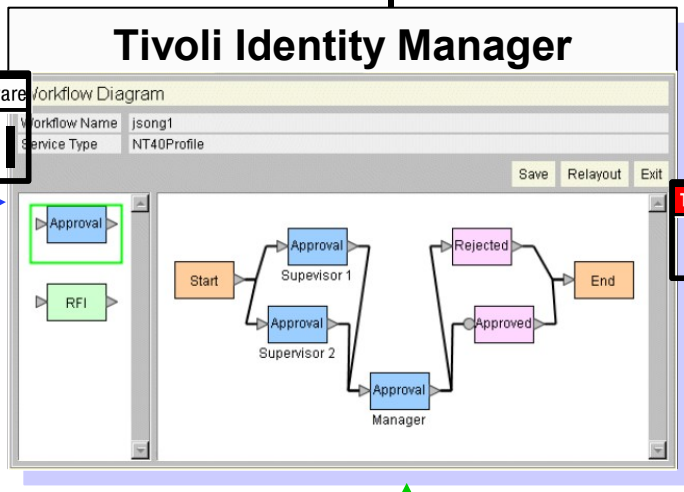
Aprovisionamiento basado en Politicas para toda la infrastructura IT



Gestión de cuentas en 70 tipos distintos de sistemas, aplicaciones de negocio, portales, etc



Sistemas RH/ Repositorios de información de Personas



Tivoli Identity Manager Express: rápido retorno de inversión para clientes SMB

1

Fácil de instalar

Instalación fácil y rápida a través de un launchpad

2

Fácil de desplegar

Configuración remota del adaptador; grupos de adaptadores y wizards que facilitan el despliegue

3

Fácil de manejar

Interfaz de usuario intuitiva, administración simple e informes listos para usar. Gestión del dia a dia consistente

Tivoli Federated Identity Management

Escenario Típico

Muchas empresas o multiples negocios dentro de la misma empresa

Reto: Compartir información de usuario a través de transacciones de confianza entre colaboradores

