Sobre el Manejo de Identidades y Control de Acceso

Applicación a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Luis Casco-Arias – Gerente de Producto de IBM Security

Agenda

- Nuevas tendencias en el manejo de información
- Retos para mantener la seguridad y el cumplimiento con los reglamentos
- Impacto del manejo apropiado de las identidades y el control del acceso
- Discusión

3 Lecciones principales

1. Cumplimiento con las leyes de privacidad require también controlar las identidades y sus accesos
2. Soluciones para el manejo de identidades son la forma mas eficaz y effectiva de mitigar los riesgos de privacidad
3. IBM ofrece un marco completo e integrado de servicios y soluciones de Seguridad para comenzar desde cualquier punto

Bienvenidos al Planeta Inteligente

Nuestro mundo se está volviendo más.....

Conectado

1E12

Para el próximo año, se estiman 2E9 de personas tendrán acceso al Web... y 1E12 de objetos también – carros, electrodomésticos, cámaras, calles, tuberías – volviéndose en un "Internet de Cosas."

Instrumentado

90%

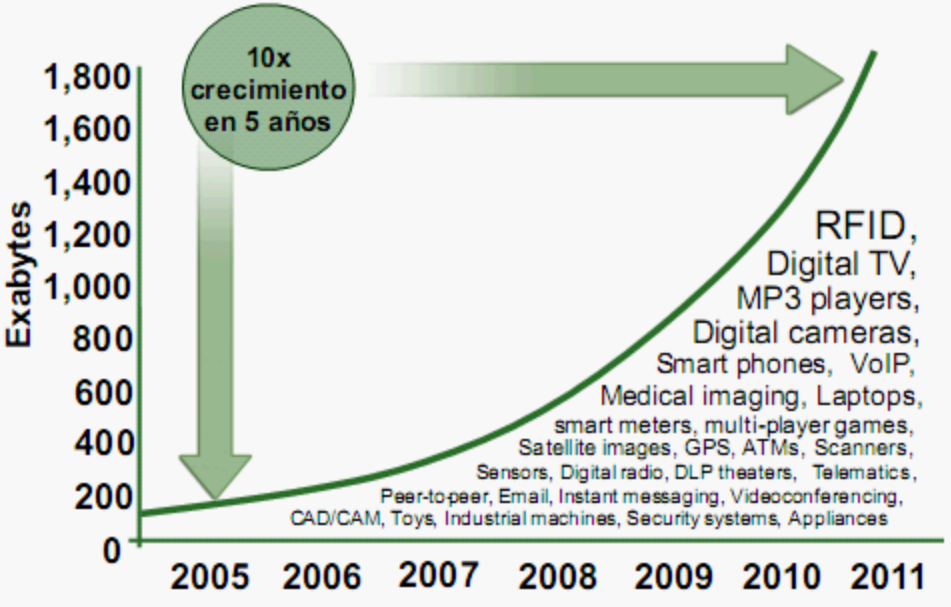
Casi 90% de las innovaciones en los automóviles está relacionada con sistemas de software y electrónica. 30-60% del valor está en el software.

Inteligente

173.8 millones

de Smart phones vendidos en 2009. Más que el número de laptops vendidos el mismo año, por el 2º año consecutivo.

En solo 5 años, el mundo estará 10x más instrumentado. Dispositivos conectados al Internet aumentarán de 500M a 1E12



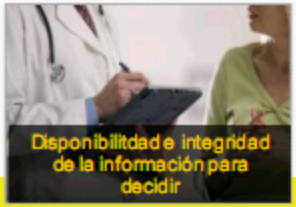
Aproximádamente 70% del universo digital es creado por individuos, **pero las empresas son responsables por 85%** de la seguridad, privacidad, confiabilidad, y cumplimiento normativo.*

* *"As the Economy Contracts, the Digital Universe Expands", IDC, May 2009*

El estado de la seguridad en el Planeta Inteligente

Nuevas posibilidades.
Nuevas complejidades.
Nuevos riesgos...

"Hemos visto más cambios en los últimos 10 años que en los 90 previos"
Ad J. Scheepbouwer, CEO, KPN Telecom

