Reduciendo Gastos y Aumentando la efectividad con Soluciones de Seguridad

Vicente Gozalbo Moragrega
IBM Tivoli Security Leader Spain

IBM Software

PCTY2010

Pulse Comes to You

Optimizing the World's Infrastructure
[**27/05/2010** Lisboa]

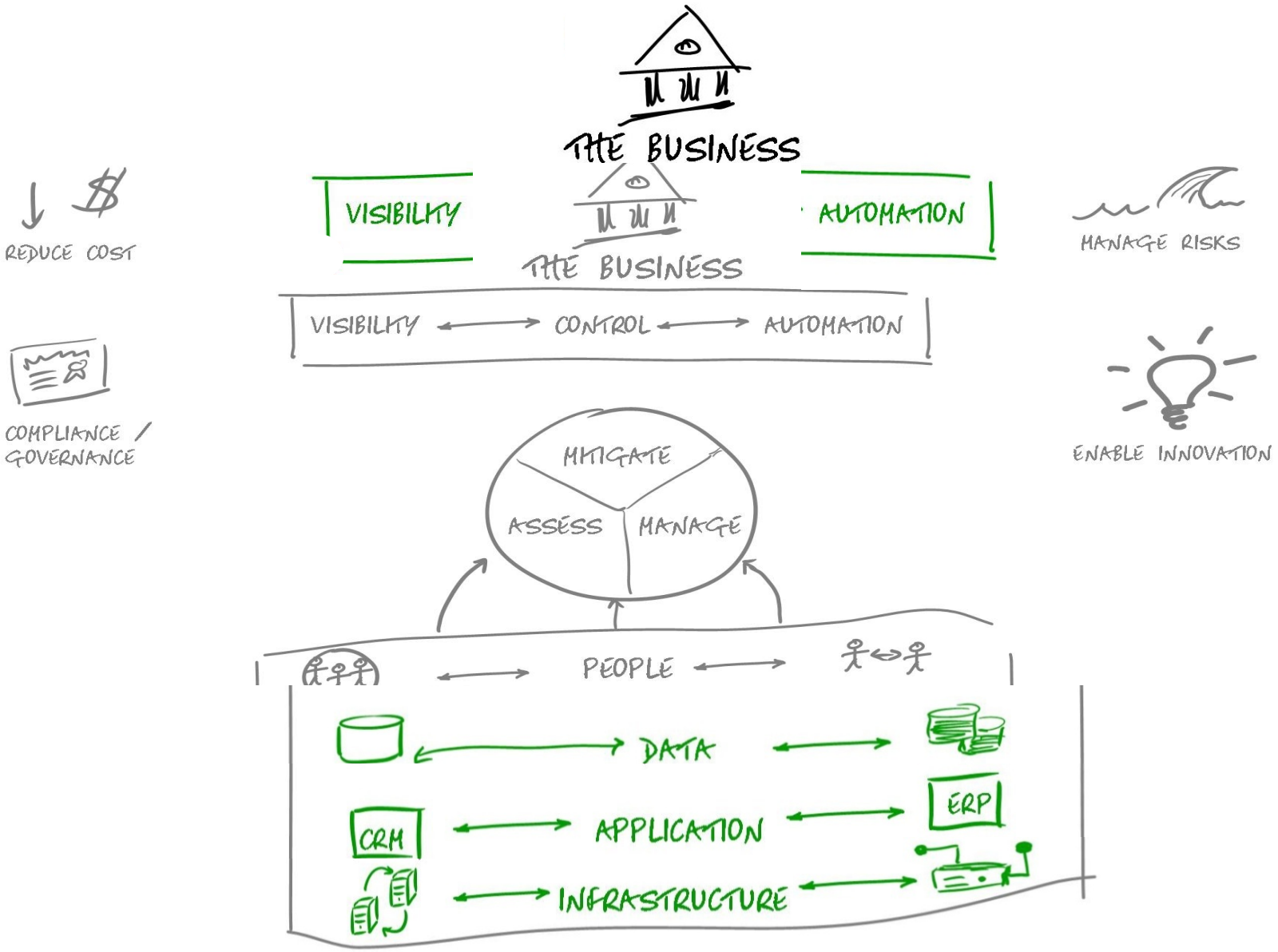
Introduction

IBM Software

PCTY2010

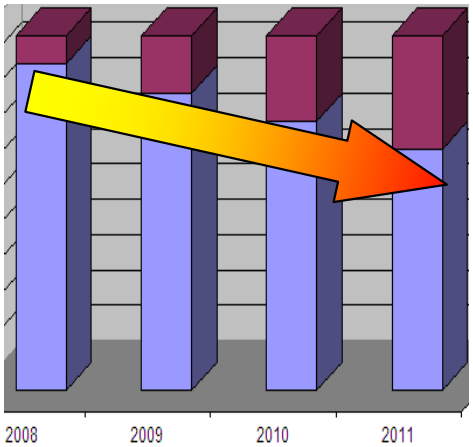
Pulse Comes to You

Reducing costs, Managing Risks, Having Innovation, enhancing Compliance



Retos de Negocio: Necesito Disminuir mis Costes y Aumentar la Eficiencia… mejorando la Seguridad

Debo disminuir los costes asociados a la infraestructura y gestión de la seguridad IT (TCO).



- Mantener seguros los activos tecnológicos e información me supone **un 10% del presupuesto** IT y va creciendo año a año.
- Esos gastos **restan presupuesto** a otras inversiones de más valor para la compañía

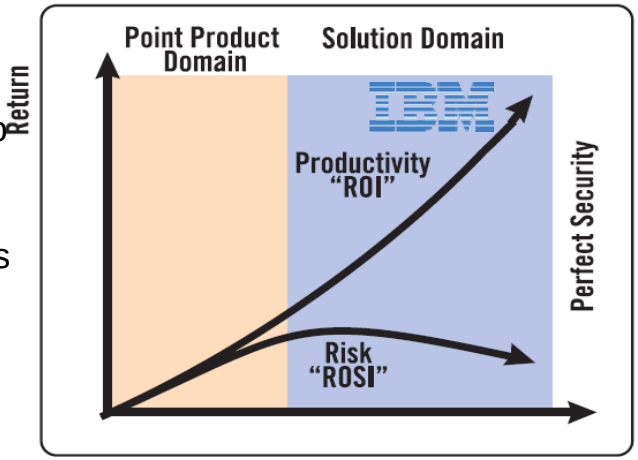
Hay que aumentar la eficiencia de los empleados, redes y sistemas.

▪**Las incidencias de seguridad** como ataques, contraseñas olvidades, robo de información confidencial, generan indisponibilidad de sistemas, bajo rendimiento de redes, ineficiencia de los empleados y sanciones que **impactan en la cuenta de resultados** mi organización.

Debo obtener un ROI, TAMBIÉN, de las Inversiones de Seguridad

- Dada la **frenética evolución** da las tecnologías de seguridad, tenemos gran diversidad de **soluciones de nicho** que suponen un gasto descontrolado y que **pierden efectividad** con el tiempo y **multiplica su TCO.**

•La carencia de una gestión de la seguridad del usuario nos supone **el 70% de los gastos de HelpDesk** y dobla los de administración de seguridad.



•**La seguridad** en mi organización constituye un **obstáculo** para cualquier nuevo negocio

Y además, siempre necesito mejorar la seguridad.