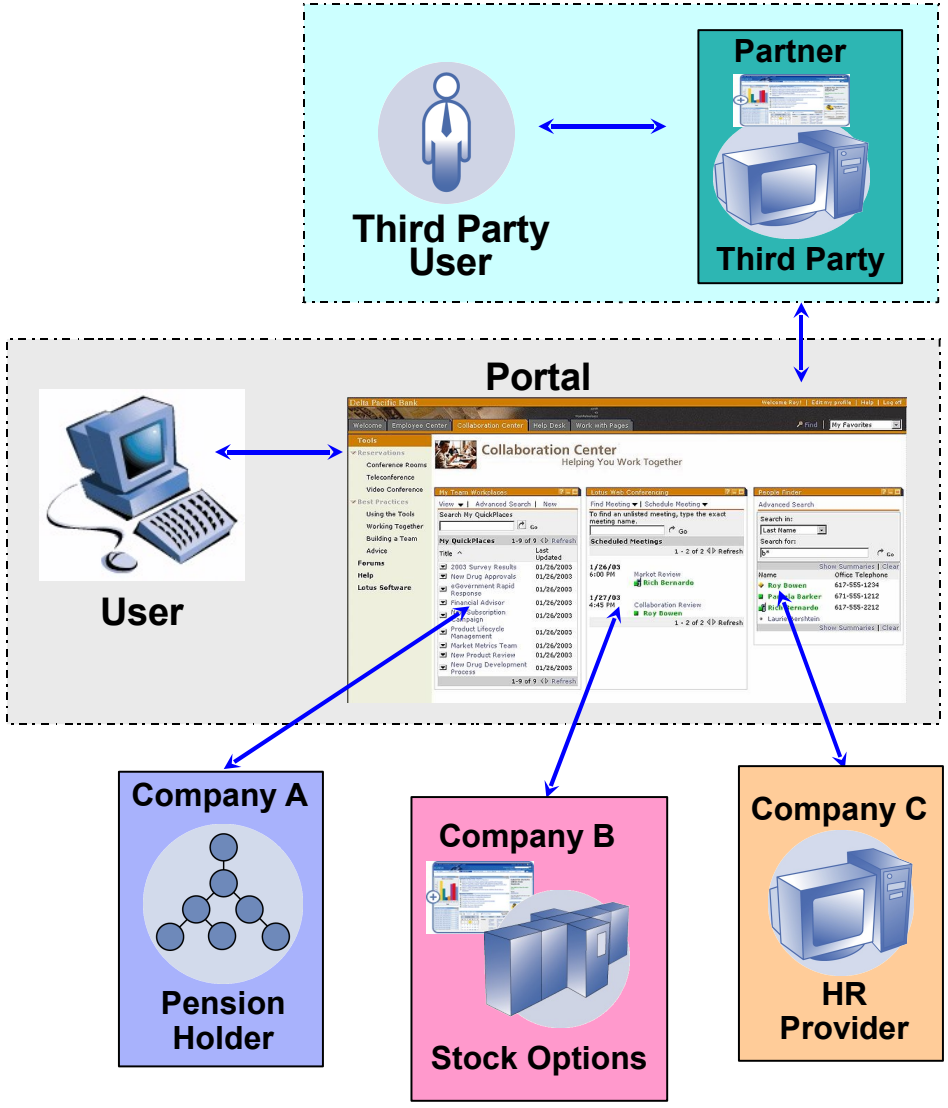
Propuesta de Valor

Disminuir los costes de las gestión de usuarios y help-desk

Mejorar la experiencia del usuario

- Registro de usuarios racional
- Single Sign-On Federado

Permitir el intercambio de negocio seguro y de confianza

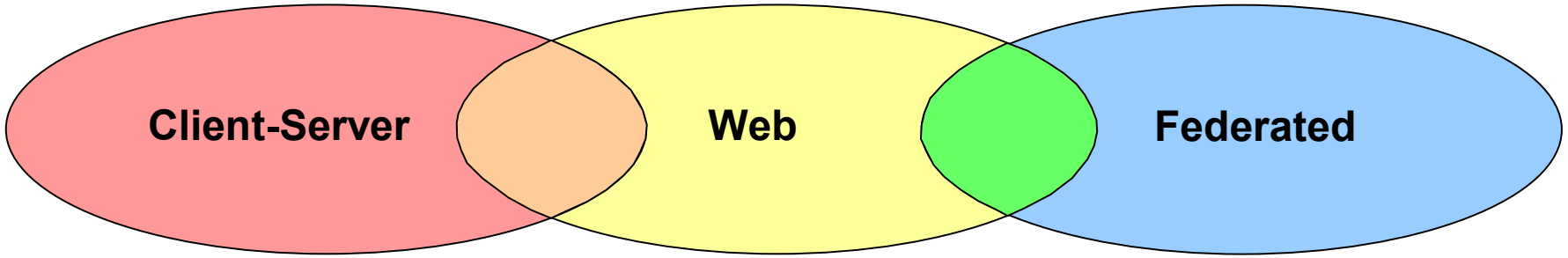


Tivoli Access Manager for Enterprise Single Sign-On

- **IBM Tivoli Access Manager for Enterprise Single Sign-on** es el core de la solución de Single Sign-on.
- IBM Tivoli Access Manager for E-SSO: **Desktop Password Reset Adapter** permite al usuario final hacer por sí mismo el reset de su contraseña de windows, sin necesidad de llamar al help desk, directamente desde su estación de trabajo.
- IBM Tivoli Access Manager for E-SSO: **Authentication Adapter** permite a las organizaciones utilizar cualquier combinación de tokens, smart cards, métodos biométricos y contraseñas para controlar el acceso a sus aplicaciones.
- IBM Tivoli Access Manager for E-SSO: **Provisioning Adapter** permite a los administradores de sistemas distribuir directamente los credenciales de usuario (identificador de usuario y contraseña) a TAM for ESSO.
- IBM Tivoli Access Manager for E-SSO: **Kiosk Adapter** permite terminar de forma automática sesiones inactivas y hacer shutdown de las aplicaciones para los usuarios de puestos compartidos o kioskos.