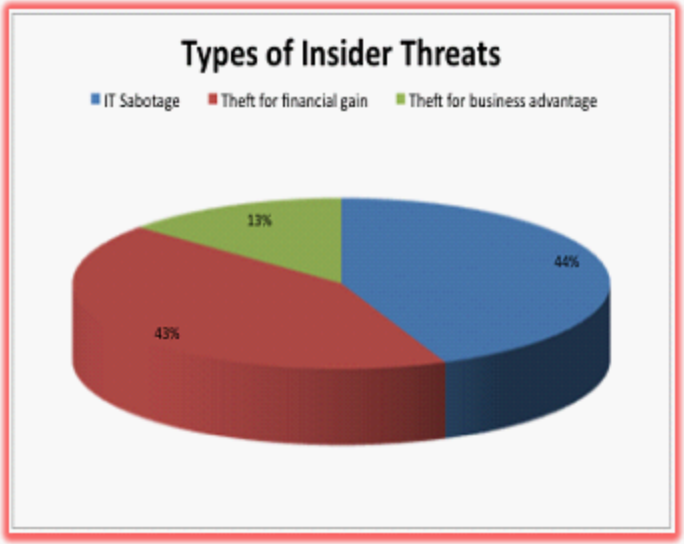


La Seguridad permite afrontar estos riesgos e innovar confiadamente

Personas registradas válidamente pueden causar daños (no) intencionalmente

Usuarios pueden abusar de sus privilegios

- 50+% de los encuestados en un estudio del eCrime en 2007-09 sufrieron por lo menos 1 "insider incident" malicioso
- El sabotaje de IT y el robo para aventajarse en los negocios son generalmente cometidos por usuarios técnicos y privilegiados
- La perdida promedio por e-crime es $465,000 por compañía impactada
- La guía de "CERT best practice" recomienda: "Use cuidado extra con los sys-admin, usuarios técnicos o privilegiados".



Fuentes:

- 2010 Cybersecurity (e-crime) Watch Survey (conducted by CSO, the U.S. Secret Service, CERT and Deloitte's Center for Security & Privacy Solutions)
- Ponemon Institute's Cost of Cyber Crime Study 2010
- "Common sense guide to detection and prevention of insider threats" 3rd edition - v3.1, CERT, Jan 09

A quién le importan los usuarios privilegiados?

su auditor...

Reglamento	Relación al control de cuentas Privilegiadas
Payment Card Industry (PCI) Data Security Standard (DSS)	Proteger los datos del portador de tarjetas (#3) Desarrollar y mantener la seguridad de los sistemas y aplicaciones (#6) Restringir acceso a los datos de los portadores de tarjeta a razón de la necesidad-de-saber para el negocio (#7) Controles insuficientes sobre las cuentas privilegiadas impactarían negativamente la capacidad de la empresa de cumplir estos requisitos.
California Senate Bill 1386 (now California Civil Code 1798) Otros Reglamentos de Privacidad del Estado	SB 1386 requiere que las organizaciones que pierden información privada de los residentes de California, que lo reporten a los individuos afectados. Usuarios privilegiados no autorizados pueden sobrepasar los controles normales de acceso y audito en la mayoría de los sistemas para obtener información privada sin que la empresa lo note.
Sarbanes-Oxley Act (SOX) Section 404	Requiere que la administración corporativa tome la responsabilidad de establecer y mantener controles internos adecuados y procesos para el reporte del estado financiero. Controles insuficientes sobre las cuentas privilegiadas impactarían negativamente la capacidad de la empresa de cumplir estos requisitos.
EU Data Protection Act	Pautas técnicas apropiadas deben aplicarse contra el trato ilegal de datos personales y contra perdidas accidentales del los mismos... incluyendo el control de acceso a la información Controles insuficientes sobre las cuentas privilegiadas impactarían negativamente la capacidad de la empresa de cumplir estos requisitos.

Requisitos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

- Clasificación y protección de datos
- Establecer y mantener medidas de seguridad
- Aviso de Privacidad.
- Comunicar transferencia de datos.
- Designación de Chief Privacy Officer
- Ventanilla de atención

Presión de las Consecuencias

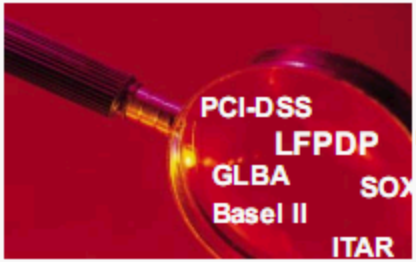
- Multas (hasta de 76MDP)
- Sanciones
- Delito (condena hasta de 10 años)

Muchas otras fuentes también reflejan los mismos requisitos comerciales para el manejo de identidades y el control de acceso

- FFIEC — Financial Services regulatory requirements
- ISACA — Information governance, control, security & audit regulations
- COBIT — Control objectives for information & related technology regulations
- BITS — Financial Services industry standards
- ISO (International Organization for Standardization) — ISO 27001 International standard for information security
- IBM — Commercial security standards (GSD, ISeC)

Los retos que incitan a manejar identidades digitales

- **Gobernabilidad, riesgo y cumplimiento**
  - Motivación
    - Establecer un proceso de rendición de cuentas y seguimiento de audito para los reglamentos externos y las políticas internas.
  - Reto Original
    - Tiempo/costo de la preparación del complimiento normativo
    - Audito reprobado
    - Requisito de certificación debido a la proliferación de accesos



HIPAA
FISMA
J-SOX
ISO 27001

- **Seguridad**
  - Motivación
    - Mitigar el riesgo de fraude, robo de propiedad intelectual, pérdida de datos personales, etc…
  - Reto Original
    - Incidentes o brecha previa
    - Poca visibilidad de los riesgos basados en accesos de usuarios
    - ID durmientes o identidades compartidas
    - Falta de rastreo de las actividades de los usuarios privilegiados