- **Los ataques actuales** allanan mis infraestructuras y provocan **indisponibilidades**, falta de rendimiento e incidentes contínuos de seguridad.
- Los **Antivirus y Firewalls han perdido efectividad** por sí solos (El 60% de los desktops a nivel mundial se consideran infectadas por malware).
- **Aplicar parches es un caos: El 70%** de los sistemas **no están parcheados** al último nivel de seguridad y **el 40% nunca tienen el parche** disponible a tiempo.
- **No tengo solución** de protección para el **nuevo entorno virtualizado.**

Reducing Costs with IPS technology

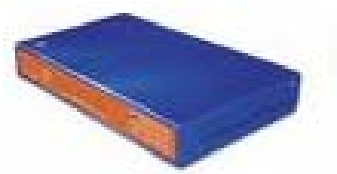
IBM Software

PCTY2010

Pulse Comes to You

Renovación Tecnológica de la seguridad perimetral

Sistemas de protección obsoletos e ineficaces



Appliances de Protección de intrusiones Proventia GX

- **Elimina el** tráfico malicioso, ataques conocidos o desconocidos
- Protege **proactivamente** sistemas que no disponen o no pueden disponer de parche de seguridad, **ayudando a planificar** mejor las operaciones.
- **Aumenta la disponibilidad y el rendimiento (hasta 70%)** de los sistemas y las redes (hasta un 90%), permitiendo **diferir nuevas inversiones** en actualización de electrónica de red.
- **Única solución** disponible en el mercado para **protección de entornos virtuales.**

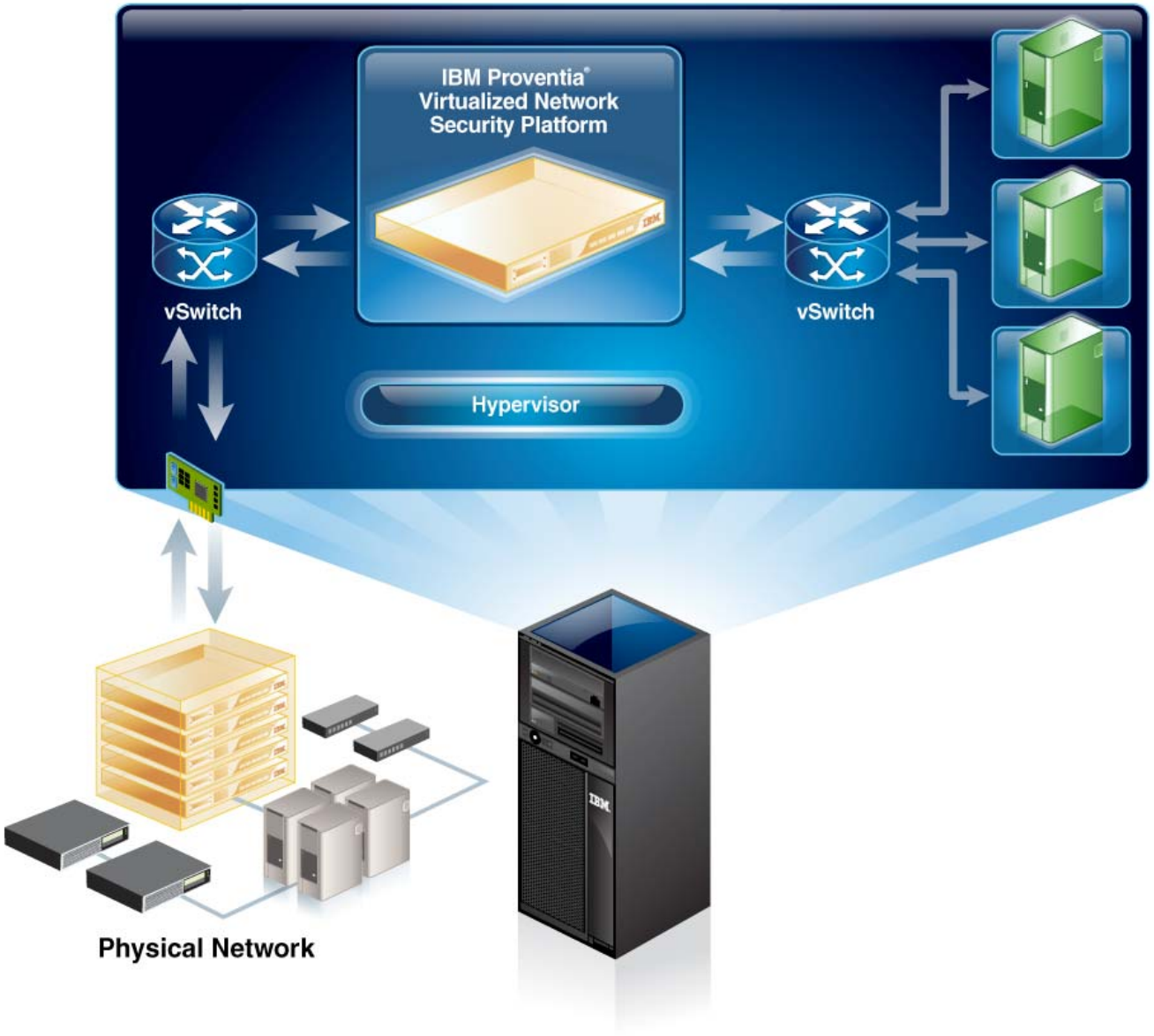
Sistemas multifunción

Serie MX

Multitud de dispositivos de seguridad

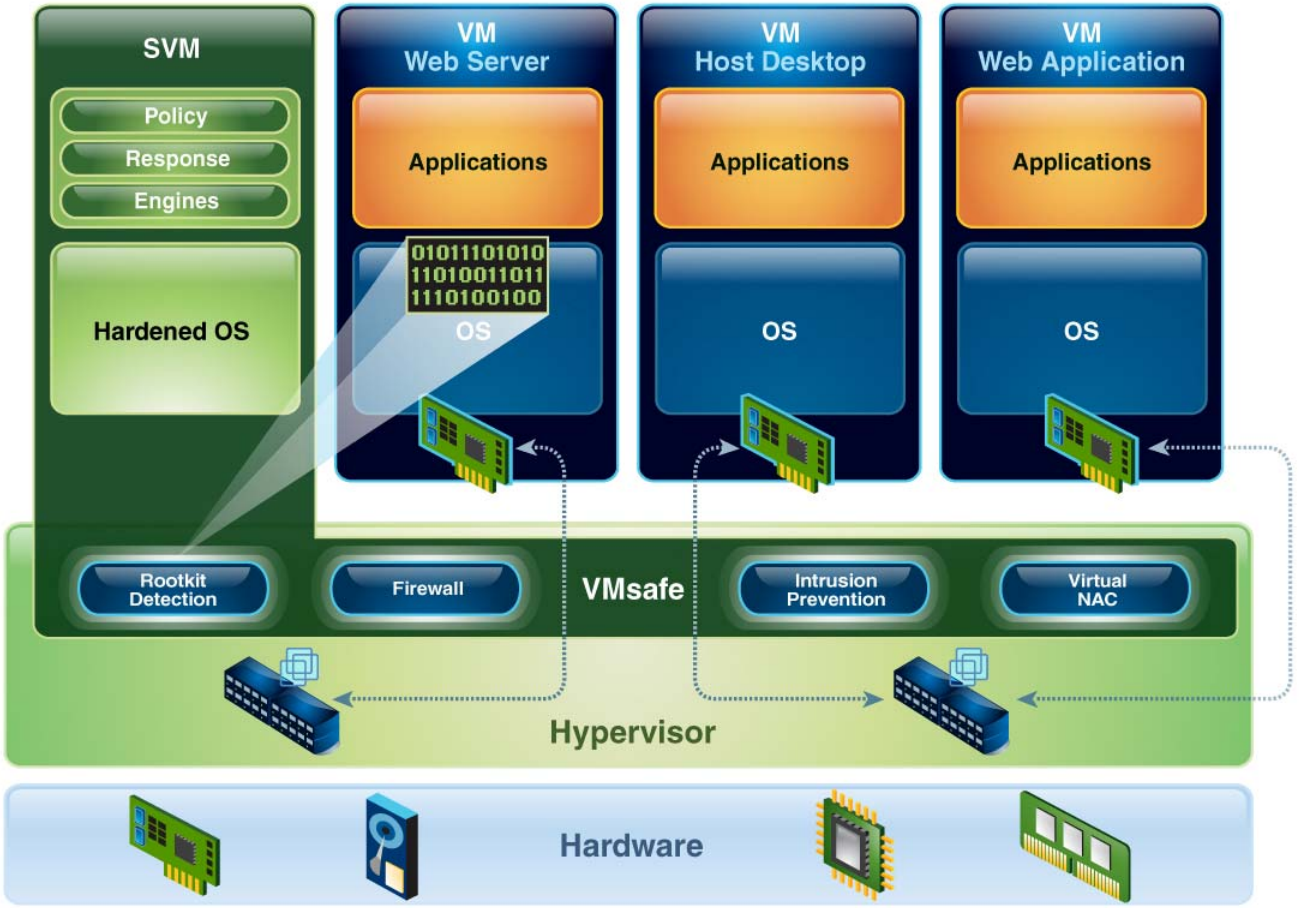
- **Consolida 6 distintos dispositivos** tradicionales de seguridad: Firewall, IPS, Antivirus, AntiSpam, control de la navegación, VPN,
  - **Agrupa costes** de licencias y mantenimientos
  - **Optimiza** las tareas de **gestión**
  - **Disminuye** necesidad de **ancho de banda**
  - **Menor consumo** energético.
  - **Aumenta la eficiencia** de los usuarios.

