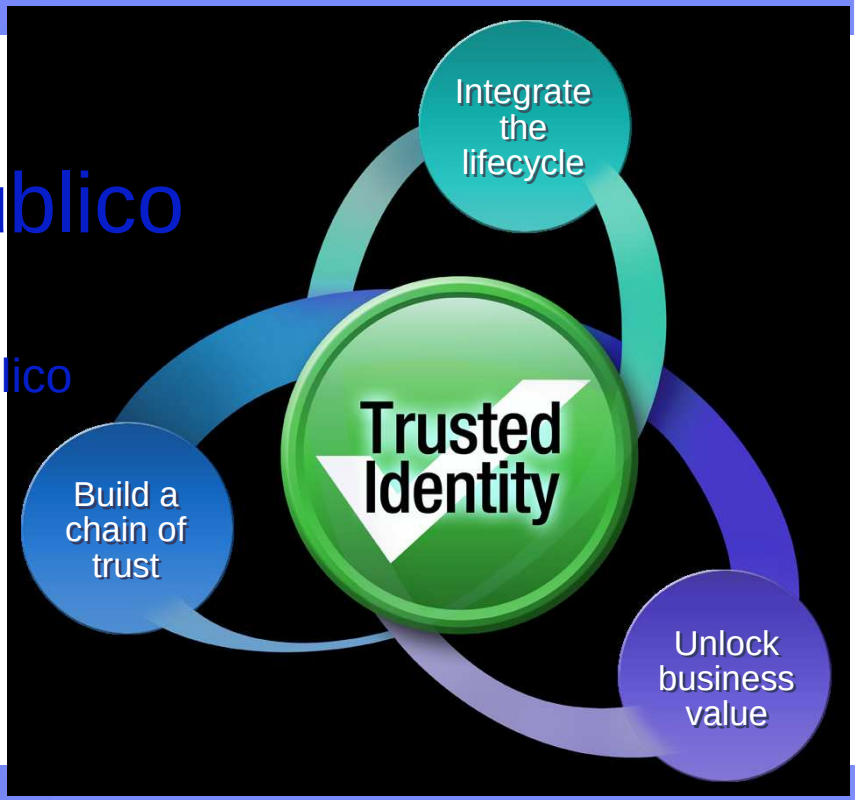
IBM

Seguridad en el Sector Público

Soluciones de identidad segura en Sector Público



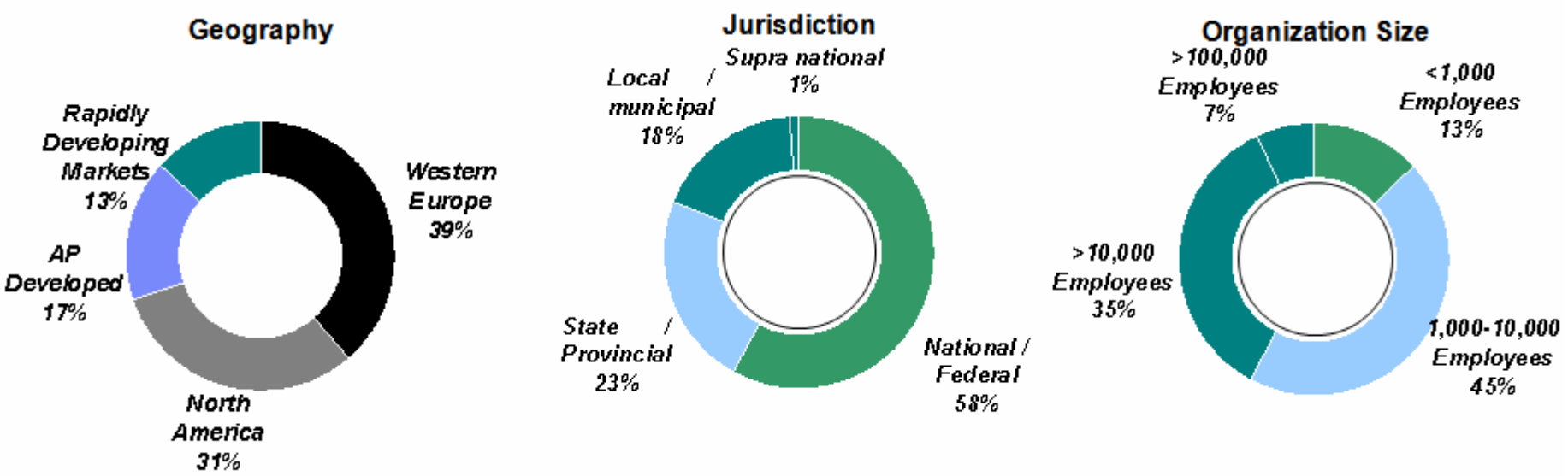
Javier Arcos Yagüe
Líder de Soluciones para el Sector Público,
IBM Software, SPGI IMT

IBM Institute for Business Value

Global Government

Hemos entrevistado 287 CIOs del sector público de un total en la encuesta de 2,500 CIOs

Este estudio representa organizaciones del sector público de diferentes tamaño en 48 países, operando a diferentes niveles jurisdiccionales



Se entrevistron a CIOs personalmente en sus oficinas, **durante Enero-Abril 2009**. La idea era la de entender los **problemas a los que se enfrentan y la prioridades en sus roles y en la función de IT** para llevarla a cabo.

La mayor comparación es con las respuestas con sus homonimos en el sector privado. Tambien hemos comparado las respuestas entre niveles de gobiernos nacionales, autonomicos y locales. Se han identificado los **“líderes en ejecución”.**

Los retos y oportunidades a los que se enfrentan los CIOs del sector público varían en función de su organización, misión, responsabilidad a pesar de que muchos son compartidos

Gobierno Nacional / Central	Gobierno Regional / Estatal	Gobierno Municipal / Estatal
Desarrollar la **modernización del gobierno** . (ej. Gobierno 2.0) Necesidad de una **respuesta a los requerimientos regulatorios** y riesgos, incluyendo **la seguridad de los datos y la privacidad**	**Intensa presión por la reducción en los presupuestos** debido a la desaceleración económica Necesidad creciente de una **colaboración efectiva – a niveles nacionales y locales**	**Crecimiento de la importancia económica de las ciudades** **Necesidad de usar el IT para proveer de servicios más flexibles para los ciudadanos**

A todos los niveles de Gobierno

Demanda de una **mayor transparencia de los responsables públicos y de los políticos**