Casi 2/3 de los Ex-empleados Roban Datos Cuando Salen

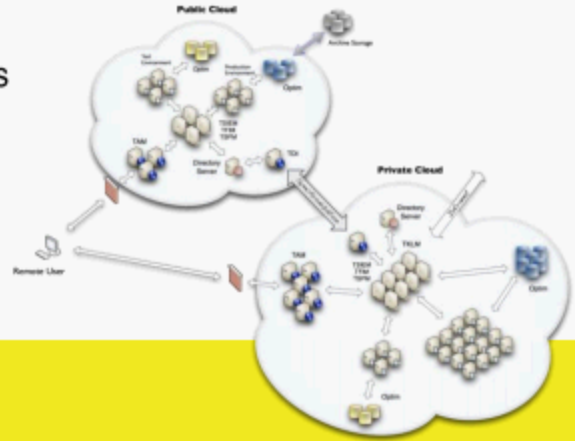
PCWorld

"59% de los trabajadores que dejaron sus posiciones, tomaron información confidencial con ellos."

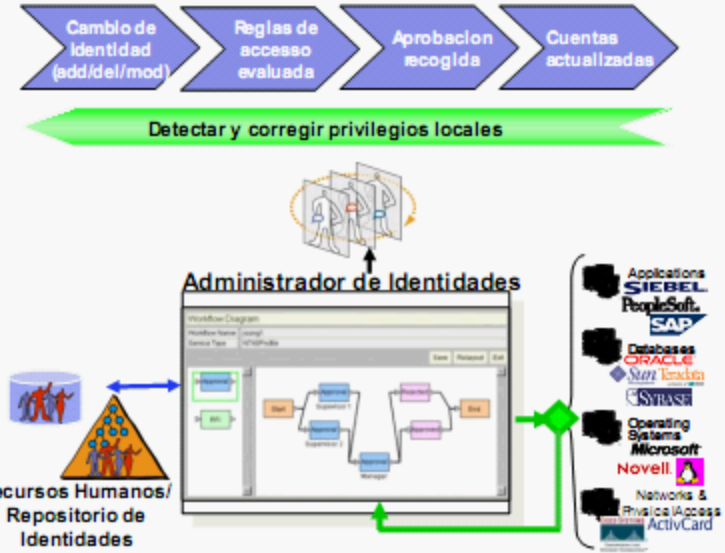
- **Reducción de costos (via automatización)**
  - Motivación
    - Optimización de los procesos de acceso a recursos dentro del entorno de IT y del negocio
  - Reto Original
    - Costo/tiempo de la administración manual del acceso a usuarios
    - Manejo de un gran número de cambios en aumento
    - Expansión del control sobre los derechos a los recursos
    - Demora o expansión de proyectos de aproviosamiento de usuarios

… nuevos requisitos para aplicar controles con contexto de Negocios *afrontando las tendencias en el data center y las implementaciones cloud*

- Gobernabilidad dirigida por la política empresarial
  - Controles de acceso con contexto
    - Consciente de la identidad
    - Consciente del contenido
    - Consciente de la transacción
  - Gobernabilidad orientada al Negocio
    - Gobernabilidad de IAM
- Apoderar a las personas, habilitar la colaboración
  - El rol de "actor del negocio" tomado en cuenta en el ciclo de vida
  - Habilitar a los usuarios, administradores, los responsables del negocio, y responsables de las aplicaciones
- Seguridad distribuida como un servicio (SSaaS)
  - integración con aplicaciones de negocios
- Interoperabilidad por medio de "open standards"



Los sistemas de manejo de identidades y acceso (IAM) automatizan, auditan, y remedian los derechos a acceso a través de la infraestructura de IT



- Descubra las ***personas*** asociadas con las cuentas y ***porqué*** tienen acceso
- Arregle cuentas en incumplimiento normativo
- Automatice el ciclo de provisión de privilegios a través de toda la infraestructura de IT
- Concuerde con sus procesos de trabajo

La Gorbenabilidad de IAM crea un puente entre el Negocio e IT, para cumplir con los requisitos evolucionarios en el entorno del manejo de accesos

Maneje el crecimiento y escala del acceso de usuarios

Añada Contexto de Negocios

Role Management

Entitlement Management

User → Roles → Applications → Access Rights

Susan

Cardiologist
Chief Resident
Emergency Room Nurse
Radiologist
Lab Technician

Laboratory
Radiology
Admission, Discharge, Transfer (ADT)
Ambulatory Clinical System

RACF/ACF2/ Top Secret
Execute, Read, Update, Alter
UNIX
Read, Write, Execute
SAP/Oracle
Alter ,Delete, Execute, Index, Insert, Select
LDAP/Active Directory
Read, Write,Search

Gobernabilidad IAM

Resuelva el control débil del manejo de accesos

Privileged Identity Management
Administer, control and monitor privileged identities

Maneje conflictos de acceso

Separation of Duties
Nurse cannot have role of Doctor
Nurse admitting patient cannot discharge on own