Virtual appliance protege segmentos de red virtuales

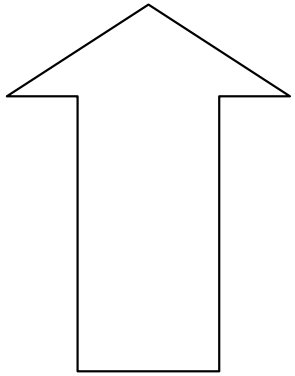


Virtual Server Protection para VMware

- Protección dinámica para todas las capas
  - Hypervisor
  - SO
  - Red
  - Aplicaciones
  - Máquinas virtuales(VM)
  - Trafico interno



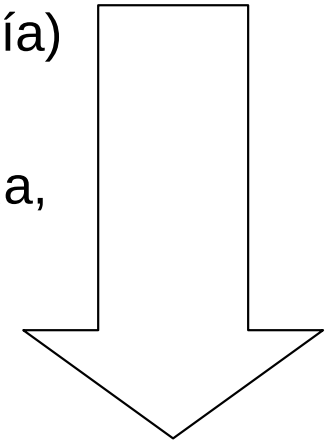
Más efectividad y seguridad, Menores Costes



- **Protección Más eficaz**
  1. Cercana al 100%
  2. Proactiva
  3. Todo el espectro tecnológico
  4. Certificada por el sector

Reducción de costes

1. Consolidación (políticas y tecnología)
2. Mayor disponibilidad
3. Menor consumo de ancho de banda, mayor rendimiento.
4. Solución virtualizada
5. Planificación en la aplicación de parches



Reducing Costs and Securing identities with SSO and Identity Management

IBM Software

PCTY2010

Pulse Comes to You

Por qué Aumentar la Eficiencia

- En términos contables, cuando los beneficios son escasos, un ligero aumento de la eficiencia supone un gran aumento de los beneficios

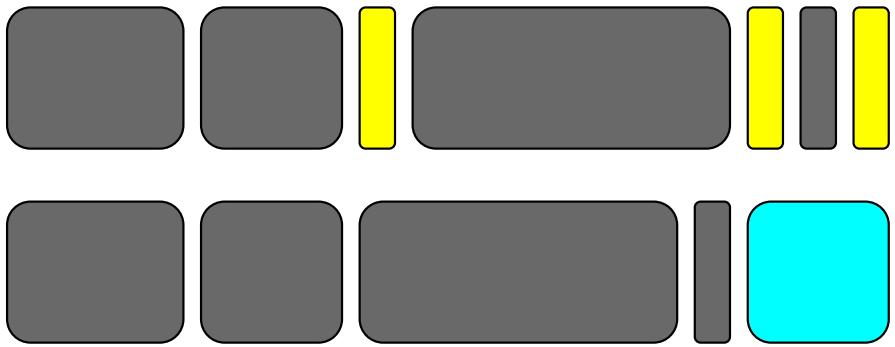
Aumento de la eficiencia	5%

Situación Previa	
Numero empleados	5000
Ingresos	350.000.000,00 €
Gastos	300.000.000,00 €
Beneficio	50.000.000,00 €

Despúes de la mejora de la Eficiencia	
Numero empleados	5000
Ingresos	367.500.000,00 €
Gastos	300.000.000,00 €
Beneficio	67.500.000,00 €

Aumento del beneficio	35%

Cómo se Aumenta la Eficiencia: Mejorando procesos con Innovación



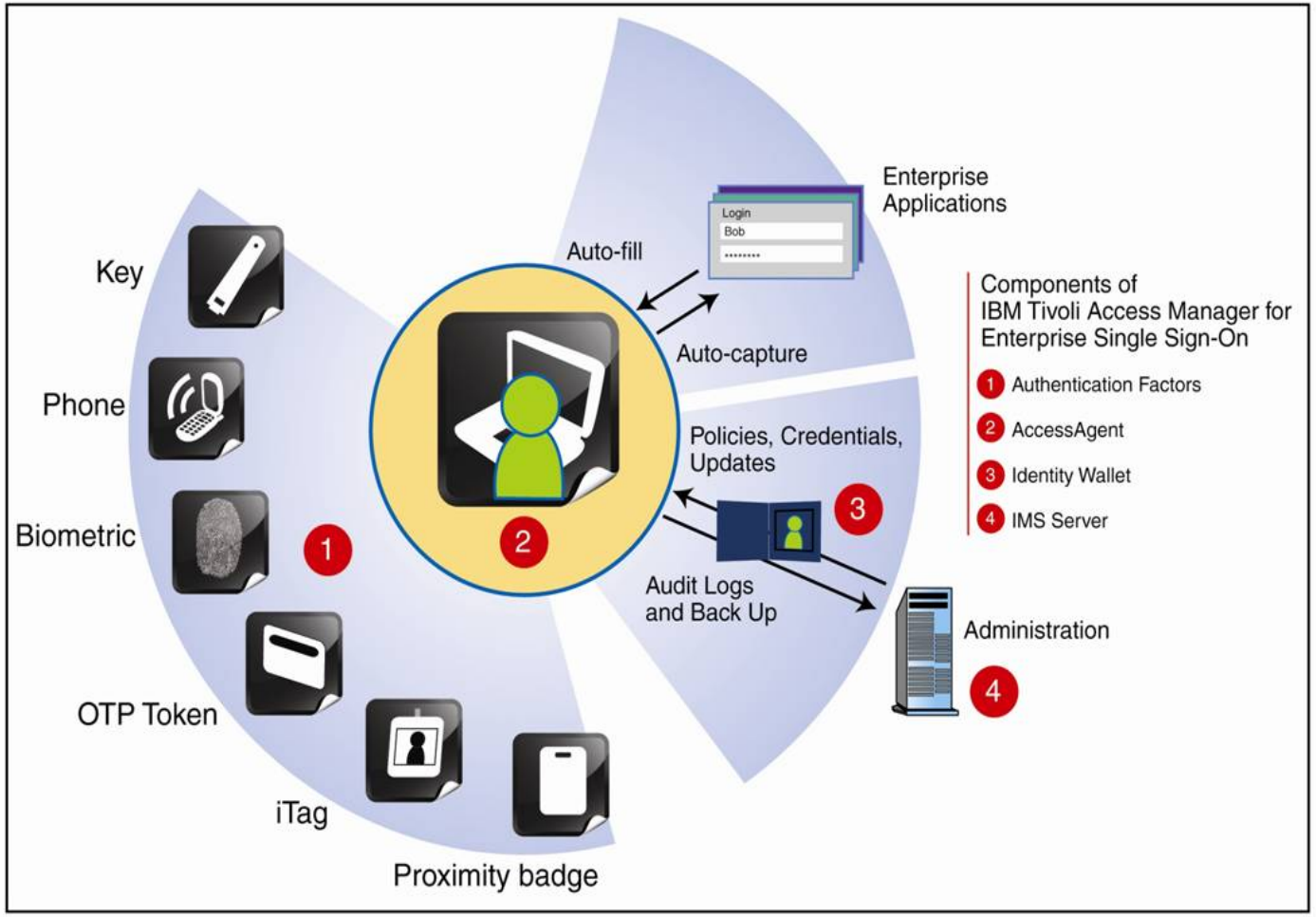
- El proceso de logon y de aprovisionamiento de usuarios es el proceso IT que más necesita ser mejorado en todas las corporaciones
- Afecta a todos los usuarios
- En muchos casos, más de un 5% de su tiempo útil