TAMES: Elemento clave de Single Sign-on completo

¡ La solución Tivoli de Gestión de Identidades ofrece cobertura total !

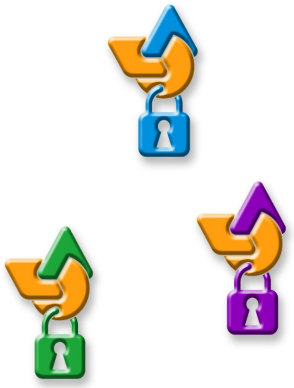


Tivoli Federated Identity Manager

Tivoli Access Manager for e-business

Tivoli Access Mgr. for E-SSO

Control de Accesos



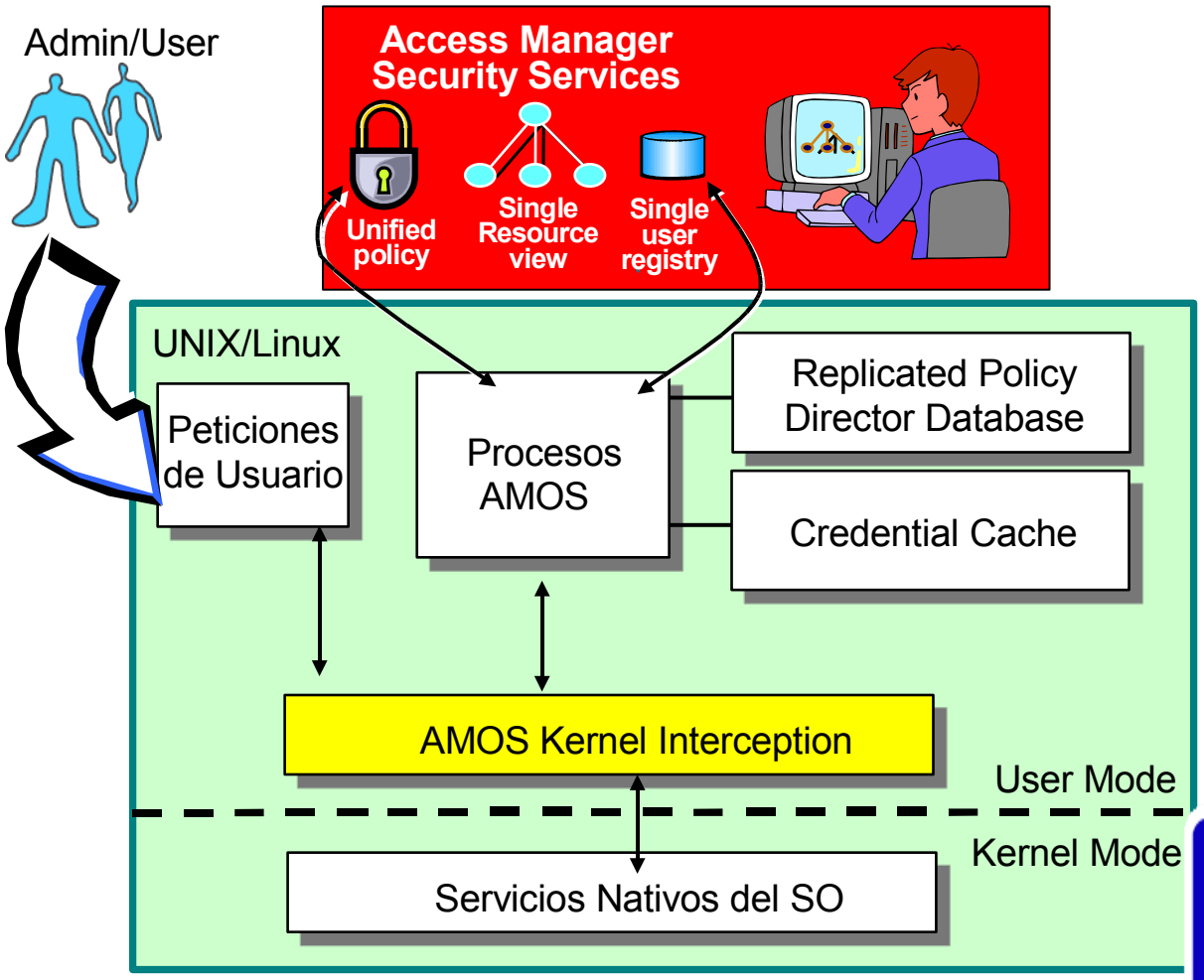
Hasta ahora

- Seguridad codificada en cada aplicación
- ¿Modificación de las políticas de acceso? Múltiples lugares
- Autenticación en cada aplicación

Tivoli Access Manager for ebusiness