Evite brechas de acceso

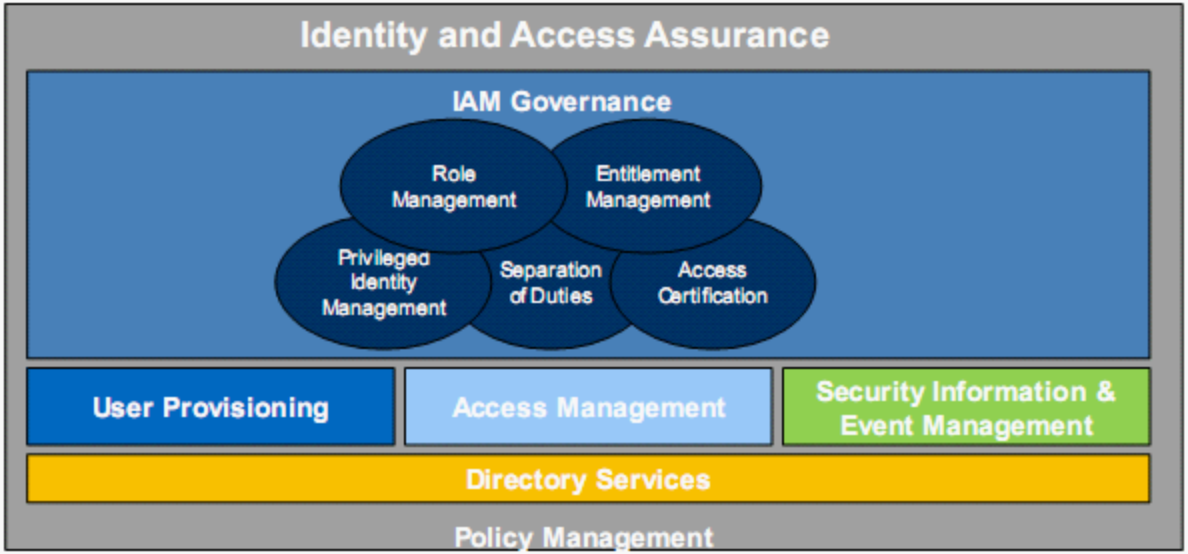
Access Certification
Certification Triggers: SOX, HIPAA, SAS 70, Basel II, FISMA, etc..