- Muda, o tareas que no agregan valor:
  - Repetición de trabajos
  - Equivocaciones
  - Controles innecesarios
  - Tiempos muertos

- Repetición de trabajos: Tener que hacer logon a las distintas aplicaciones
- Equivocaciones: Poner mal la contraseña
- Controles innecesarios: Aplicaciones que piden la contraseña cuando el usuario ya se ha identificado
- Tiempos muertos: usuarios que no pueden acceder a la aplicación corporativa por olvidar/caducar/resetear la contraseña. Usuarios que no tienen sus credenciales por falta de aprovisionamiento

Tivoli Access Manager for Enterprise Single Sign-On

- **Logon Único**
- **Compatible con sistemas de autenticación robusta**
- **Soporta estaciones de trabajo compartidas**
- **Autoservicio de contraseñas**
- **Administración basada en web**
- **Acceso remoto para [illegible]**

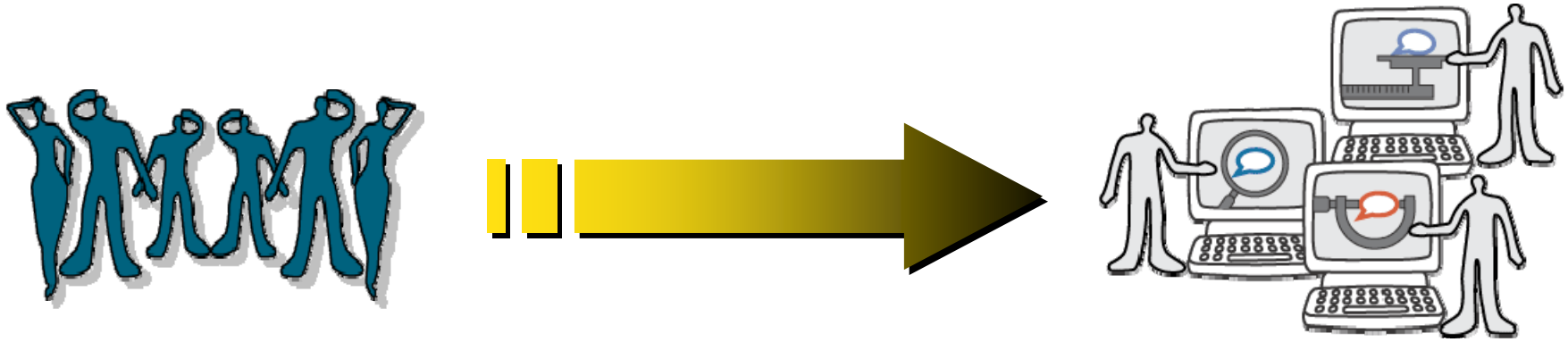


Compatibilidad con múltiples dispositivos de autenticación robusta

- Identificador de Acceso físico
  - Muy bajo coste de integración y TCO
- Dispositivo de Sonar
  - Detecta continuamente la presencia del usuario
- RFID Activo
  - Detecta continuamente la presencia del usuario
- Smart Cards en USB
  - Las credenciales pueden ser guardades en la SC
- **Biométricos**
  - **Ya no se necesita Ninguna contraseña**
- Dispositivos OTP
  - Contraseñas dinámicas