- Servicios de seguridad comunes, aislados de cada aplicación
- Administración centralizada y delegada
- Granularidad en la definición de políticas de acceso
- Web Single sign-on

Tivoli Access Manager for Operating Systems



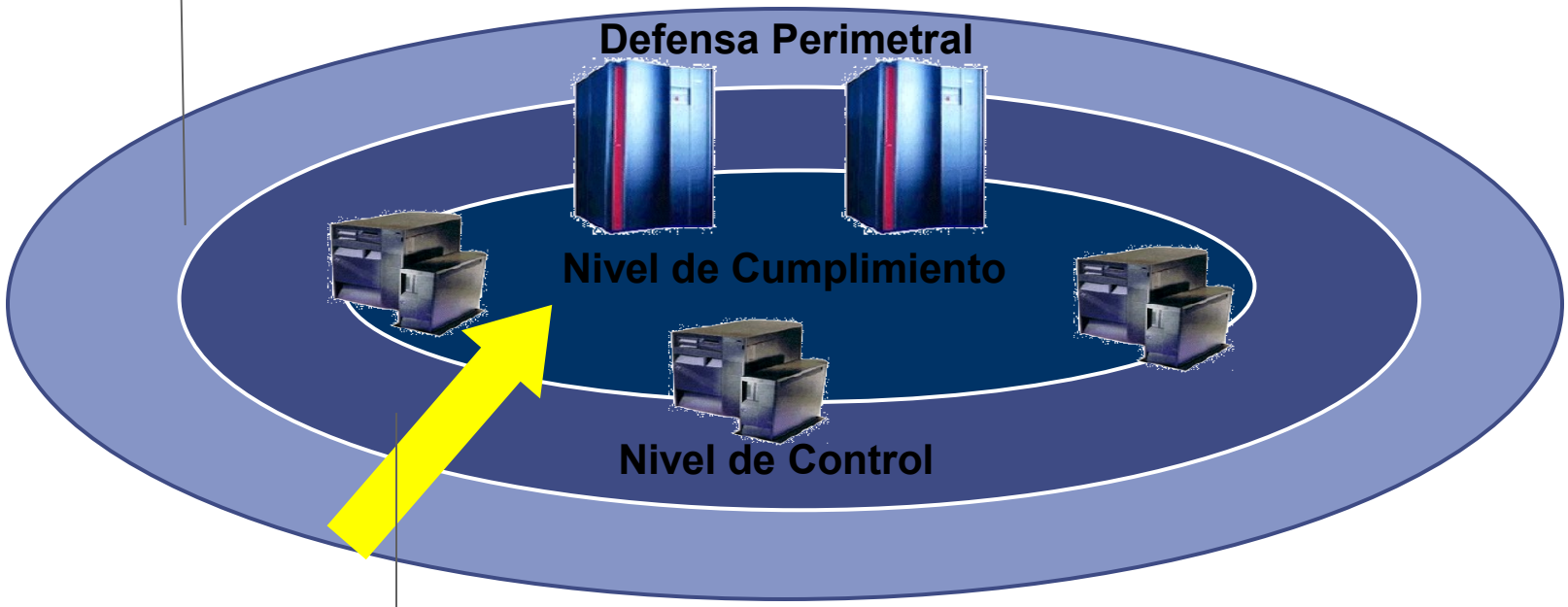
- **Protege:**
  - Recursos de lo Sistemas de Archivos
  - Servicios remotos de Red
  - Servicios Locales de Red
  - Servicios de Login – Cuando y desde Donde
  - Cambios de usuario y grupo
  - Y más

Clave: Control más granular sobre los accesos de root y resto de los usuarios

¿Donde nos centramos?