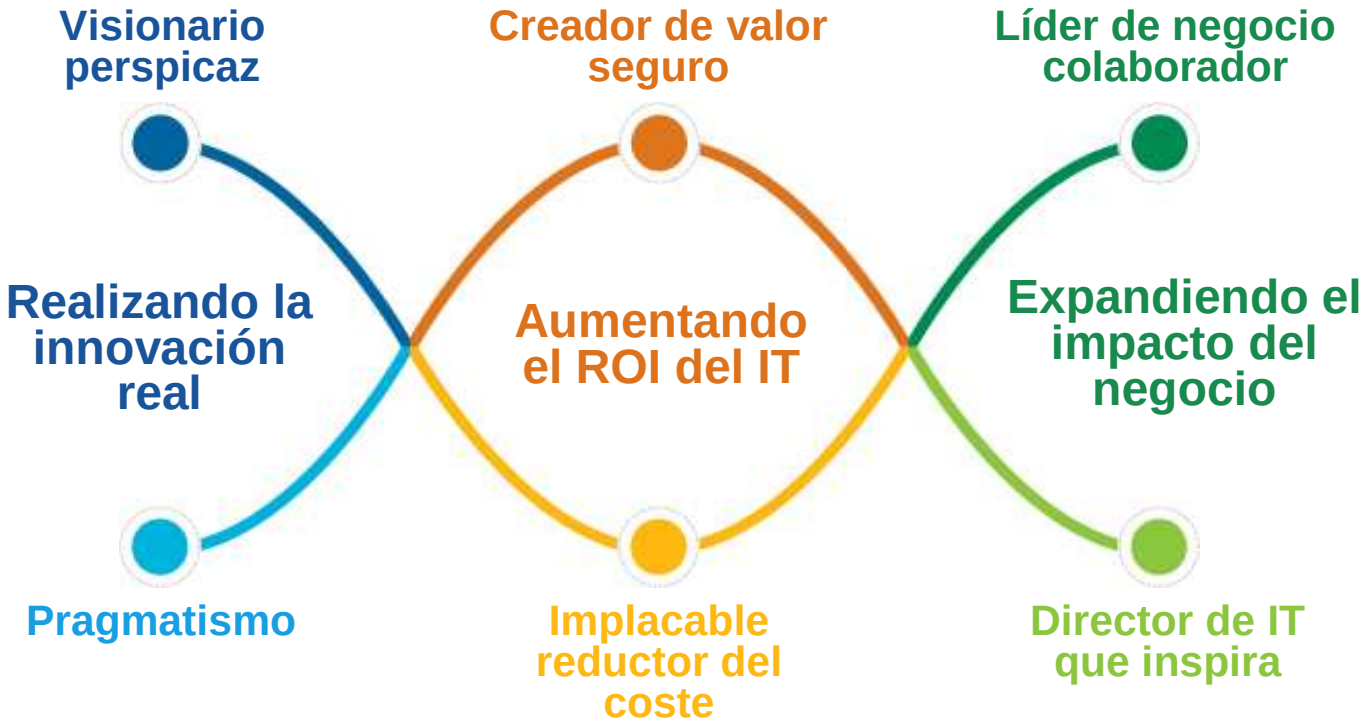
Necesidad **de gestionar y manejar un gran volumen creciente de información para proveer una mayores y mejores servicios coordinados** de los gobiernos

Presión creciente de IT para proveer de eficiencias en costes

Racionalización del IT

Eficiencias operacionales, ej., servicios compartidos, outsourcing, insourcing , offshoring, integración de servicios

Los CIOs que más éxito tienen reúnen tres pares de roles que parecen contradictorios en si pero que son actualmente complementarios



Mediante la integración de estos tres pares de roles, los CIOS realizan la innovación real, e incrementan el ROI del IT y expande su impacto en el negocio

Conclusiones de la voz del CIO en el Sector Publico

- **CIOs del sector público tienen la oportunidad de definirse a sí mismos en un nuevo papel - en el corazón de la transformación del Gobierno**. Sin embargo, los CIO del sector público se ven amenazados por una creciente demanda de los servicios públicos y los recortes presupuestarios futuros. La naturaleza de las organizaciones del sector público puede poner muchos obstáculos en el camino del cambio.

- **Los CIOs del sector público se están preparando para afrontar estos reto**s – reportan un interés en las soluciones con visión de futuro y están trabajando cada vez más con la alta dirección - más de lo que los CIOs del sector privado. El progreso es especialmente avanzada a nivel sub nacional, donde administraciones locales y organizaciones estatales y regionales están utilizando el IT cada vez más para prestar servicios a los ciudadanos.

- Sin embargo, **existen diferencias entre las expectativas, la aspiración y la entrega; progresos notables y constantes en muchos casos y planes con visión de futuro está aún por realizarse**. En todos los casos hay **un largo camino que recorrer para obtener los beneficios totales que prometen las tecnologías de la información y comunicación.**

La necesidad del CIOs del sector público ahora para cumplir tres objetivos:
Hacer de la innovación real - en estrecha colaboración con las áreas del programa para ofrecer un rendimiento mejorado mediante el uso de las TI
Elevar el rendimiento de la inversión de la información y la tecnología - crear valor a través de una mejor utilización de la información y administrar más eficientemente los costos de TI.
Expandir impacto de la misión - convencer a los dirigentes del sector político y público que es una misión crítica para los retos del futuro y el cultivo de las habilidades de TI para cumplir con la función de TI mejorada.

La encuesta pone de relieve los factores de seguridad como uno de los desafíos más importantes a los que enfrentan los CIOs en el sector público

"IT es la única bala de plata que los responsables del sector público tienen para proveer de servicios más eficientes a pesar de los recursos limitados"

Public sector CIO, Local / Municipal Government, U.K.

Obtener el derecho básico, garantizar que los datos son seguros y confiables a través de una gestión eficaz de datos y la entrega de la rutina de operaciones de TI de manera eficaz, para liberar tiempo CIO para las partes más estratégica de la función.

Sample Size (Overall) = 2598, Valid Cases (Overall) = 2598, Sample Size (Global Govt.) = 287, Valid Cases (Global Govt.) = 287

IBM Research 2009

IBM Research 2009 - Seguridad

La vulnerabilidad y las amenazas están cambiando: las pérdidas de información y datos debidas a la falta de cuidado y mala conducta interna se duplicó en 1H 2008. La pérdida de datos y el robo alcanzó un máximo histórico en 2008.