Efectividad de la política de cumplimiento normativo

Business ↔ IT

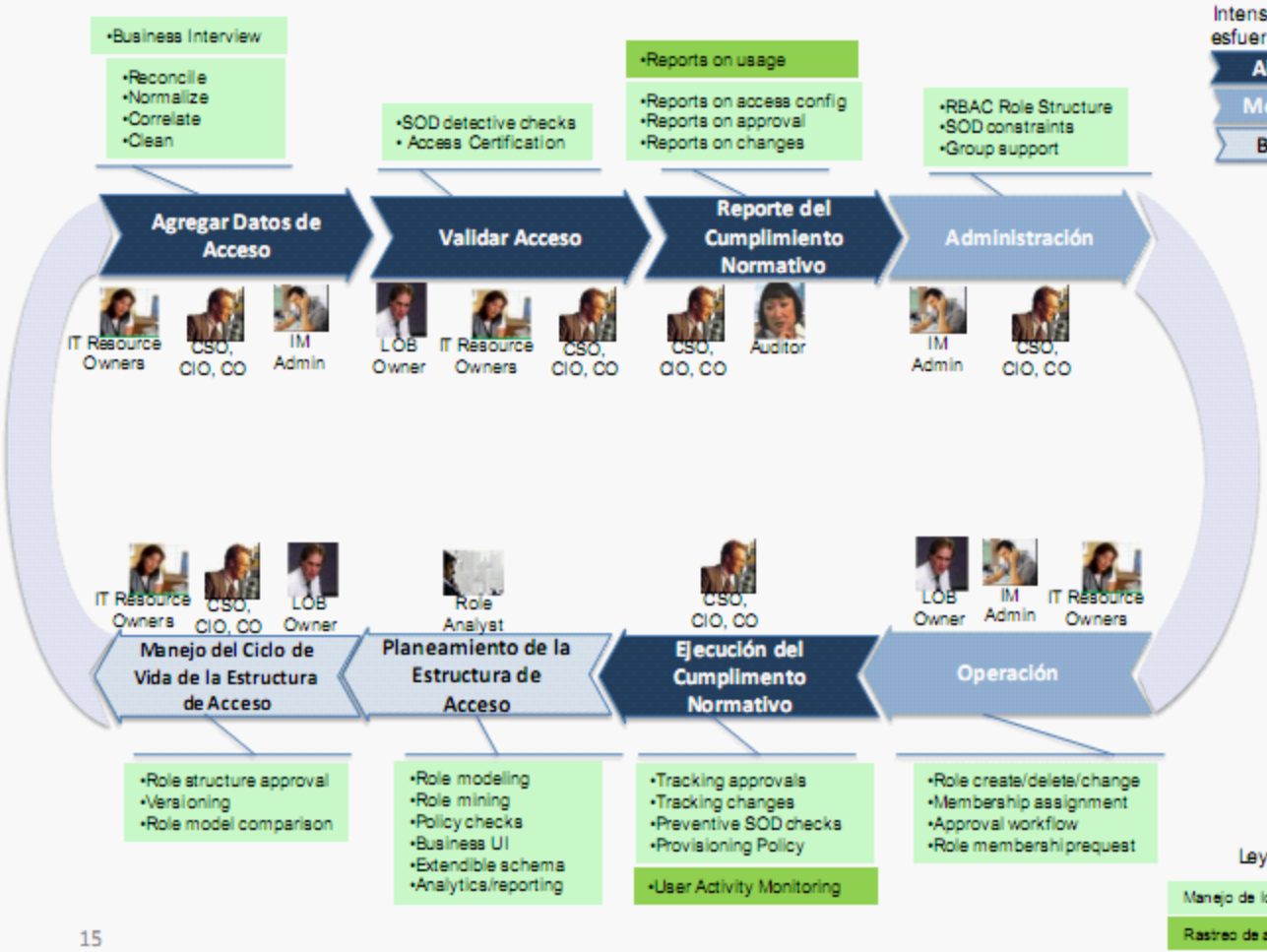
User Activity Monitoring

Las nuevas capacidades de la Gobernabilidad de IAM aprovechan y expanden la infraestructura de IAM ya desplegada



"Identity and Access Assurance" permite gobernar y ejecutar el acceso a los recursos mientras provee un circuito-cerrado para el cumplimiento normativo.

La Gobernabilidad de IAM cumple con las necesidades críticas de los clientes

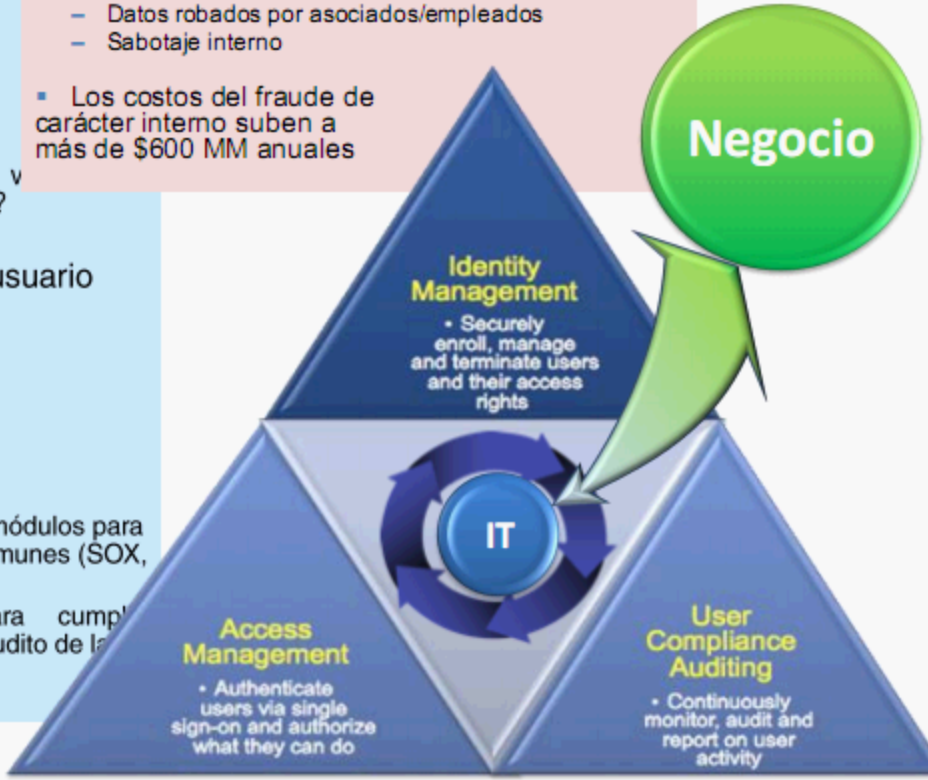


Escenario: Maneje el riesgo de los ataques internos y los auditos reprobados con la certificación de accesos, el seguimiento de la actividad del usuario, y los reportes

El problema:

- 3 de cada 10 ataques a las Empresas son de carácter interno:
  - Errores del empleado/usuario
  - Datos robados por asociados/empleados
  - Sabotaje interno
- Los costos del fraude de carácter interno suben a más de $600 MM anuales

- Garantía del acceso actual
  - Tienen los usuarios el nivel de acceso?
  - Se certifican los accesos periódicamente?
  - Hay verificación de v a la separación de derechos?
- Rastreo de la actividad del usuario
  - Volumen de actividad
  - Tipo & localización
  - Tiempo de actividad
  - Usuarios privilegiados
- Reporte del cumplimiento
  - Reportes predispuestos en módulos para las Leyes o Reglamentos comunes (SOX, PCI, Basel II, etc…)
  - Reporte de diseño flexible para cumpl con los requisitos de audito de l empresa.



