Deloitte.

Gobernanza en la Gestión de Identidades y Accesos

Seminario de IBM: Un paso más allá en la gestión de identidades y accesos

4 de noviembre de 2014

Índice

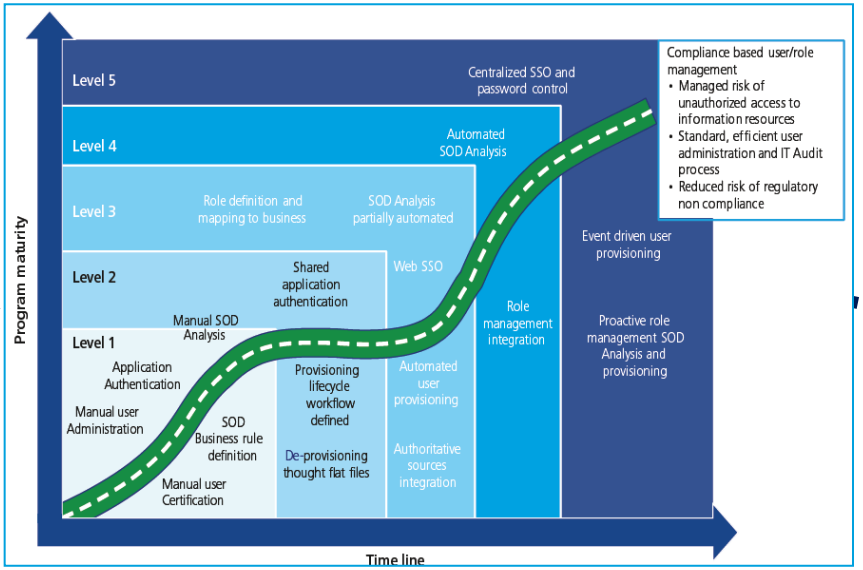
1. El universo del Gobierno de Identidades y Accesos

Visión y Estrategia

¿Quién puede acceder y desde dónde?

¿Cuáles son las políticas a validar?

¿Cómo medir la efectividad de controles de acceso?



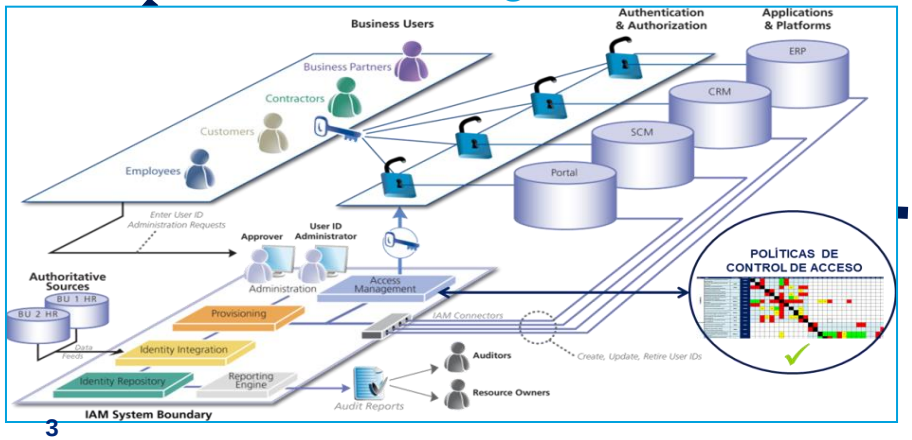
¿Cómo identificar incompatibilidades entre permisos?

¿Cómo verificar los incumplimientos de políticas de acceso?