La defensa perimetral tradicional se ha convertido en menos eficaz, debido al rápido crecimiento del volumen de información, una rápida adopción de las nuevas tecnologías (Web 2.0, el acceso ubicuo, SaaS y el cloud computing) y la necesidad de flexibilidad para colaborar a través de fronteras de empresa.

Las tecnologías y políticas de seguridad estarán mas adaptadas y complementadas con un solución multicapa de seguridad para la contención que se extiende sobre la plataforma, la arquitectura orientada nubes de computación / centro de datos, middleware y servicios, la colaboración y comunidad para proteger los objetos de negocio individuales (p.e., registros de clientes).

La seguridad en la información empieza con los activos críticos de negocio y procesos de una empresa. Las necesidades más significativas son la implementación de procesos de gobierno para una identificación de confianza sistemática y una continua monitorización y auditoría.

Las violaciones de la seguridad y el fraude son continuas. Nuevas tecnologías de detección del fraude emergerán como un complemento a las tecnologías existentes hoy que proveen de alertas tempranas de seguridad acerca de mayores brechas de seguridad y transacciones fraudulentas.

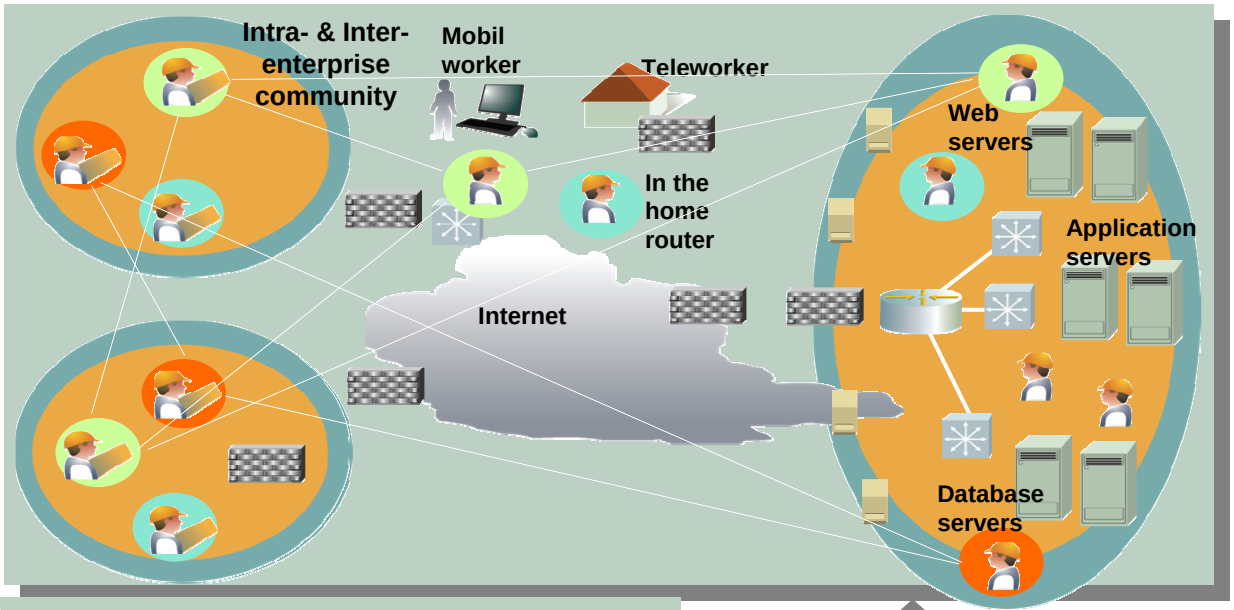
IBM Research 2009 - Seguridad

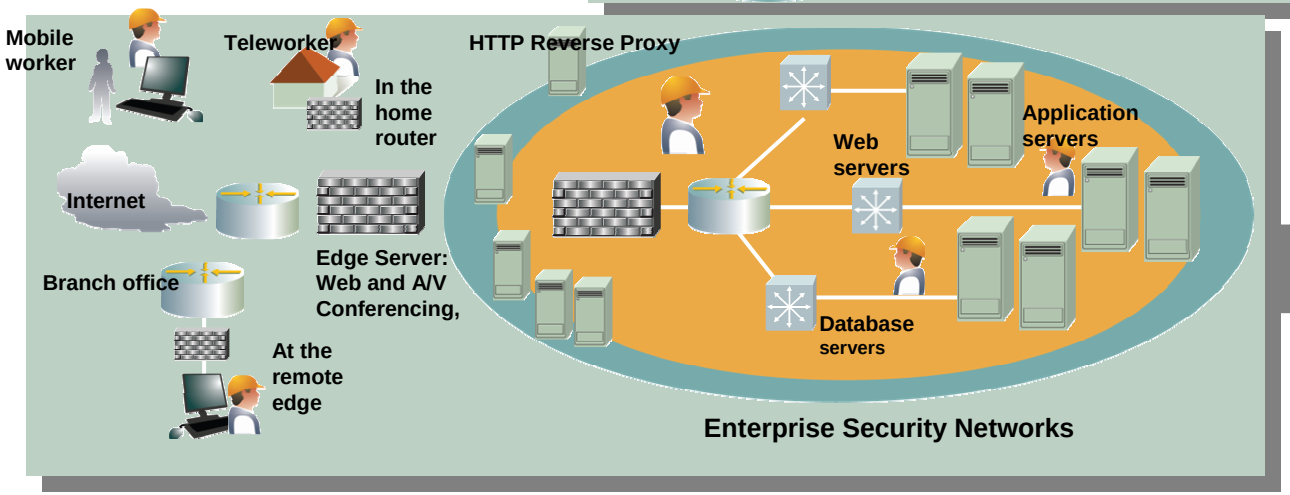
Somos testigos de la rápida desaparición de la seguridad perimetral tradicional en la empresa debido al modelo de soluciones de múltiples puntos de seguridad se está desmoronando

Motivos para abrir el perímetro de la empresa:

- **Outsourcing (SO & BPO)**
- **Colaboraciones a través de organizaciones y con otros organismos / empresas**
- **Trabajadores móviles**
- **Acceso Ubicuo y**
- **Web 2.0**