Mientras la seguridad tradicional mantiene a los intrusos fuera…

- **Firewalls, VPN, Anti-Virus, Detección de Intrusión**



… IBM se centra en controlar a las personas invitadas a entrar

…Y asegurando que se hace de forma segura

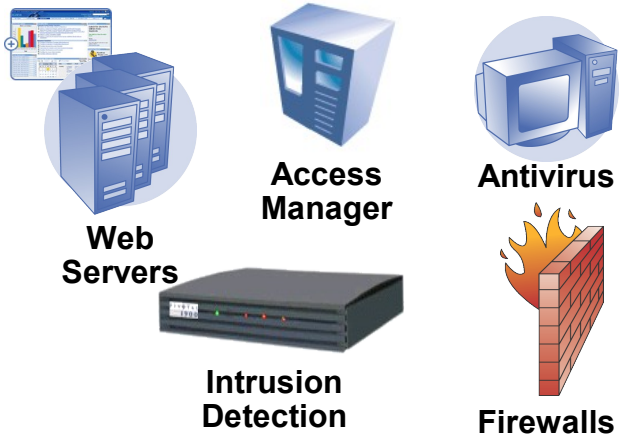
La información: clave del nivel de Cumplimiento

Evaluar los datos es dificil y consume mucho tiempo
Pero, la evaluación de datos de seguridad es la base para:

- **Mejorar la seguridad TI**
- **Mitigar el riesgo**
- **Auditoría y cumplimiento**

Información sobre las defensas perimetrales y el nivel de control

- Consolidar
- Correlacionar
- Mitigar



Informacion sobre los sistemas

- Identificar las vulnerabilidades de seguridad TI
- Cumplir las auditorias y regulaciones

¿Cómo y por qué surgen las vulnerabilidades de seguridad?