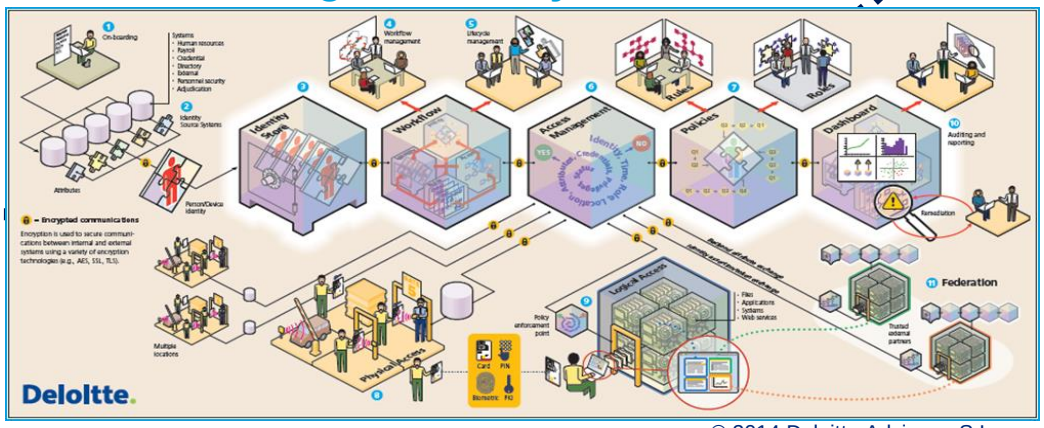
¿Cuál es el rol del negocio en el control de acceso?

¿Cómo avanzar hacia un **marco de gobierno en IAM** repetible, medible, eficiente y adaptado a las necesidades de la organización?

Tecnología



Organización y Procesos



2. Aprendiendo de los errores del pasado…

Debe diseñarse una estrategia IAM a la medida de cada organización

- La **integración** con otros procesos es clave
- **¿Qué quiero conseguir?**

No es un proceso exclusivamente tecnológico

- **Alineamiento con políticas** globales de seguridad
- Necesidad de **implicación de áreas no-IT**
- **Requisitos normativos y legales** a considerar

Es crucial contar con un partner solvente, pero el camino debe recorrerlo uno mismo…

- Contar con partners expertos es una palanca para lograr éxito en un menor tiempo
- Adicionalmente, deben valorarse las capacidades internas que deben incorporarse

Equilibrio entre coste y beneficio

- **Beneficio rápido** para ser viable en el medio y largo plazo.
- Evitar un **apalancamiento excesivo en el cumplimiento** legal

3. Tendencias actuales y futuras en el Gobierno IAM

"The Extended Enterprise"

Criterios de decisión de la organización

- **Mínimo impacto** en los sistemas y redes
- **Facilidad de uso** para el usuario final
- **Grado de exposición** de los servicios de TI
- **Reutilización de las identidades** locales de las filiales y de terceras partes confiables
- **Facilidad para la gestión**, configuración y provisión

La casuística del *extended enterprise*

- **Nuevas necesidades**: usuarios en movilidad, flexibilidad y agilidad en la adquisición y venta de filiales.
- **Heterogeneidad de sistemas de TI**: propios, externalizados y en *cloud*, corporativos y de filiales.
- **Unificación de accesos** en la medida de lo posible y mismos criterios y requisitos para nuevos sistemas.
- **Solución fácilmente integrable**: mecanismos y estándares que sean fácilmente integrables en sistemas actuales.
- **Escalabilidad**: modelos de acceso para la provisión de nuevos servicios y desarrollos que se integren con los ya establecidos.

3. Tendencias actuales y futuras en el Gobierno IAM

"The Extended Enterprise" (continuación)

¿QUIÉN?

Usuarios

Corporativos vs. No corporativos

Externos Clientes Administradores

¿DESDE DÓNDE?

Dispositivos

Ordenadores
Portátiles
Móviles y *tablets*

Corporativos
No Corporativos
Particulares

Ubicaciones

Interior de la empresa
Exterior de la empresa
Desde filiales

¿A QUÉ?

Aplicaciones

Corporativas

Negocio

Colaboración

Soporte y desarrollo

¿POR QUÉ?

Evidencias

- Workflow de solicitud y aprobación
- Trazabilidad del permiso concedido
- Informes de auditoría

¿ES CORRECTO?