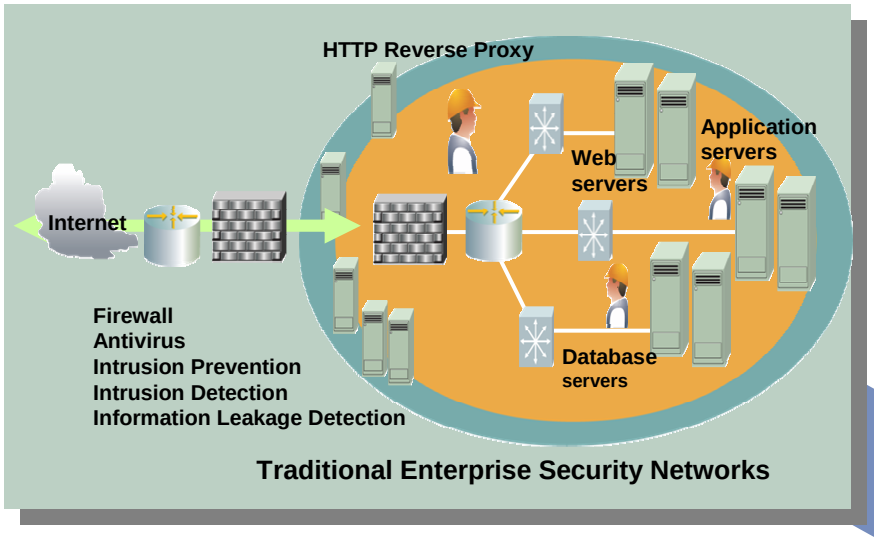
- **Cloud Computing, SaaS**





IBM Research 2009 - Seguridad

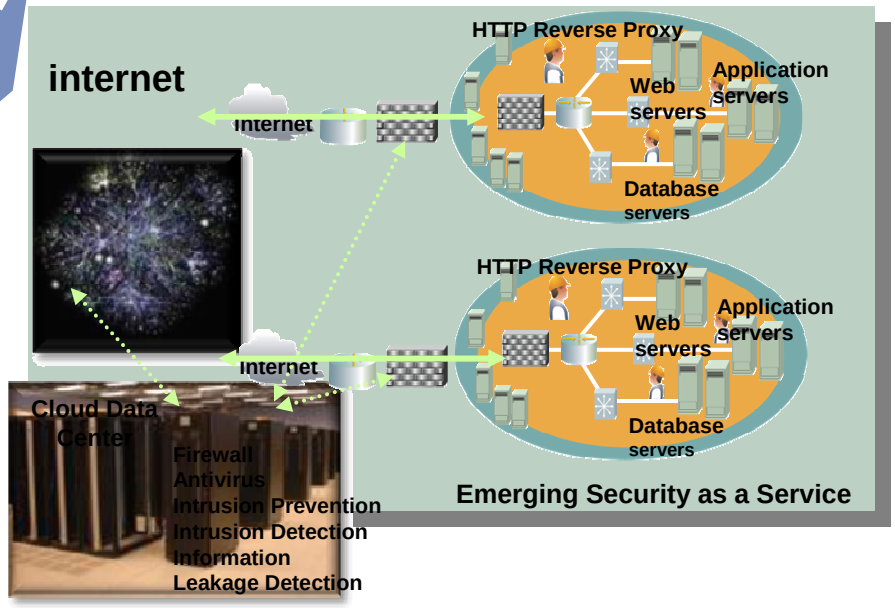
Seguridad / Conformidad como un servicio es una nueva oportunidad de crecimiento para Cloud computing



Metodologías para el nivel de la empresa de seguridad y cumplimiento en el proceso de negocio y de TI son onerosas y complejas: Las soluciones desarrolladas internamente a menudo son ad hoc y propensas a errores

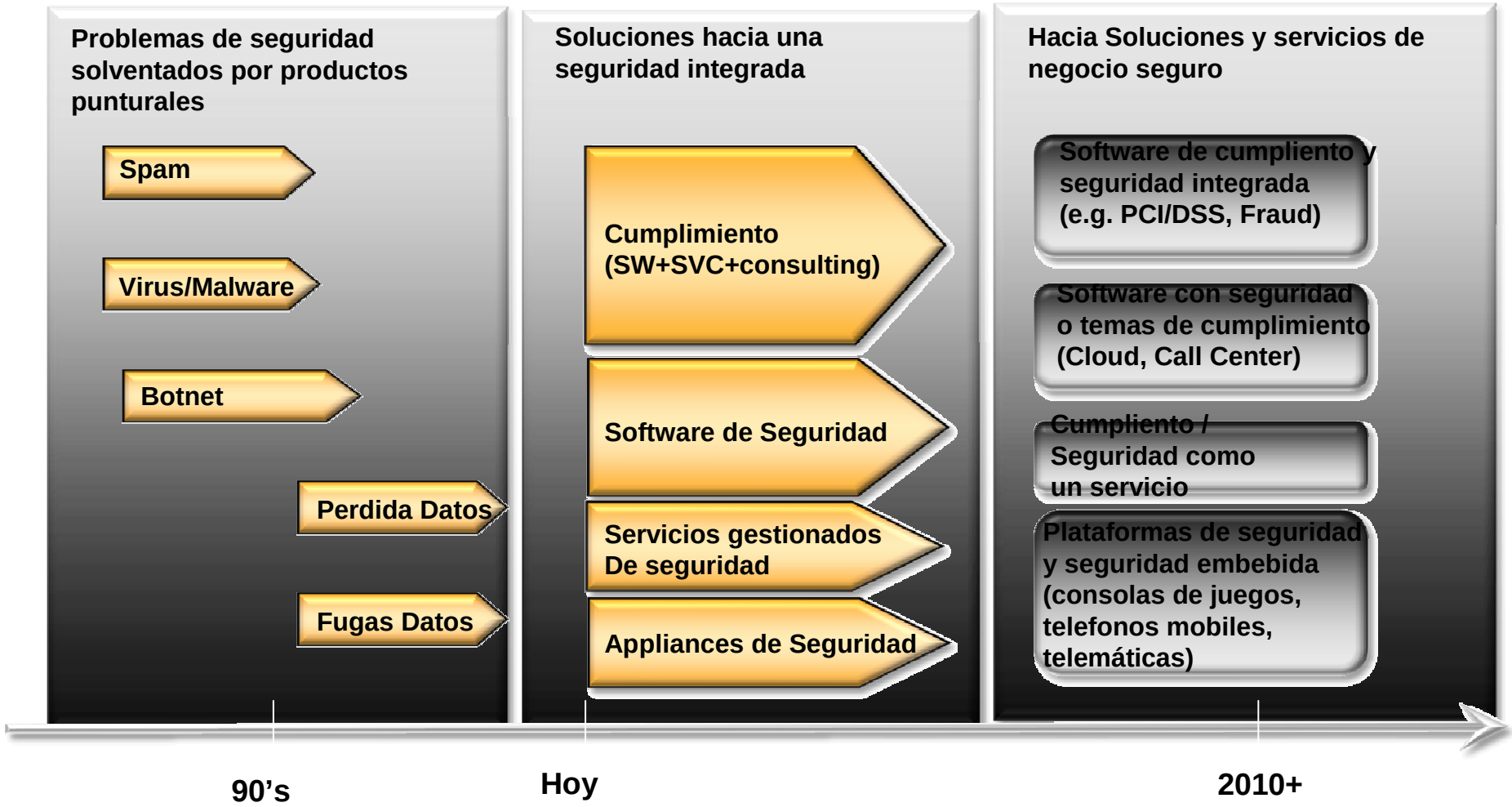
Mover la seguridad y el cumplimiento en cloud (como un servicio), cerca de carga puede implicar obligaciones reglamentarias:

- **Los primeros serán los que pueden aprovechar los efectos de escala para un conocimiento superior (por ejemplo, la señal es débil y detectores de alerta temprana)**
- **Las mejores prácticas garantizadas y diseño por expertos en la materia**
- **Rendimiento coste óptimo para la ejecución de la seguridad y el cumplimiento de las cargas de trabajo relacionadas**
- **Facilita la construcción de la inteligencia colaborativa en la realización de detección, alerta temprana, la prevención y remediación de vulnerabilidades de seguridad y control de defectos de negocios / violaciones**



IBM Research 2009 - Seguridad

El entorno de seguridad evolucionará hacia soluciones integradas que proveerán del cumplimiento y evolucionaran en servicios en nube "Cloud"



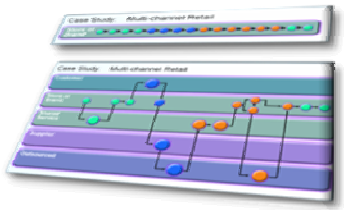
IBM Research 2009 - Seguridad

La seguridad en la información empieza con activos de negocio y procesos corporativos críticos. Las regulaciones actuales (e.j. SOX 404, SAS 70, PCI/DSS and HIPAA) tienen requerimientos específicos en la auditoría / control de negocio para asegurar el cumplimiento de la seguridad en la información

Identificación sistemática de los activos de la empresa (de acoplamiento flexible con unidades de negocio potencialmente opuestas objetivos de negocio gestionado pe. Por los trabajadores regulares, los contratistas y socios comerciales) y la aplicación de una protección afinada y apropiada en toda la empresa, ha sido un gran reto para muchas empresas

IBM Research 2009 - Seguridad

La contención y vigilancia se produce en varios niveles, cada uno de los cuales ofrecen capacidades de aislamiento adicional, tanto de externas como internas vulnerabilidades.



SOA

SCADA

Data Center

Internet

Colaboración y comunidad

SOA, Informacion

Middleware (DBMS, App Server)