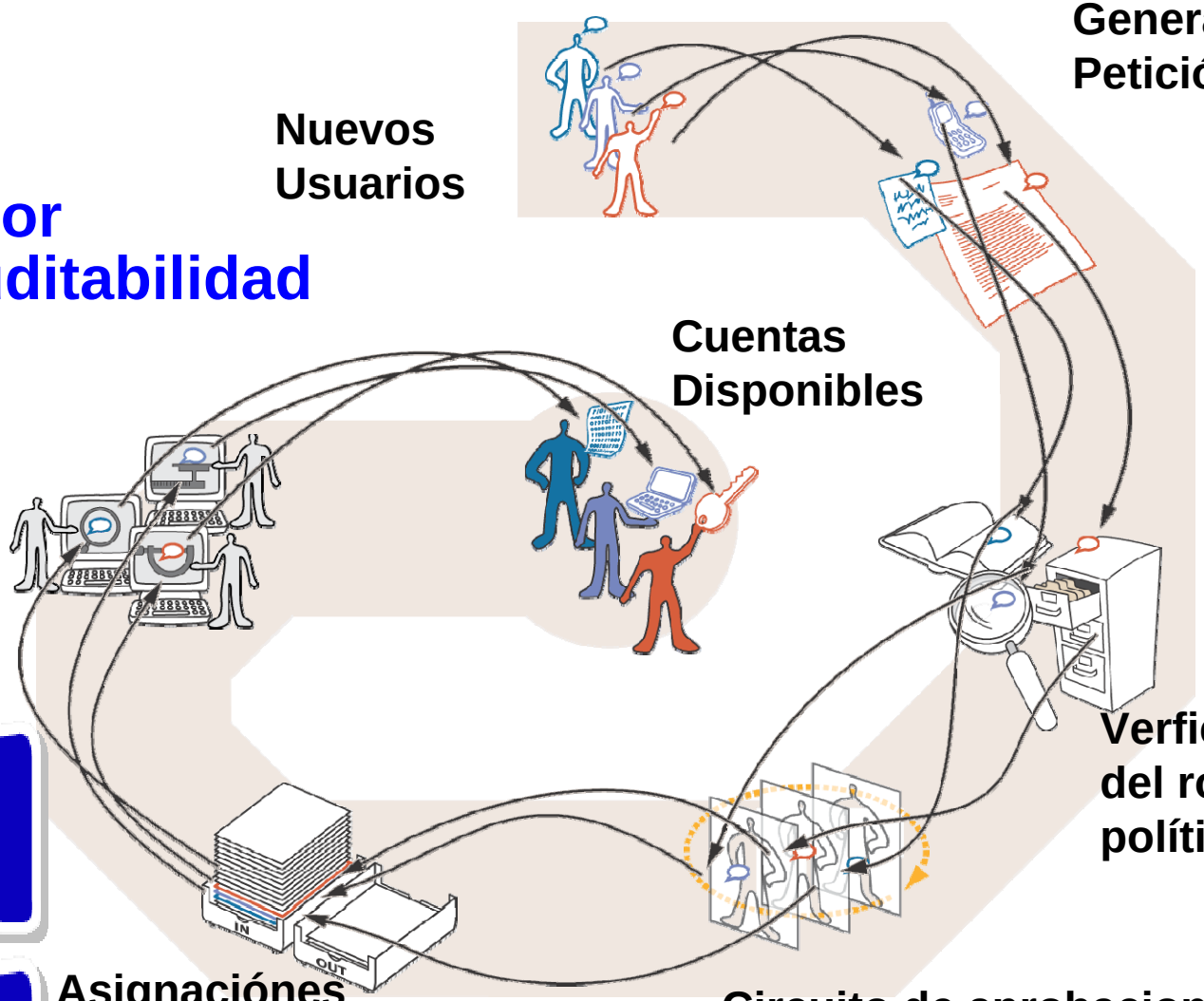
Gestión de Identidades

Gestión de las relaciones entre las personas y su tipo de acceso a sistemas finales



Problemática real: Procedimientos “manuales” dispares y entrelazados

Procesos lentos
Propensos al error
No facilitan la auditabilidad



Mayor tiempo en la habilitación de cuentas

Fallos habituales en la deshabilitación de cuentas

Limitado por la capacidad y ocupación de los administradores

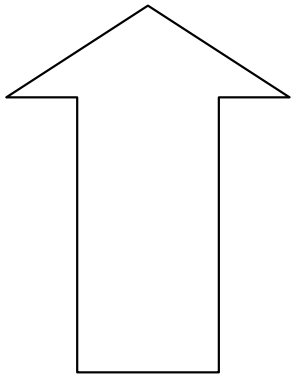
¿Por qué IBM TIM?

1. Método de adquisición de cuentas flexible
2. Plantillas y asistentes configurables y extensibles
3. Simulación de políticas
4. Mejor productividad con la Post Office
5. Análisis de Separación de deberes automático.
6. Agrupación de derechos de acceso (entitlements)
7. Vistas de usuario basadas en su propio rol
8. Disponibilidad de distintos tipos de rol.
9. Ciclo completa de certificación de políticas de seguridad
10. IdM basada en roles o basada en peticiones
11. Workflow de aprobaciones
12. Máxima usabilidad del Interfaz de usuario
13. Control y Gestión de usuarios privilegiados (demo video)
14. Roadmap de producto

Propuesta

- SSO: Prueba de concepto de 1-2 días:
  1. En una estación de trabajo con acceso a todas las aplicaciones
     a) Opcional, en una estación de trabajo de una compañía a fusionar
  2. Se descarga el software, con licencia por un mes, de internet
     1. http://www.ibm.com/developerworks/ssa/downloads/tiv/accessmanager/index.html
  3. Servidor TAM ESSO virtualizado
  4. Se instala agente, en la estación
  5. Se preparan las plantillas de integración de las aplicaciones
  6. Se presentan los resultados

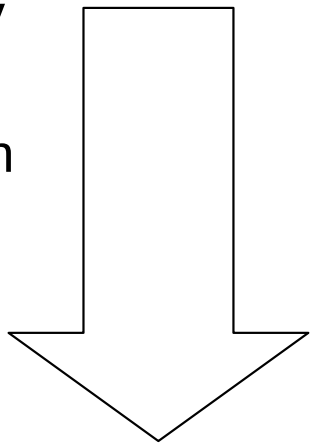
Gestión de Identidades y Single Sign On



- **Protección Más eficaz**
  1. Protección del eslabón más débil, los usuarios
  2. Mayor Robustez de las contraseñas
  3. Control de acceso a todas las aplicaciones
  4. Facilita la Segregación de deberes

Reducción de costes

1. Automatización de tareas de usuarios y administradores
2. Facilita los informes de auditoría (Quien accede a qué)
3. Aumenta la eficiencia de los usuarios
4. Facilita el control y administración de Cambios



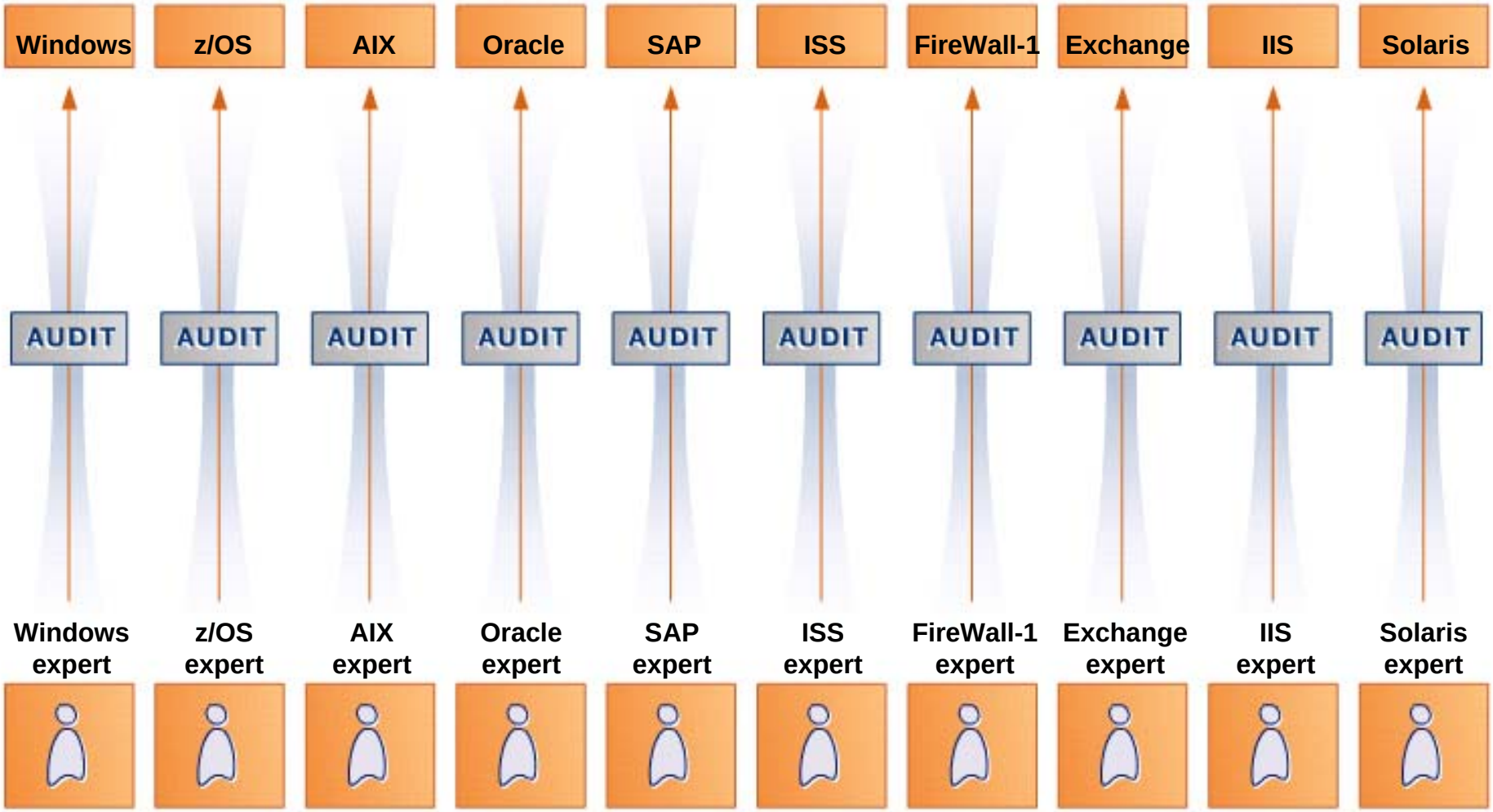
Reducing Costs and Improving control with Regulatory Compliance Mangement