Criterios de decisión

- Correlación de eventos ante potenciales situaciones de fraude
- Trazabilidad del acceso al sistema
- Indicadores de riesgo.
- Mecanismos de autenticación basados en factor adicional.

4. El reto del Gobierno de Identidades y Accesos

Requisitos del negocio en el Gobierno de identidades digitales

- **Visión global** de las múltiples **"identidades digitales"** de empleados y usuarios externos
- **Minimizar** carga de trabajo en **Help Desk** debida a la gestión de cuentas de usuario y contraseñas
- **Involucrar** a las áreas de **negocio** (RRHH, Organización, responsables de área/oficina,…) en la autorización y vigencia de los permisos
- Mecanizar el **cumplimiento** de las **mismas políticas** de control de acceso en múltiples sistemas *(segregación de funciones, usuarios "huérfanos" o inactivos,…)*
- **Trazabilidad** centralizada e **histórica** de los accesos que dé respuesta a las auditorías e investigaciones forenses
- Asegurar el **cumplimiento regulatorio y legal** y **poder demostrarlo** ante terceros

Requisitos del negocio en la Gestión de acceso a recursos TIC

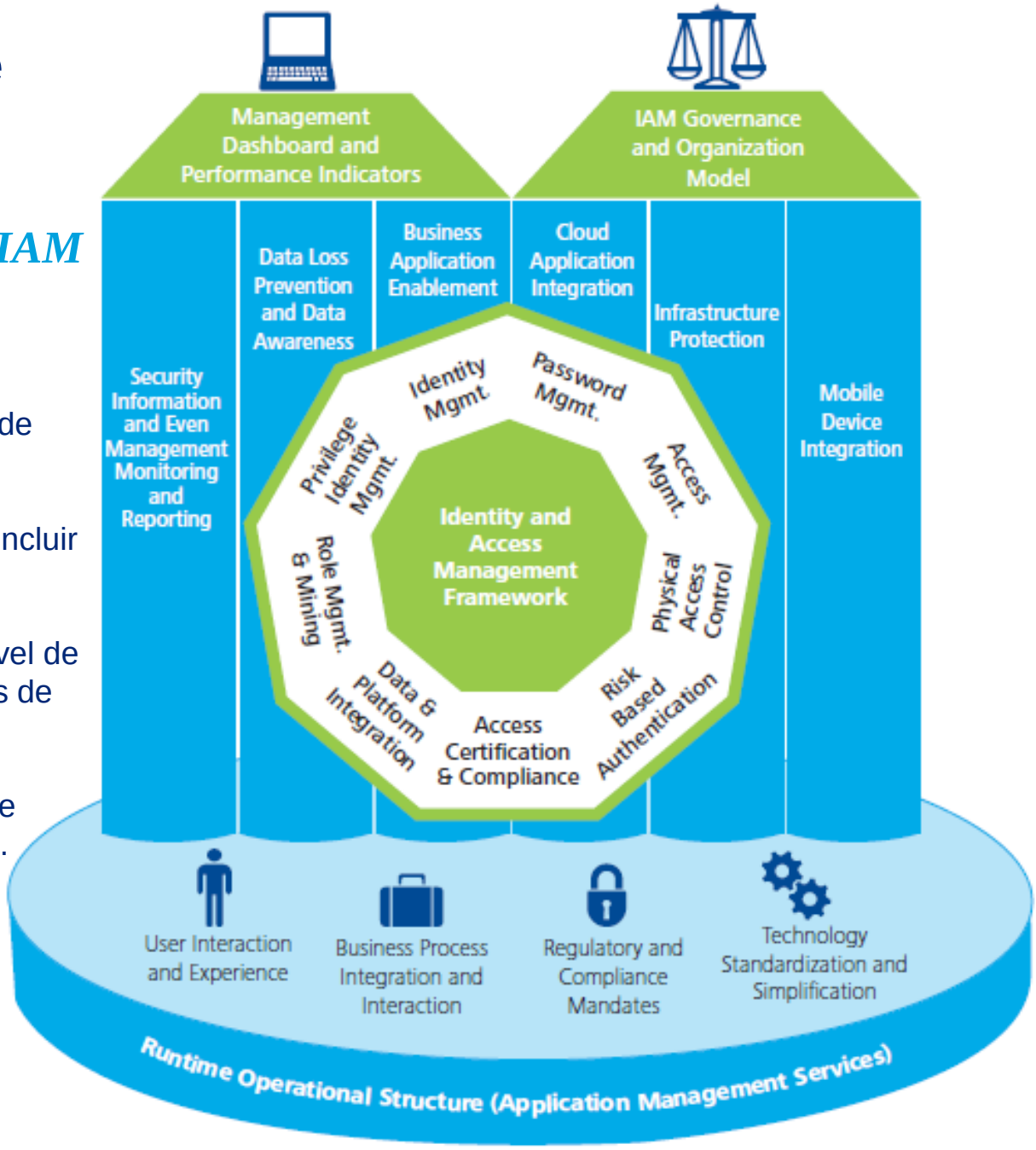
- Mayor **permeabilidad** ante procesos de **integración y separación** de empresas y entornos informáticos
- **Unificar y simplificar** los mecanismos de acceso a los diferentes sistemas, **sin comprometer la seguridad**
- Permitir **accesos remotos** cumpliendo las políticas e independientemente de su ubicación física
- Mayor control en la **concesión y revocación** puntual de accesos a trabajadores **eventuales**
- Integrar los **desarrollos propios** de software en el modelo de control de acceso corporativo
- **Evitar situaciones de fraude** en el acceso indebido a los sistemas de información