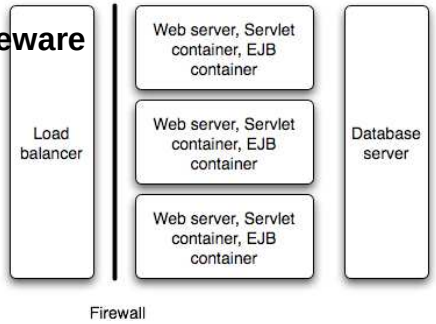
Data Center/Network/Cloud

Plataforma

Comunidad

Red de Negocio y social

Middleware Stack



Consola de juego

Smart phone

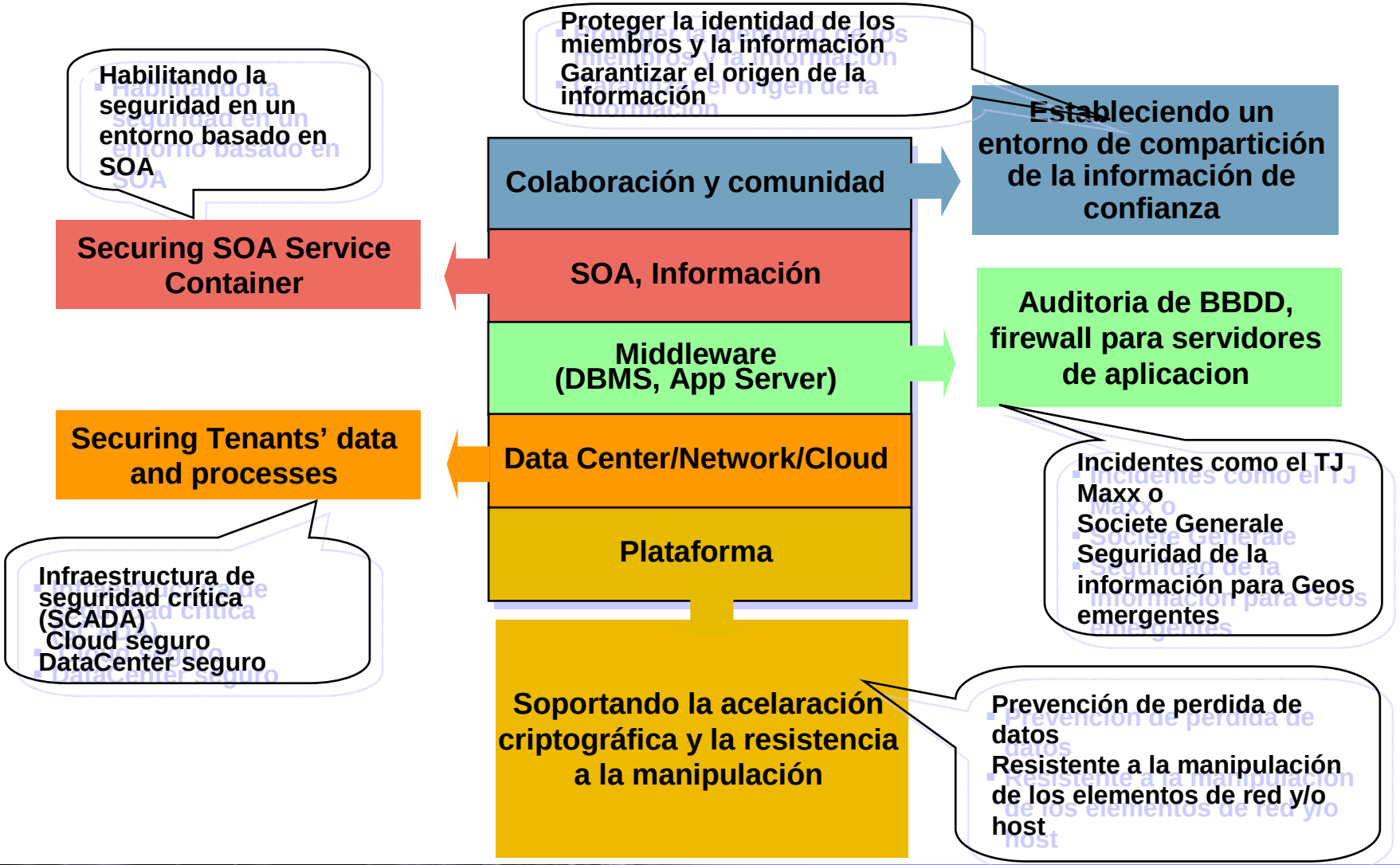
Telematicos

Cliente

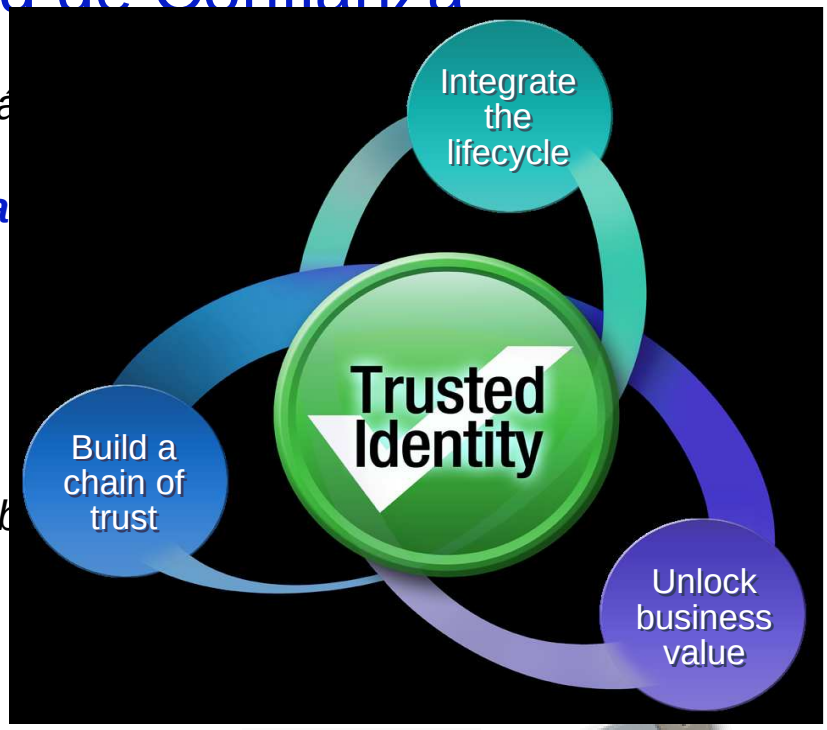
Servidor

IBM Research 2009 - Seguridad

La contención y vigilancia se produce en varios niveles, cada uno de los cuales ofrecen capacidades de aislamiento adicional, tanto de externas como internas vulnerabilidades.



Solución de gestión de la Identidad de Confianza



•*Las soluciones para la gestión de la identidad se está convirtiendo en un* ***nuevo punto de influencia en la economía global, donde la confianza en la identidad y en los credenciales de identificación son esenciales*** *para todas las transacciones.*

•*Los* ***Gobiernos necesitan dar respuesta a los requisitos establecidos por la UE para afrontar las amenazas cibernéticas así como los esfuerzos nacionales para fortalecer la seguridad*** *contra el robo de identidad, el fraude, la delincuencia y el terrorismo.*

• ***La identidad de confianza esta focalizada en las personas y la identidad, incluye también las aplicaciones y los sistemas que requieren protección*** *utilizando todos los componentes del Framework de IBM.*

Identidad en Gobierno

Licencias, permisos, documentos de viaje, identificación de los ciudadanos, los beneficios de salud ,

- ***Reducir el fraude en las prestaciones sociales***
- ***Mejorar los servicios a los ciudadanos***
- ***Mejorar la seguridad pública***

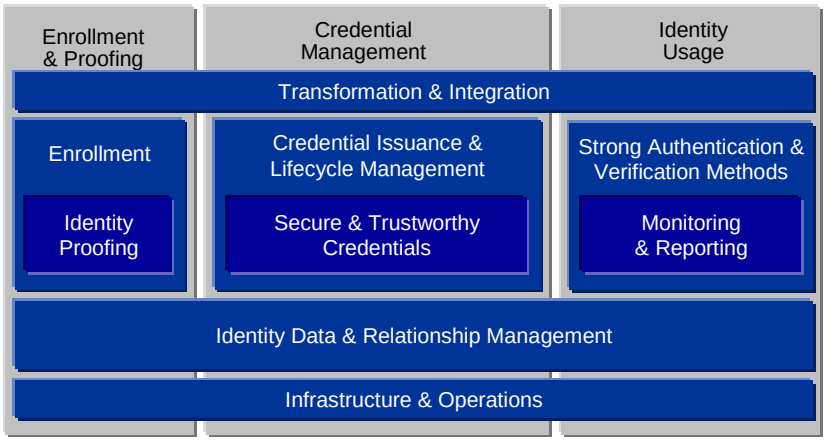
¿Qué es la identidad de confianza?

El enfoque de IBM se basa en la gestión estratégica del riesgo desde el principio hasta el final y a través de todas las áreas dentro de una organización .

Identidad de confianza

Identidad de confianza

La identidad de confianza esta focalizada en las personas y la identidad, implica las aplicaciones y los sistemas que requieren protección utilizando todos los componentes del Framework de IBM.



¿Cual es una iniciativa de Identidad de Confianza?