IBM Software

PCTY2010

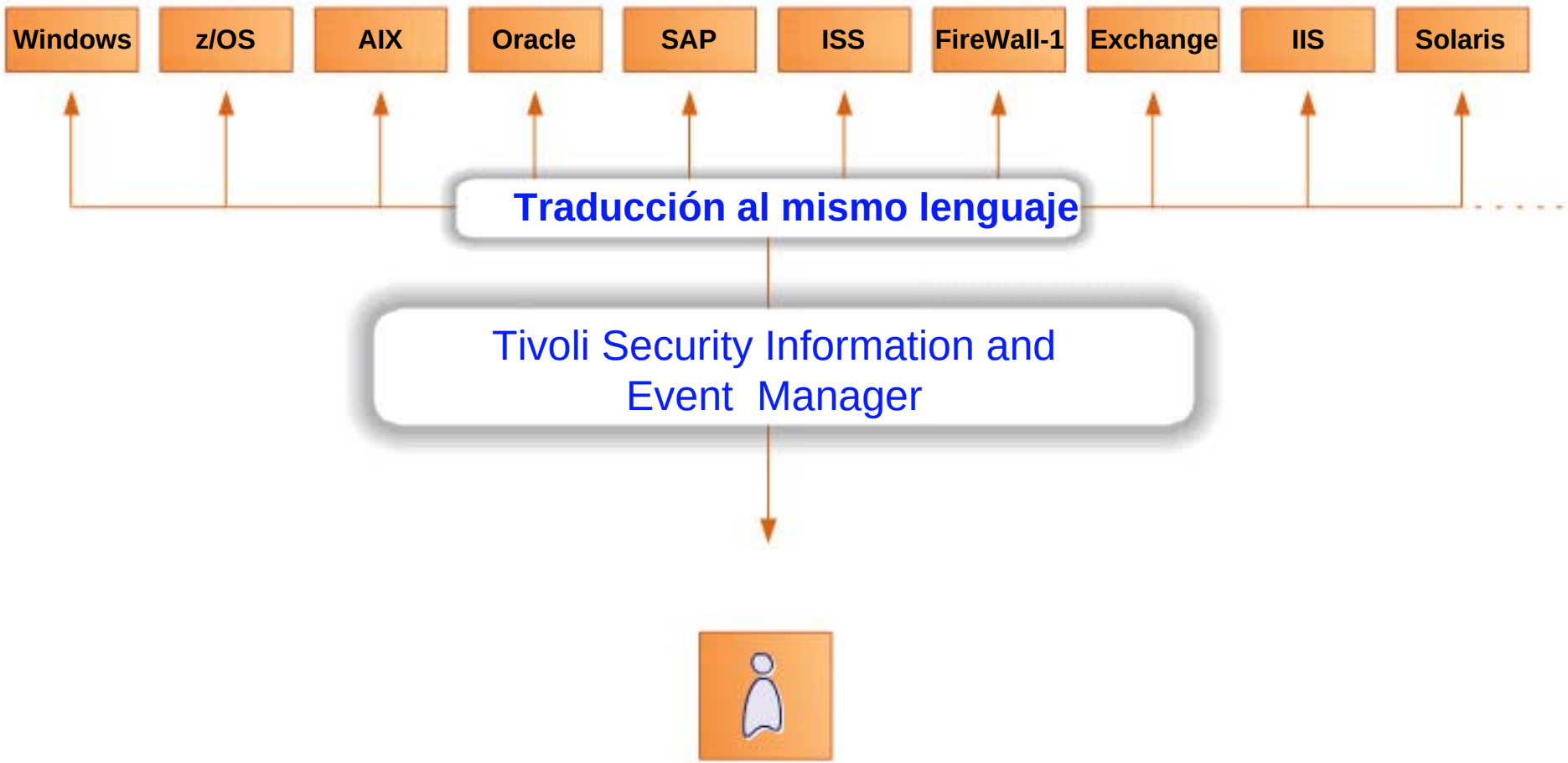
Pulse Comes to You

El análisis de la actividad de los sistemas debe ser realizado por expertos de cada entorno



No se obtiene una visión global de qué está ocurriendo, ni se aprovecha toda la información generada

Integración y correlación de eventos de seguridad



Tivoli Security Information Event Manager (TSIEM) ahorra tiempo y dinero a su departamento de seguridad de la información y cumplimiento mediante la automatización de la monitorización a través de la empresa.

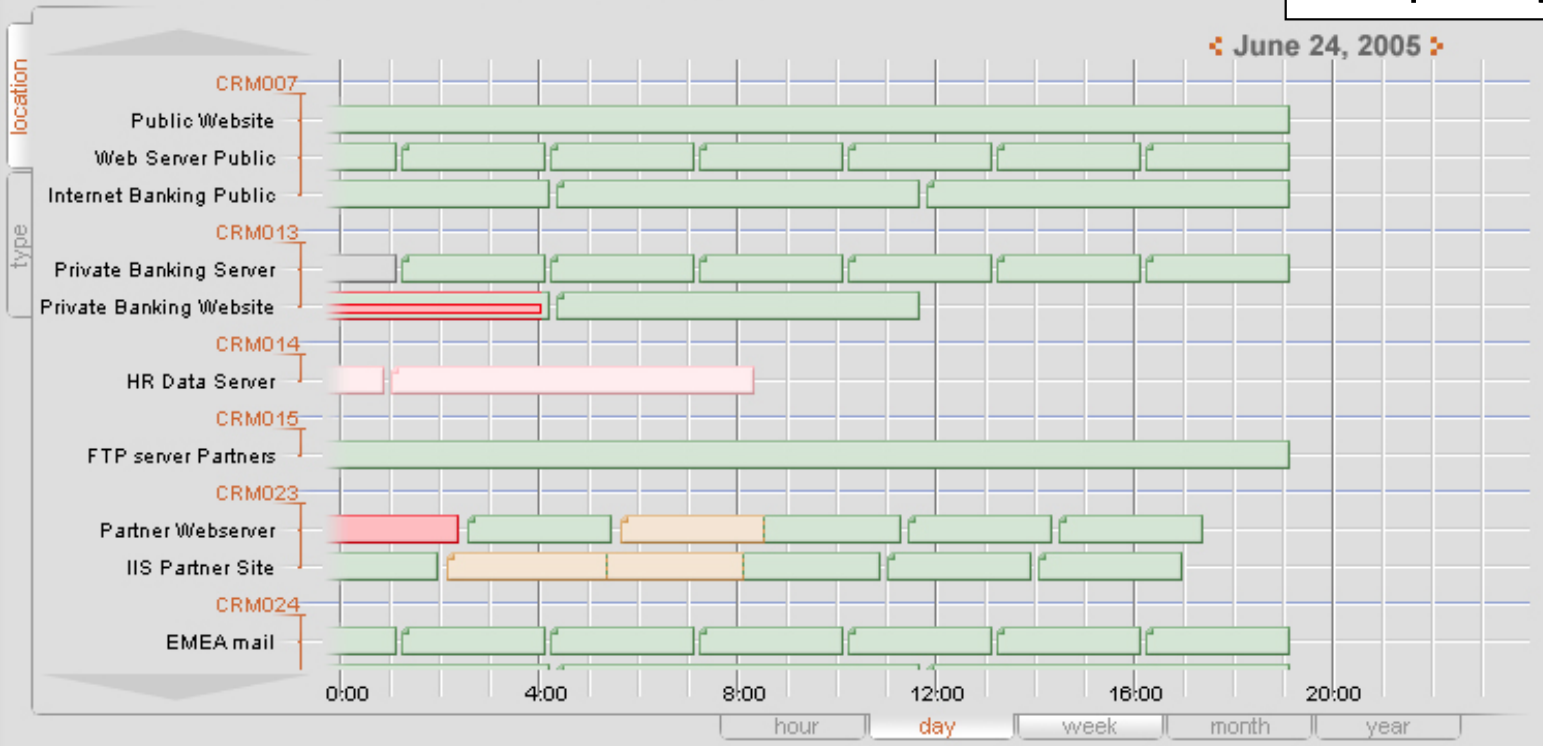
Log Continuity Report
Prueba instantánea para los auditores y reguladores de que la gestión de logs está completa y es continua.