Garantizar que se cumplen los **requerimientos legales**, de **negocio** y de las áreas de **Organización**, **Auditoría Interna** y **Seguridad TIC** en relación a la autorización de acceso a los sistemas de la compañía.

4. El reto del Gobierno de Identidades y Accesos

Factores clave para un Gobierno IAM efectivo y eficiente:

- **Orientado al negocio** (políticas, marcos de control interno, cuadros de mando).
- **Experiencia de usuario mejorada** para incluir los roles de negocio.
- **Monitorización y reporte flexible** y al nivel de detalle adecuado (acorde a las exigencias de control interno de la entidad).
- **Reingeniería de procesos** de **RRHH** y de habilitación de funciones para el **negocio**.
- ***Compliance* continuo** a un coste reducido.



4. El reto del Gobierno de Identidades y Accesos

¿Por dónde empezar?

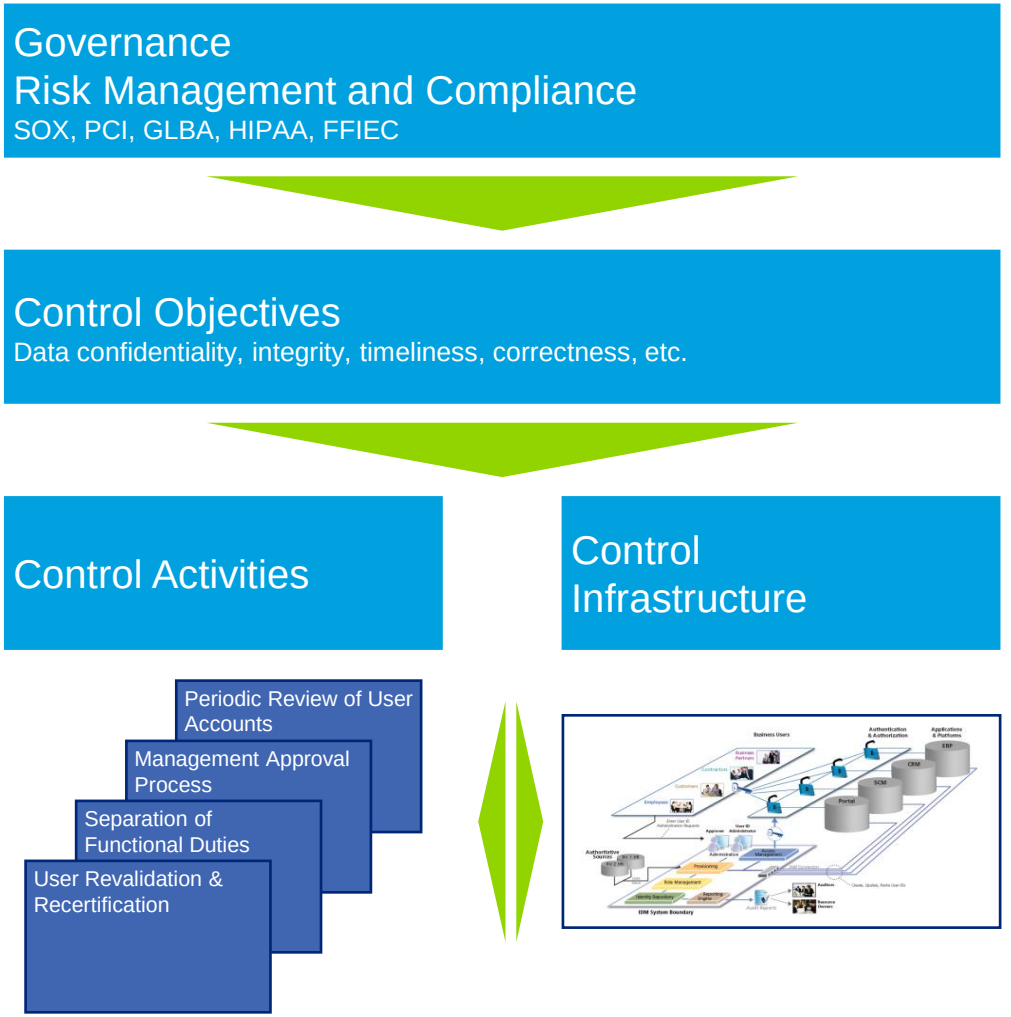
Políticas	• ¿Se conoce quién accede a las aplicaciones de negocio, y puede demostrarse? • ¿La información presentada a los reponsables de negocio para aprobar los permisos es suficientemente completa?
Procesos	• ¿Se analiza la viabilidad de los permisos asignados basándose en necesidades de negocio y funciones del puesto? • ¿El tiempo de concesión o revocación de accesos puede medirse? ¿Es acorde a lo que espera el negocio?
Autorización basada en roles	• ¿Se identifican y reportan problemas de segregación de funciones en las auditorías? • ¿Se aplican estas mismas restricciones a los usuarios externos y usuarios administradores?
Administración de usuarios	• ¿Cómo se utilizan y justifican los accesos mediante usuarios privilegiados? ¿Pueden asociarse a personas concretas? • ¿Cuánto tiempo emplea Help Desk en las tareas habituales de (des)activación de password a mano?

4. El reto del Gobierno de Identidades y Accesos

Integración con marco de control y políticas de seguridad existentes

- Una solución de Gobierno IAM permite que los procesos y controles de acceso se apliquen en múltiples aplicaciones de negocio y otros sistemas.