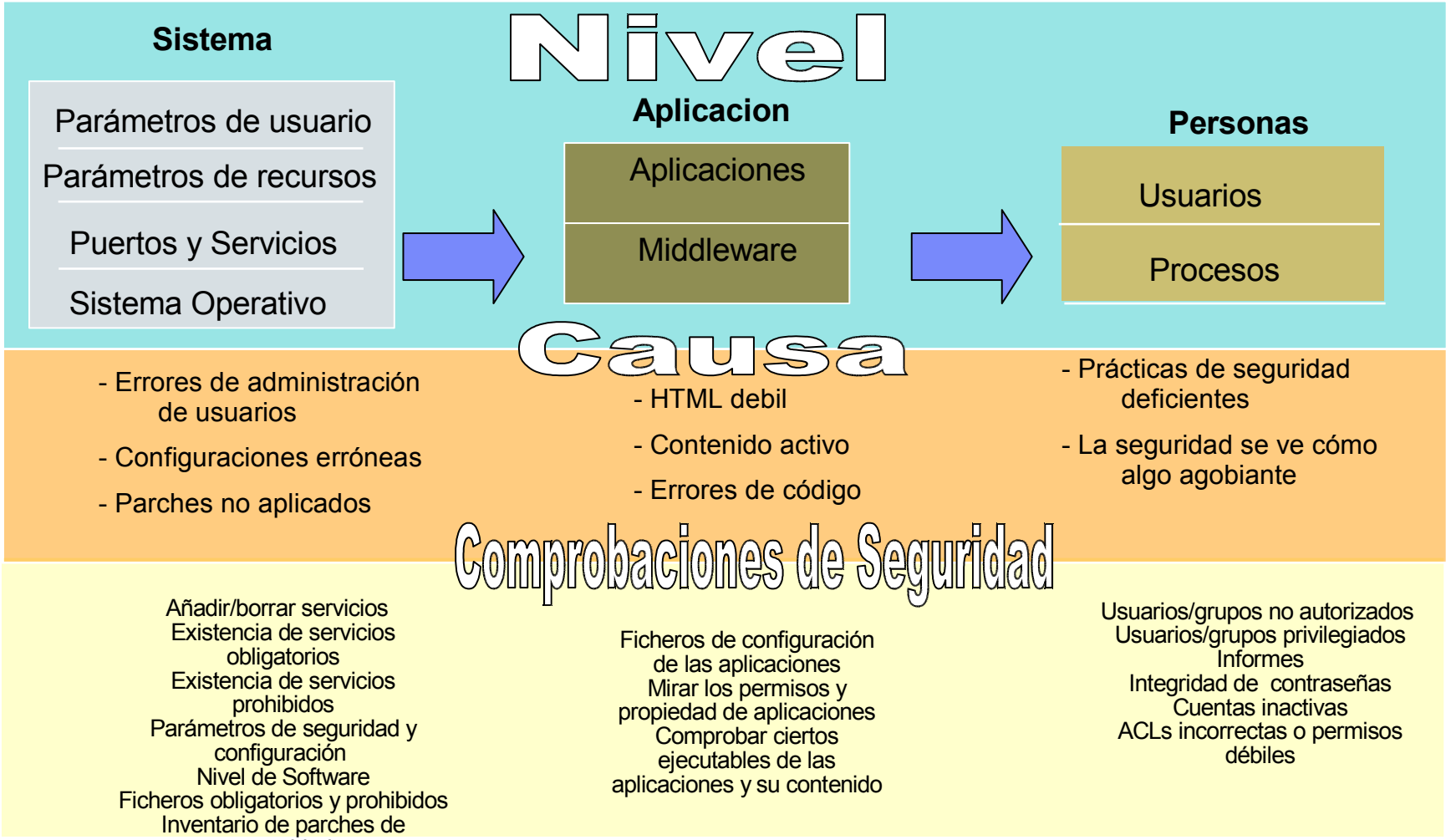
- "A lo largo del 2005, el 90% de los cyber ataques continarán aprovechandose de los defectos conocidos de seguridad para los que ya existe un parche o para los que ya se conoce una medida preventiva" – Mark Nicolett, Research VP at Gartner
- Y los ataques van en aumento

Year	2000	2001	2002	2003 Q1-3
Incidents	21,756	52,658	82,094	114,855

From CERT/Coordination Center Incident Reports, 2000-2003:

- ¿Cual es la causa de la explosión de vulnerabilidades?
  - Defectos de Software
  - Falta de controles técnicos de seguridad
- ¿Por qué es tan dificil que proliferen las buenas prácticas de seguridad?
  - Entrega a los usuarios de sistemas sin configurar
  - Los usuarios no saben cómo configurar sus sistemas de manera efectiva
  - Los administradores tienen miedo de interrumpir la operación de los sistemas al instalar un parche o configurar un parámetro de seguridad