Porqué Identity & Access Assurance?

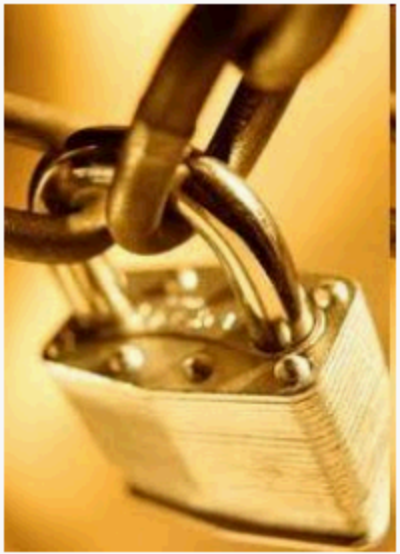
- Optimice el cumplimiento normativo
- Aumente la Seguridad - Contrarreste el Riesgo
- Reduzca Costos
- Mejore la Productividad y el Servicio de IT

Optimize el Cumplimiento Normativo

- Evite la reprobación del audito
- Reduzca el costo del proceso de cumplimiento
- La Gestión de Identidad y Acceso puede:
  - Rastrear el incumplimiento y actividad del usuario
  - Remediar deficiencias
  - Identificar cuentas durmientes o huérfanas
  - Ejecutar políticas de acceso automáticamente
  - Identificar conflictos en la separación de derechos
  - Ejecutar reglas de contraseñas fuertes
  - Automáticamente comenzar el proceso de aprobación y certificación
  - Validar la identidad del usuario
  - Facilitar la autenticación fuerte
  - Centralizar y automatizar los reportes para cumplimiento normativo

Aumente la Seguridad

- Prevenga (otras) brechas internas
- Aprovisione credenciales fuertes / confiables
  - Disuada el "hacking" de las contraseñas
- Automatice la identificación de cuentas durmientes y huérfanas para la rápida remediación
  - prevenga el uso no autorizado de recursos
- Use la certificación de acceso para garantizar la necesidad empresarial del acceso
- Identifique conflictos en la separación de derechos
- Maneje cuentas privilegiadas y compartidas
- Mejore el tiempo de reacción a auditos reprobados
- Gobierne los usuarios privilegiados (acceso root)
- Detecte y corrija cambios al acceso de IT no autorizados
- Garantice la confianza y lealtad de sus clientes



Reduzca costos y mejore la productividad y servicio de IT

- Aprovisionamiento de usuarios centralizado y automático reduce el esfuerzo para manejar el ciclo de vida de los usuarios
  - Creación de cuentas y manejo de cambios cotidianos basado en un modelo de acceso por roles
  - Usuarios y sus gerentes pueden pedir acceso automáticamente ellos mismos
  - Automatice la admisión y retiro de los usuarios a los sistemas de IT
  - Aumente la productividad del usuario acelerando el tiempo para obtener acceso
- Reducción de costos del Help Desk debido a cambios de contraseñas
  - Autoservicio de acceso para los usuarios reduce el volumen de llamadas drásticamente
- Facilite la integración del contexto de identidad
- Aumente el alcance al mercado con un modelo de federación de negocios
- Habilite la colaboración vía portales basados en roles para llegar a los servicios de la Empresa

La Gestión de Identidades y Acceso capacitan la innovación

Cloud

Autenticación Multi-factor

Entornos de Computación Movil

Gobernabilidad de IAM

Analítica para Seguridad e Identidad

La visión de Gobernación de IAM de IBM

¿Cómo Proteger la Información de sus Clientes?

El Manejo de Identidades y Accesos (IAM) es primordial para el "IBM Security Framework"

- *Asigne los derechos apropiados a los usuarios apropiados en el tiempo apropiado*
- *Proteja los datos sensitivos del negocio*
- *Mantenga aplicaciones disponibles y protegidas contra el uso malicioso o fraudulento*
- *Optimize la disponibilidad de los servicios mitigando el riesgo*
- *Provea inteligencia procesable y mejore la efectividad de la seguridad para la infrastructura física.*

Porqué IBM?
es su socio de confianza…

Sabe como asegurar el éxito

Exitosamente implementa 1000s de poyectos para clientes

Provee valor por entender la perspectiva mas amplia

Seguridad entre mainframes, desktops, redes, dispositivos móviles

Les ayudamos a escoger

Cree su solución apropiada

IBM Security Solutions

Experiencia para cumplir las necesidades de su industria

Ajuste las soluciones para cumplir con los restos de su industria

Garantize exito mediante el ejemplo

Maneja la seguridad para 400,000 empleados de IBM , 7B eventos/día para clientes

Casos exitosos de clientes demuestran los resultados

Implementamos Seguridad de IT por mas de 30 años, 200 referencias de clientes

Aproveche nuestras capabilidades para llegar a su objetivos

1000s de investigadores y expertos

Asociados con un ecosistema inmenso

Una gran comunidad de asociados

Implementando soluciones de seguridad con una perspectiva única

24

Gracias!

PREGUNTAS?