Dashboard | History | Continuity | Activity | Investigate | Retrieval

Portal > Log Manager > Continuity Report

Log Continuity Report

Graph



List of Logfiles

#	Size	Start Date	Time	End Date	End Time	Eventsource Type	Eventsource Name	Machine
3	33 kb	June 25, 2005	10:00	June 25, 2005	12:00 (GMT +1)	IIS	Public website	CRM007
5	21 kb	June 25, 2005	11:00	June 25, 2005	12:00 (GMT +1)	Windows Server	Web Server Public	CRM007
2	1.3 Mb	June 25, 2005	12:00	June 25, 2005	13:00 (GMT +1)	SAP	Internet Banking Public	CRM007
3	5 kb	June 25, 2005	13:00	June 25, 2005	13:17 (GMT +1)	Windows Server	Private Banking Server	CRM013
3	213 kb	June 25, 2005	14:00	June 25, 2005	16:30 (GMT +1)	IIS	Private Banking Website	CRM013
1	94 kb	June 25, 2005	15:00	June 25, 2005	19:00 (GMT +1)	Windows Server	HR Data Server	CRM014

Export to PDF
Export to Excel
Retrieve selected Logfiles
Regenerate Report
Adjust Schedule

View
Hide Timezone (GMT +1)
By Audited Timezone
By Browser Timezone
By Other Timezone

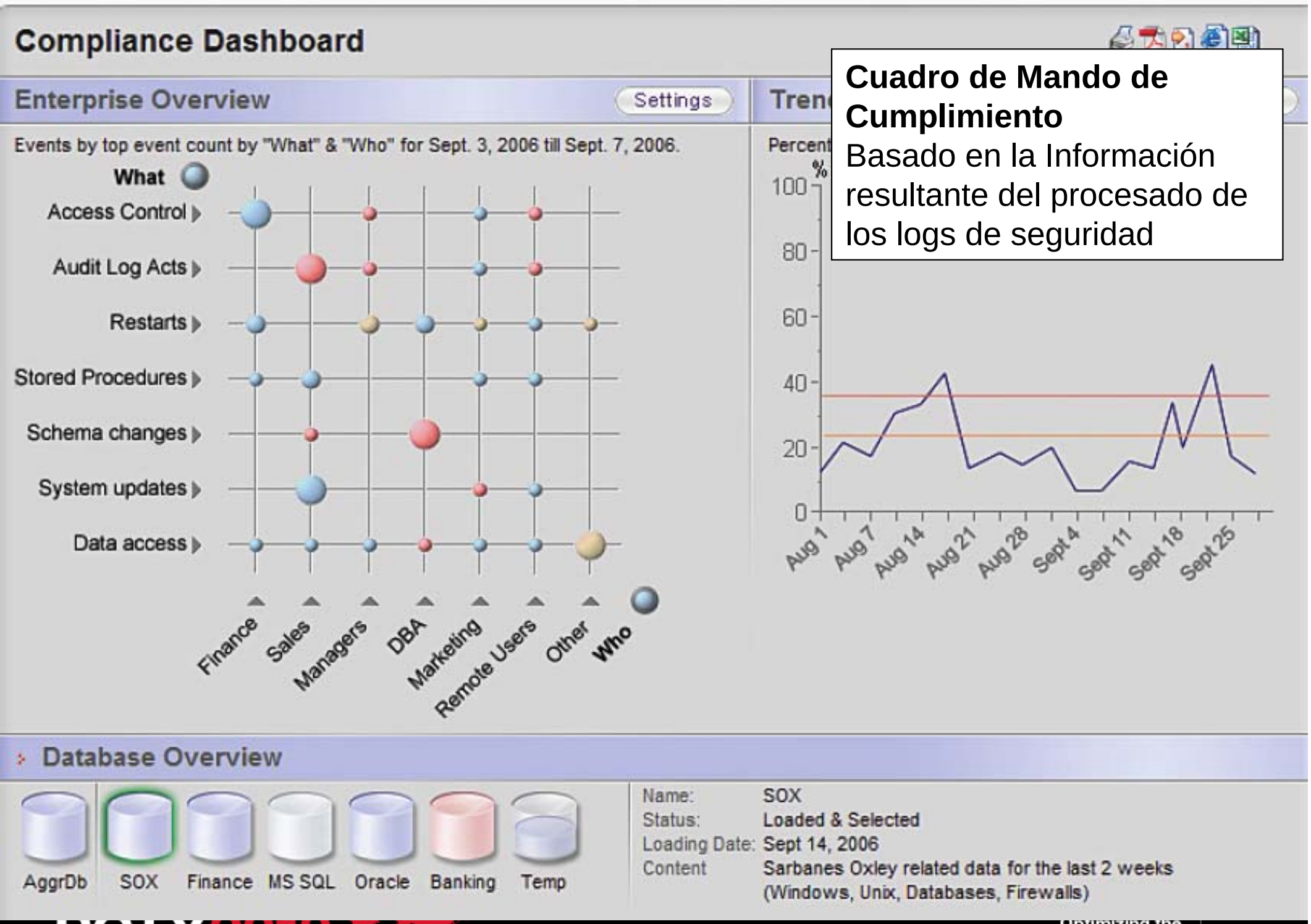
Filters

Sorting
Start Date
Start Time
Audited Machine

Legend
Continuity Logfile
Missing Logfile
Missing Sub Logfile
Failed collect, not collected yet
Delayed collect, possible lost
Archived Logfile
Corrupt Logfile