Tivoli Security Compliance Manager – Información sobre los sistemas TI



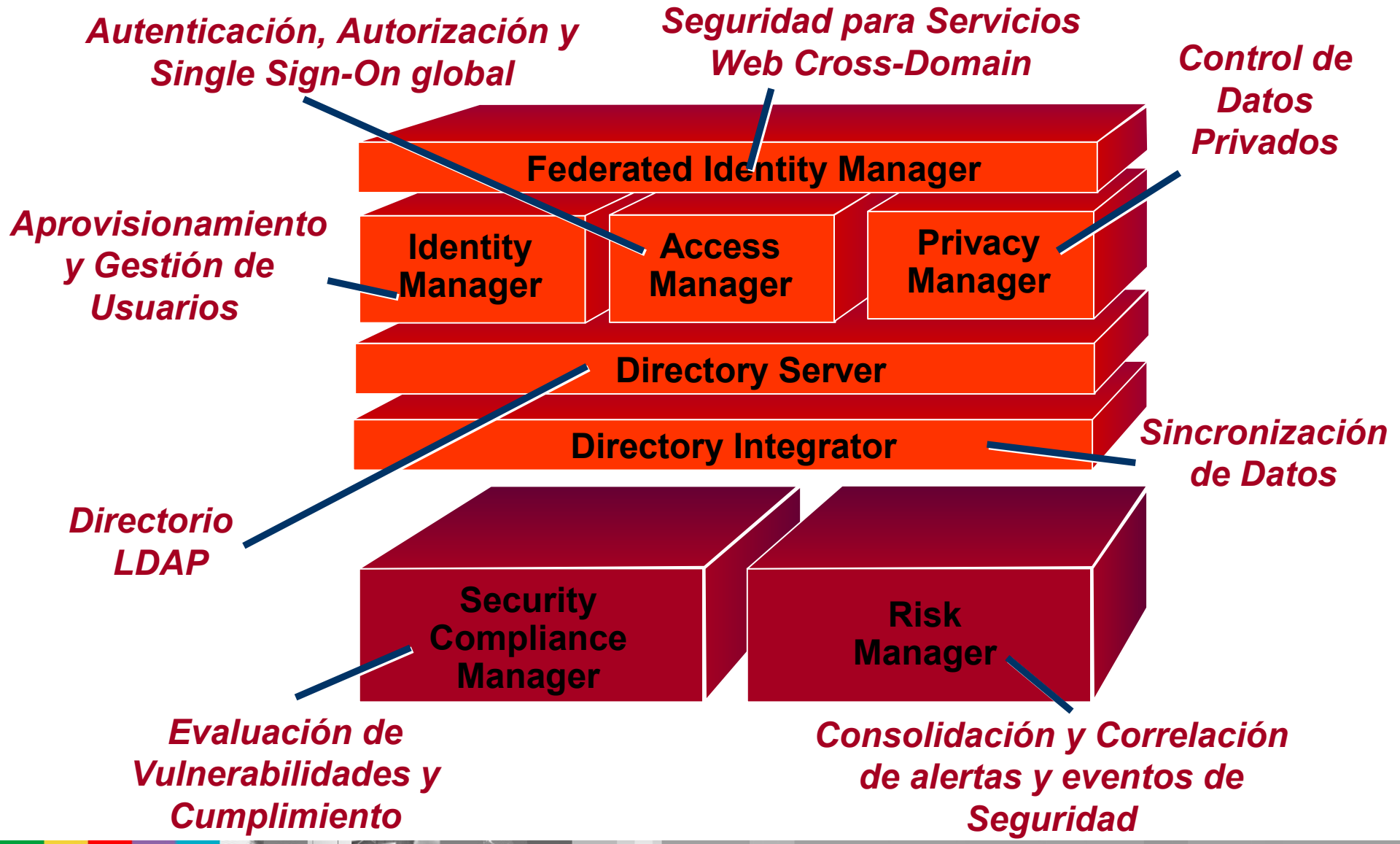
Tivoli Security Compliance Manager (TSCM)

- IBM Tivoli Security Compliance Manager es un producto de cumplimiento de políticas de seguridad que comprueba el sistema y las aplicaciones en busqueda de vulnerabilidades e identifica violaciones contra las políticas de seguridad.

Los principales beneficios para nuestros clientes:

- Ayuda a asegurar los datos corporativos y su integridad
- Identifica vulnerabilidades de seguridad del software
- Disminuye los costes TI mediante la automatización y centralización
- Colabora en el cumplimiento de regulaciones y estándares

Gestión de Identidades, Riesgos y Cumplimiento




धन्यवाद
Hindi
多謝
Traditional Chinese
ขอบคุณ
Thai
Спасибо
Russian
Gracias
Spanish
Thank You
English
شكراً
Arabic
Obrigado
Brazilian Portuguese
多谢
Simplified Chinese
Danke
German
Grazie
Italian
Merci
French
நன்றி
Tamil
ありがとうございました
Japanese
감사합니다
Korean