Llamado a la Acción

Pinpoint your real needs

- Don't let the market, analysts, or vendors determine what you really need for Identity and Access Governance

Build a roadmap for implementation

- Seek out solutions that can help you easily grow into a more complete solution, and that do not paint you into a corner.
- Who can help you long term

Look at what others have already achieved

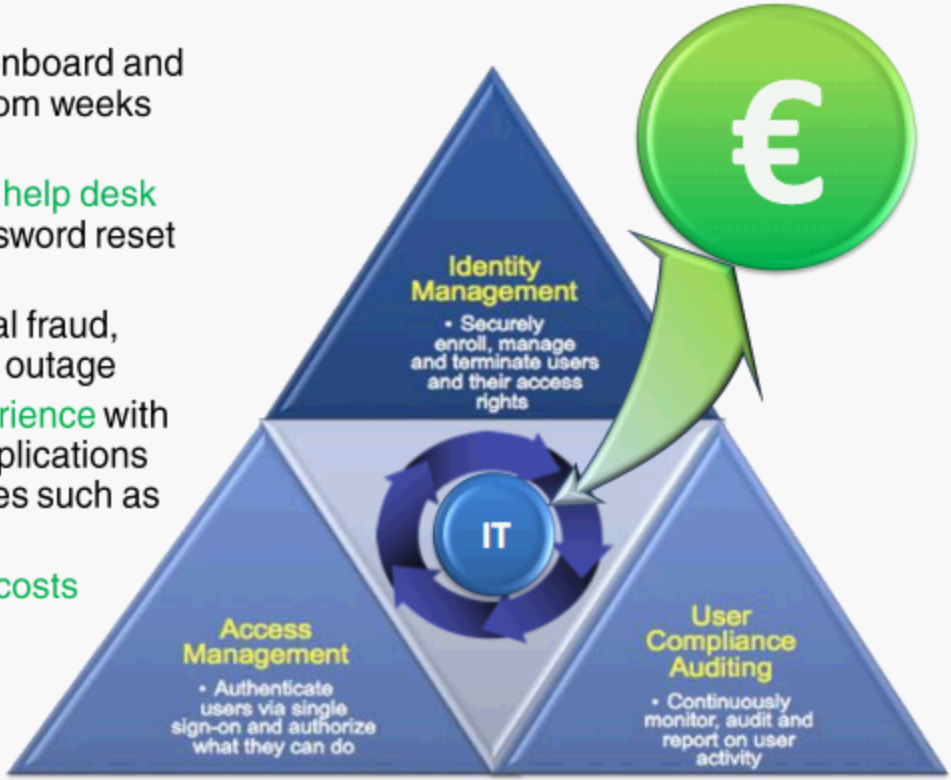
- Ask for references in the area you are interested
- Check what is the ROI they got

Plan o esquema

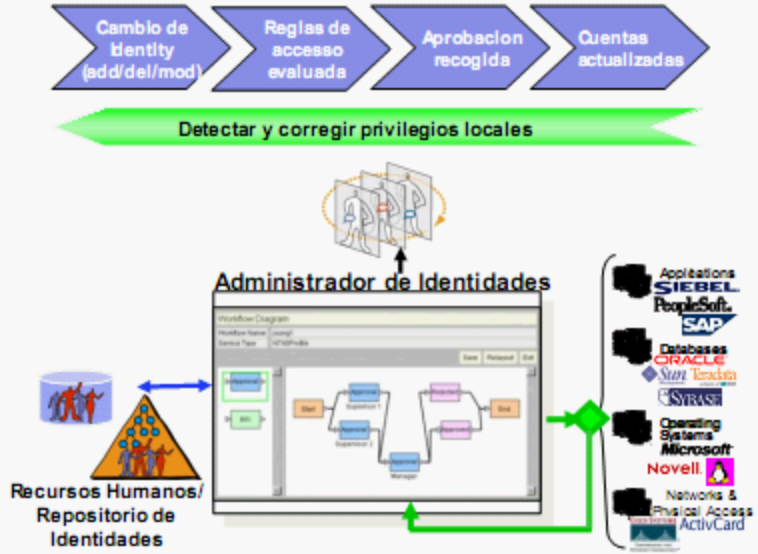
- Introducción
  - Como en otros reglamentos y leyes, tambien podemos ver que no es suficiente proteger PII directamente, sino que se tiene que tener control sobre las identidades y el acceso que estas tienen. En fin, el entorno en el cual se utiliza o adquiere esta informacion.
- El ambiente de IT y las nuevas tendencias en el manejo de informacion
- Retos en el area de Seguridad (Retos, barreras y oportunidades)
  - Esfuerzos aislados de seguridad, con soluciones de nicho o muy especificas
  - Incumplimiento de la ley implica delitos, multas, sanciones
  - Presion y obligacion de cumplir con la ley (responsabilidad legal)
    - Multa de hasta 76MDP
      - Apercibimiento
      - Reincidencia
      - Datos sensibles
    - Prisión de hasta 10 años
      - Vulnerar bases de datos
      - Tratar datos mediante engaño
      - Datos sensibles
  - Incertidumbre sobre como enfocarse en este tema… cual es el primer paso? Cuando esta terminado? ….
  - Presupuestos limitados
  - Aprovechar las disposiciones de seguridad ya en efecto
- Necesidades y requisitos para IAM (Cual es la solucion)
  - Centralización de la gestión de identidades y accesos
  - …. Otras funciones
- Impacto de IAM
  - Perspectiva de la solucion IAM
    - Bases de datos de identidad como depositos autoritario (autoritativo) de informacion personal
    - Soluciones de manejo de identidad como control sobre el personal que administra dicha informacion.
  - Beneficios para el negocio
  - Beneficios en un ambiente regulatorio
- IBM como proveedor de soluciones integradas de seguridad