- Casos en los que se necesita de una autenticación fuerte, más allá de un simple login y password para asegurar el acceso a las aplicaciones de eGobierno:
  - Long on + password + presencia de un identificador RFID
  - Long on + un password de una vez provistos por un token (e.i. RSA key) o por SMS
  - Long on + certificado o clave almacenado en chips inteligentes embebidos en targetas, USBkeys, teléfono móvil,,..
  - Lo anterior puede incluir biometria (huella táctil, voz, cara, piel)
  - Con o sin mecanismo de eFirma

Y/O

- Pruebas de identidad
  - Identificación biométrica

    > Estar seguro que detrás de un un conjunto de datos biométircos existe una unica identidad
  - Análisis de datos para prevenir el fraude en aplicaciones para identidad segura como documentos o beneficios sociales

    >analizando datos recogidos durante el proceso de dar de alta en la aplicación, comprobarlo con listas externas o listas negras

Y/O

- Combinanción de acceso logico y físico
  - Algunas aplicaciones muy sensitivas requieren usuarios bajo estas premisas

Y/O

- Credenciales de ID seguro de ciudadanos para identificacion nacional, documentos de viajes basados en targetas inteligentes con o sin biometria – provision y verificacion del ID
- Gestion de aduanas en aeropuertos, puertos y puntos dentrada en tierra y puertos

¿En qué consiste una fuerte identificación?

Métodos de autenticación segura caen dentro de una de estas tres categorias

Algo que el usuario "Sabe"

- Password
- Automated teller machine (ATM) pin
- Question and answer
- Image selection
- Grid pattern

Algo que el usuario "Tiene"

- Smart card
- Token
- Mobile device
- Grid card
- Personal computer

Algo que el usuario "es" o "hace"

- Huella táctil
- Retina
- Cara
- Voz

Cada factor de autenticación tiene una debilidad inherente que puede ser explotada

Una fuerte identificación puede ser conseguida usando dos o más de los factores anteriores de autenticación

Solución de Gestión de la Identidad de Confianza

Gestión de la identidad

PERSON

Request
Digital Identity

PROVISION OF DIGITAL IDENTITY

Primarily user IDs and passwords

DIGITAL WORLD USAGE

Use digital identity for online authentication

MANAGEMENT

Manage and monitor digital credentials

Identidad de confianza

Request
Trusted Identity

IDENTITY DATA AND RELATIONSHIP MANAGEMENT

Provides a single view of a person and manages their identity data and associated relationships

3

1

ENROLLMENT

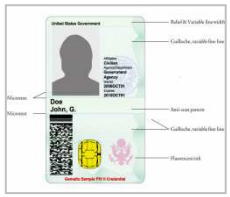
Collect biometrics, breeder documents, biographic information

PROOFING

Validate biographic and biometric information

2

CREDENTIAL ISSUANCE



Biometrics, smart chips, certificates, OTPs, etc.