Report information

Done | My Computer

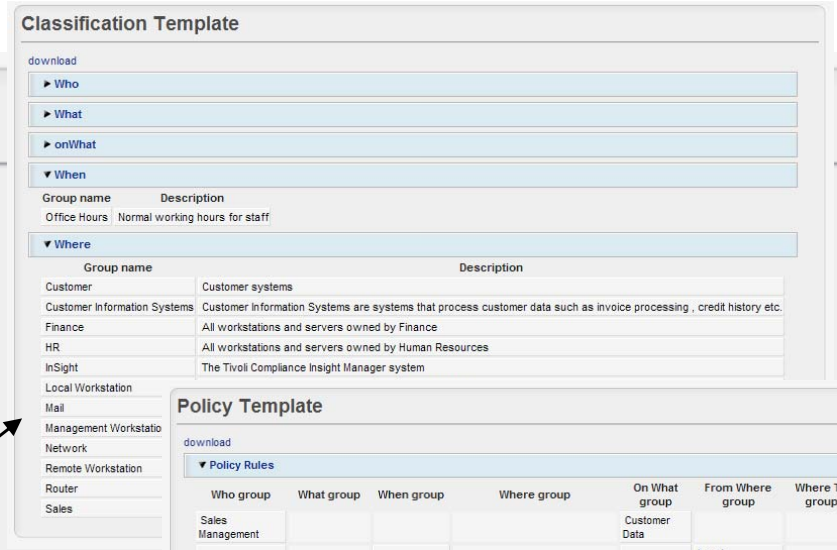


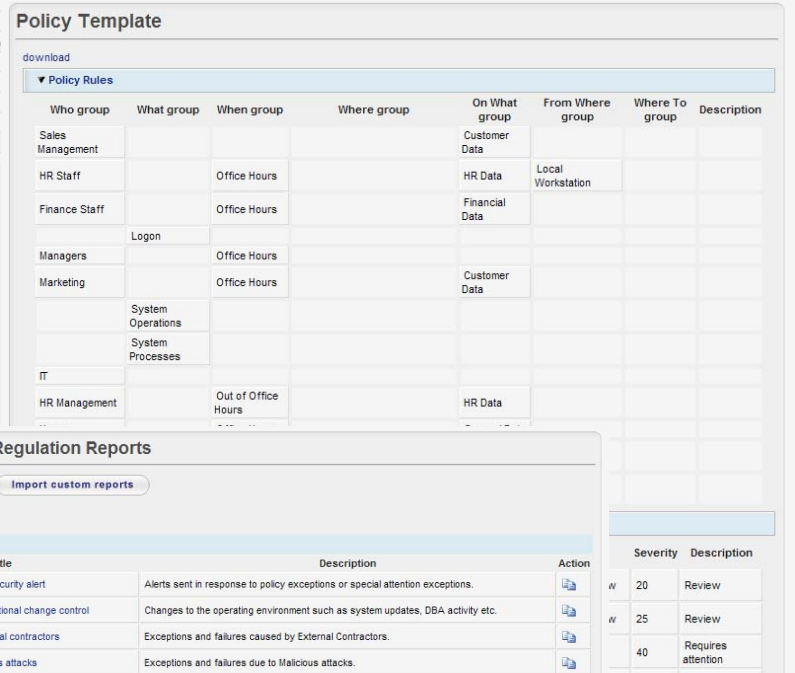
Cuadro de Mando de Cumplimiento

Basado en la Información resultante del procesado de los logs de seguridad

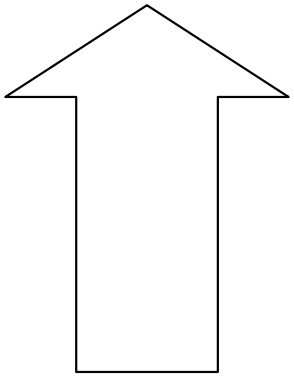
Regulations Resource Center

- **BASEL II**
  - Classification Template
  - Policy Template
  - Reports
  - Documentation
- **ISO 17799**
  - Classification Template
  - Policy Template
  - Reports
  - Documentation
- **Sarbanes Oxley**
  - Classification Template
  - Policy Template
  - Reports
  - Documentation
- **GLBA**
  - Classification Template
  - Policy Template
  - Reports
  - Documentation





Monitorización comportamiento y cumplimiento normativo

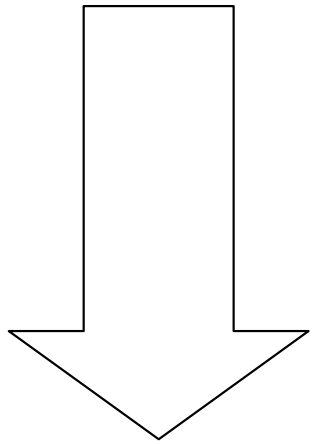


Protección Más eficaz

1. Permite tener una visión global de la seguridad
2. Correlaciona en base a reglas de negocio
3. Subraya los defectos realmente existentes
4. Permite compararse contra mejores prácticas y regulaciones

Reducción de costes

1. Baja drásticamente los costes de auditoría
2. Muy rápida integración
3. Identificar acciones de mejora rápidas
4. Informa en tiempo real, al nivel adecuado.



Resumen

Protección Más efectiva

Infraestructura

- Cercana al 100%
- Proactiva
- Todo el espectro tecnológico
- Certificada por el sector

Gestión de Identidades y SSO

- Protección del eslabón más débil, los usuarios
- Mayor Robustez de las contraseñas
- Control de acceso a todas las aplicaciones
- Facilita la Segregación de deberes

Cumplimiento Normativo

- Permite tener una visión global de la seguridad
- Correlaciona en base a reglas de negocio
- Subraya los defectos realmente existentes
- Permite compararse contra mejores prácticas y regulaciones

Reducción de Costes

Infraestructura

- Consolidación (políticas y tecnología)
- Mayor disponibilidad
- Menor consumo de ancho de banda, mayor rendimiento.
- Solución virtualizada
- Planificación en la aplicación de parches

Gestión de usuarios y SSO

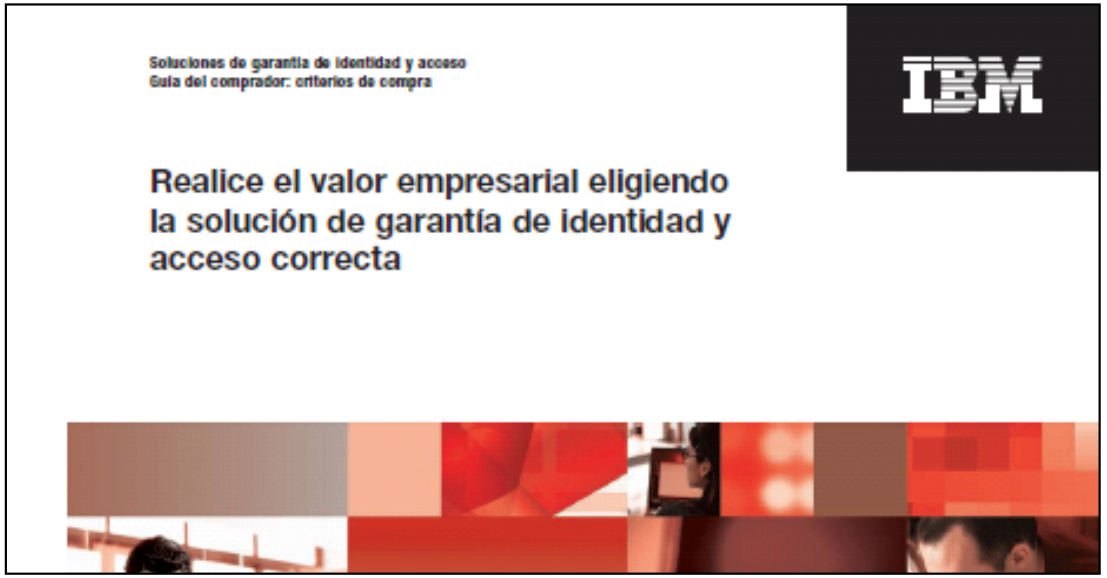
- Automatización de tareas de usuarios y administradores
- Facilita los informes de auditoría (Quien accede a qué)
- Aumenta la eficiencia de los usuarios
- Facilita el control y administración de Cambios
- Reduce los costes de HD y Administración de seguridad

Cumplimiento Normativo

- Baja drásticamente los costes de auditoría
- Muy rápida integración
- Permite lanzar acciones de mejora rápidas
- Informa en tiempo real, al nivel adecuado.
- Reduce costes de formación y especialización.

Documentación

1. Guía de compra de Gestión de Identidades y SSO
2. Reducción de costes con Tecnologías de Seguridad
3. Whitepaper de Gestión de identidades eficaz
4. Ten best Reports for Compliance
5. …



Obrigado