Implementing identity and access management can address these challenges and drive positive results

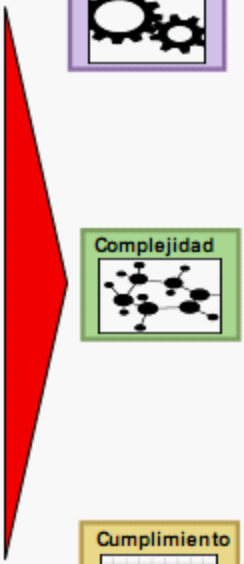
- Can reduce the time to onboard and de-provision identities from weeks to minutes
- Can significantly reduce help desk costs resulting from password reset calls
- Decreases risk of internal fraud, data leak, or operational outage
- Improves end-user experience with Web-based business applications by enabling such activities such as single sign-on
- Streamline Compliance costs



Los sistemas de manejo de identidades y acceso (IAM) automatizan, auditan, y remedian los derechos a acceso a través de la infraestructura de IT



- Descubra las ***personas*** asociadas con las cuentas y ***porque*** tienen acceso
- Arregle cuentas en incumplimiento normativo
- Automatize el cyclo de provision de privilegios a través de toda la infrastructura de IT
- Concuerde con sus processos de trabajo



Reduzca Costos

- Autoservicio de reset de contraseñas
- Aprovisionamiento automático de cuentas

Maneje Complejidad

- Política de securidad consistente
- Integre nuevos usuarios y applicaciones rapidamente

Afronte Cumplimiento Normativo

- Approvisionamiento de "Circuito Cerrado"
- Audito y reporte de los derechos de acceso

Porqué Identity & Access Assurance?

- **Soporte del Esfuezo por Cumplir con las Normativas:**
  - Validar la indentidad del usuario, rastrear su activida, facilitar la autenticación fuerte
  - Centralizando y automatizando los reportes para cumplimiento normativo
- **Contrarreste el Riesgo**
  - Mejore el tiempo de reacción a auditos reprobados
  - Prevenga brechas internas
  - Valide o certifique si accesos de usuarios todavia son requeridos
  - Gobierne los usuarios privilegiados (accesso root)
  - Aprovisione credenciales fuertes / confiables
  - Detecte y corrija cambios al acceso de IT no autorizados
  - Garantize la confianza y lealtad de sus clientes
- **Reduzca Costos**
  - Reduzca los costos del “help desk” debido a cambios de contraseñas
  - Administre eficientemente cambios de acceso debidos a cambio organizacional
  - Maneje centralmente cuentas, grupos, politicas, credenciales, y derechos a acceso durante el ciclo de vida del usuario.
  - Automatize el abordo y desbordo de los usuarios a los sistemas de IT
  - Facilite la integracion del contexto de indentidad
- **Mejore el Servicio**
  - Aumente la productividad del usuario acelerando el tiempo para obtener acceso
  - Aumente el alcance al mercado con un modelo de federacion de negocios
  - Habilite la colaboración via portales basados en roles para llegar a los servicios de la Empresa

Nuestra estrategia?: Ser completos, aprovechar a los asociados

- Professional Services
- Managed Services
- Products
- Cloud Delivered

GRC
- Security Governance, Risk and Compliance
- Security Information and Event Management (SIEM) & Log Management

Identity & Access Management
- Identity Management
- Access Management

Data Security
- Data Loss Prevention
- Data Entitlement Management
- Encryption & Key Lifecycle Management
- Messaging Security
- E-mail Security
- Database Monitoring & Protection
- Data Masking

Application Security
- Application Vulnerability Scanning
- Web Application Firewall
- Web / URL Filtering
- Access & Entitlement Management
- SOA Security

Infrastructure Security
- Vulnerability Assessment
- Virtual System Security
- Endpoint Protection
- Threat Analysis
- Security Event Management
- Managed Mobility Svcs
- Intrusion Prevention System
- Firewall, IDS/IPS MFS Management
- Mainframe Security Audit, Admin & Compliance
- Security Configuration & Patch Management

Physical Security

TREND MICRO · symantec. · FIDELIS · DSD · juniper · Check Point · cisco · BlueCoat · RAPID7 · websense · VERDASYS · MODULO Solutions for GRC