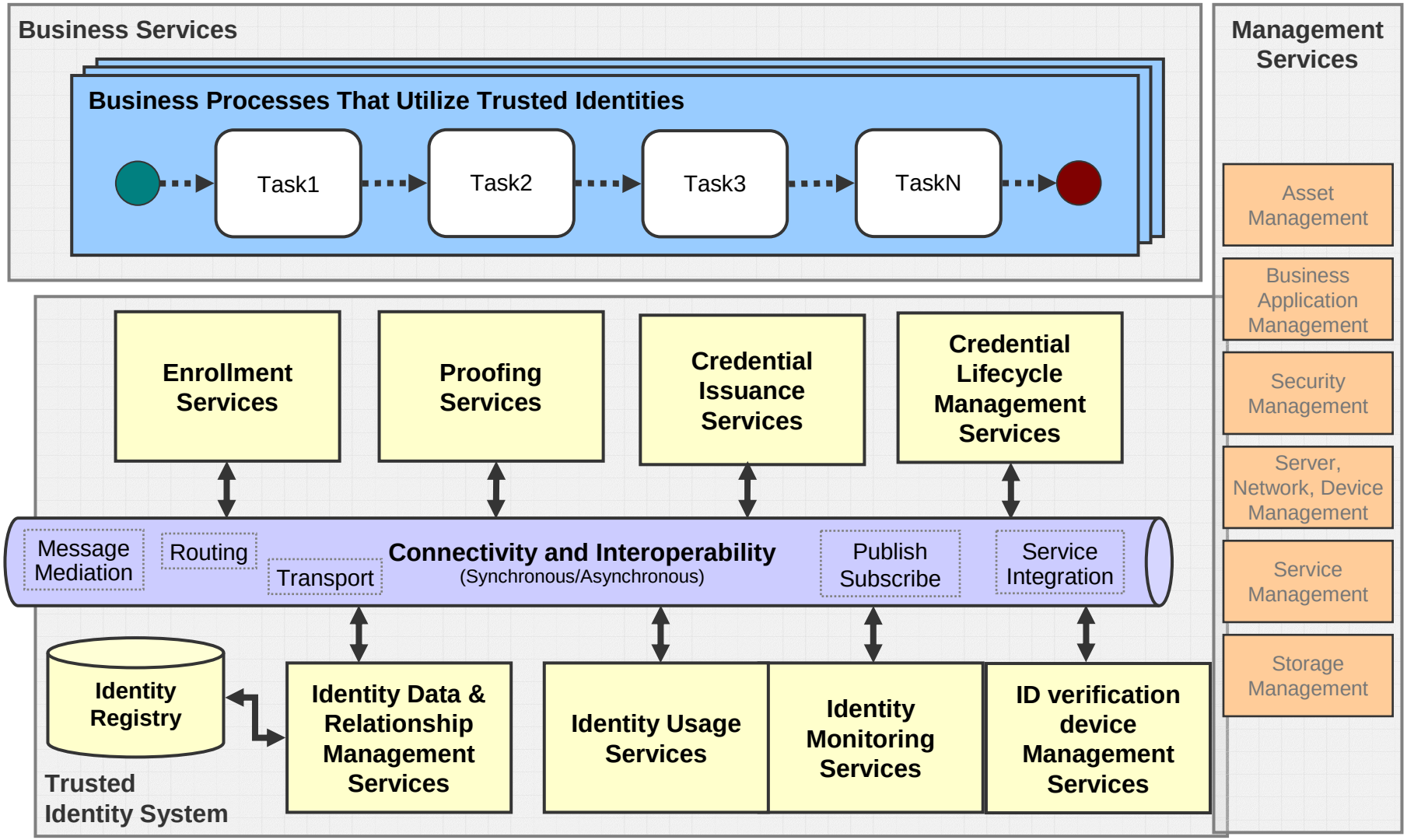
DIGITAL & PHYSICAL WORLD USAGE

Strong and multi-factor authentication

MANAGEMENT

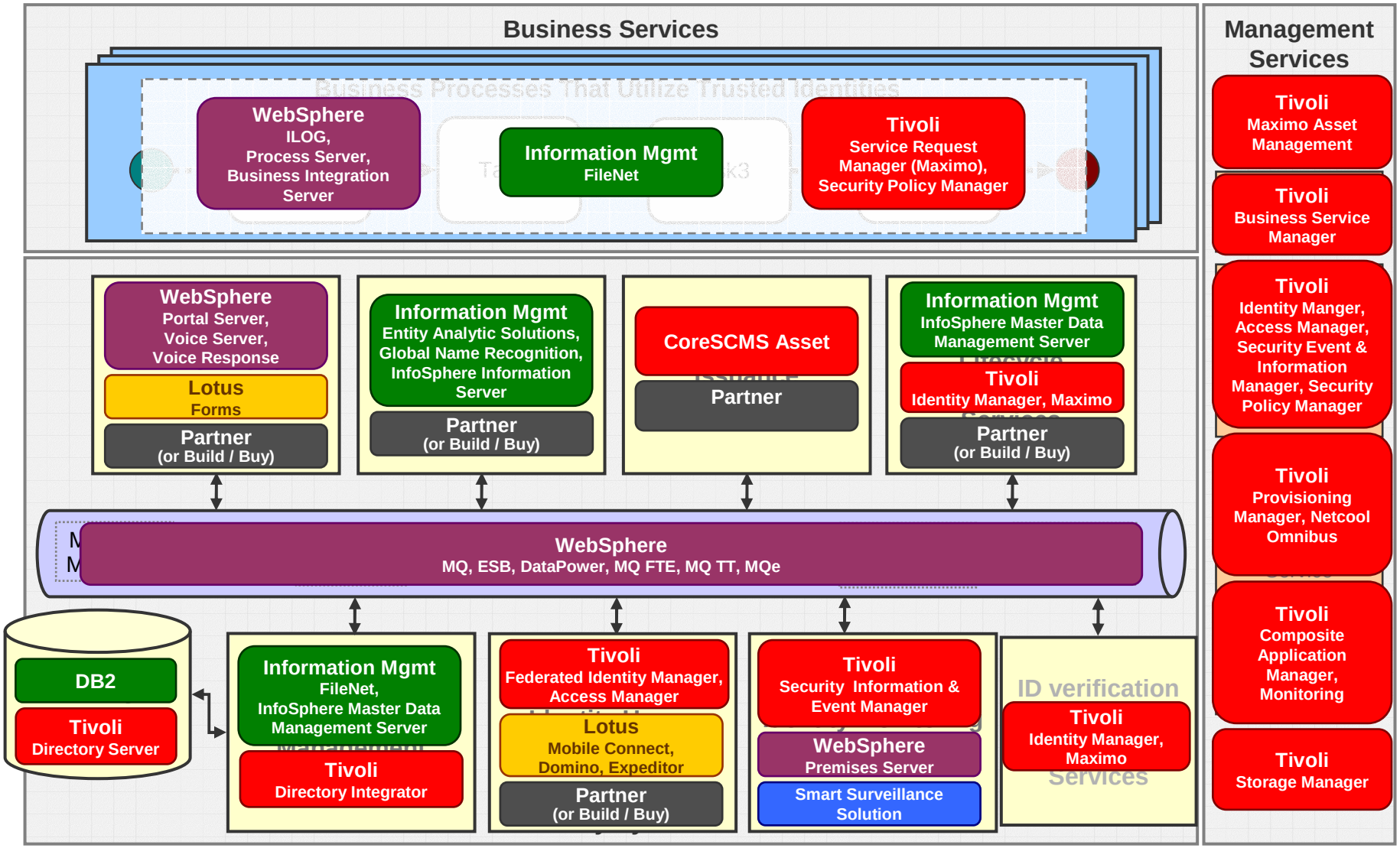
Manage and monitor trusted credentials

Arquitectura de la solución de identidad segura



Enlace con productos IBM

*Tivoli GoKit Version 1.0 3/4/2009 Page 47



Mayores Referencias

eGov services	Gilfam – paperless land registry (FR)
Employee ID assurance	American Healthcare System
Secure licensing	Canadian Driver Licensing Agency
Complex eID project	UK Driver and Vehicle Licensing Agency project
Secure Management of Asylum Seekers	DIMA Immigration Australia
Airport eGates	eGates at UK airport
2 Factor Authentication	Polkomtel - major Polish telecom provider
ePassports	Seva ePassport (India)
Unemployment Benefits	French Employment Hub

Agencia de permisos de conducir y vehículos de UK

Desafío:

Desarrollar y fabricar un nuevo permiso de conducir de alta seguridad que se ajustase plenamente a los requisitos de seguridad de la licencia de conducir bajo las Directivas de la UE, y también atender a las necesidades de evolución futura.

Solución:

IBM trabajó como socios estratégicos DVLA para especificar, administrar e implementar una solución total para el diseño y la fabricación de la licencia. Los consultores de IBM reunió a un proveedor suizo de las tarjetas de seguro, un proveedor alemán de máquinas de fabricación de tarjetas y de la investigación original y de las capacidades de desarrollo de sus propios laboratorios.

Beneficios:

Una licencia de conducir de alta seguridad, el gobierno del Reino Unido y satisfacer los requisitos de la UE

- servicio de un gobierno compartido proporcionando el máximo valor para los contribuyentes
- Continuidad del servicio público:
- 24 horas de respuesta en términos de la producción de tarjetas para cada controlador de residuos de transacciones
- El papel se redujo de 30 % a menos del 1%.

"IBM nos ha ayudado a poner en marcha una plataforma que puede ser aprovechada para entregar beneficios a los departamentos gubernamentales. Como los requisitos de la nueva tarjeta venga estaremos trabajando con IBM para ayudar a nuestros clientes de otras áreas de gobierno hasta el final a un proceso completo desde la definición inicial de las necesidades de la producción final "

-Griffiths leuan, Finanzas y Director de Estrategia en DVLA