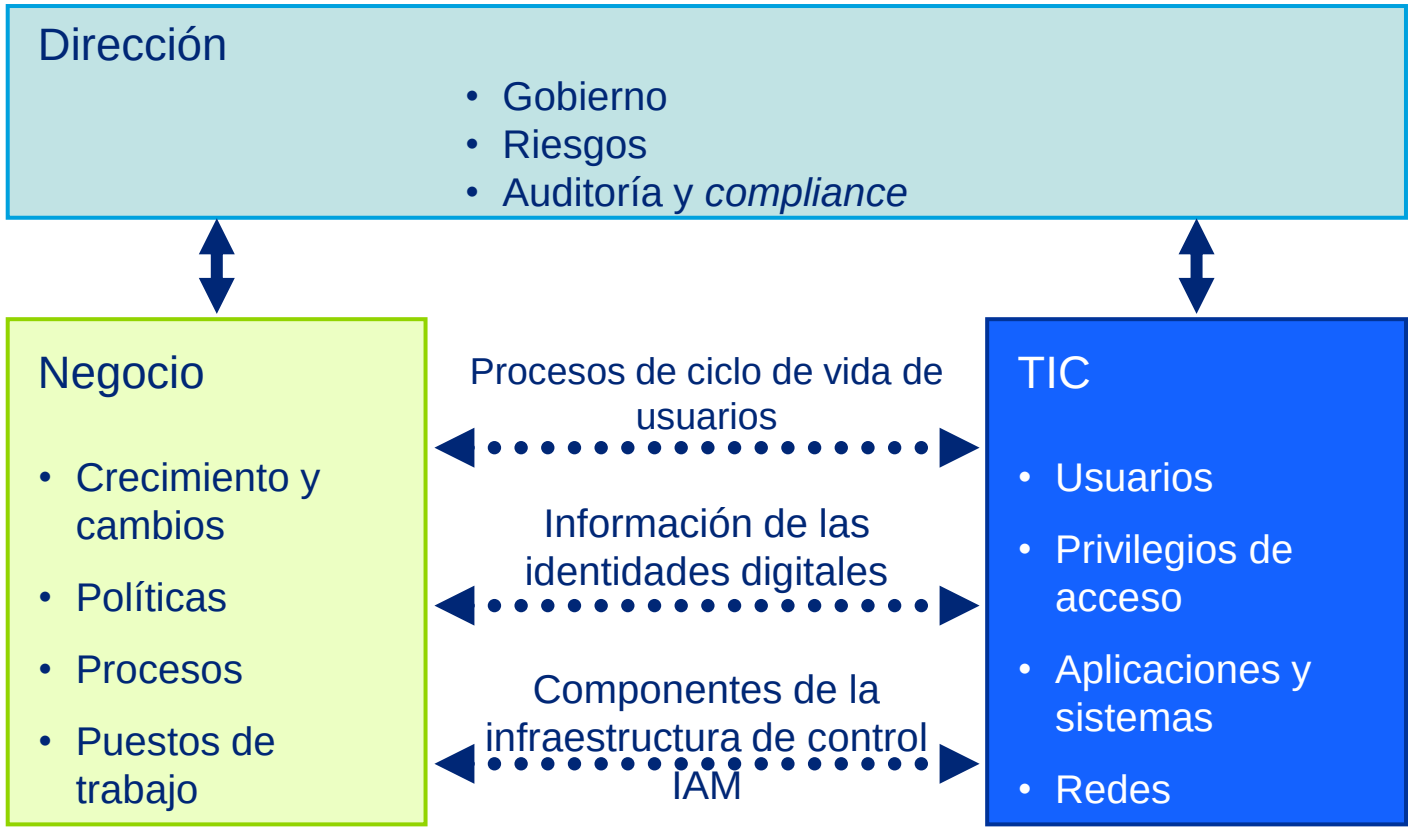
- Por ello, el Gobierno IAM proporciona una **infraestructura de control** que permite:
  - Marco de control interno de gestión de acceso a la información corporativa
  - Políticas y procedimientos de gestión del riesgo
  - Objetivos de control
  - Actividades de control



4. El reto del Gobierno de Identidades y Accesos

Facilitador de la colaboración con las áreas de negocio

Alinear los objetivos de Gobierno, Riesgo y Cumplimiento requiere múltiples niveles de colaboración entre el negocio y el personal IT relacionado con la gestión de accesos e identidades.



Si desea información adicional, por favor, visite www.deloitte.es

Deloitte se refiere a Deloitte Touche Tohmatsu Limited, (*private company limited by guarantee*, de acuerdo con la legislación del Reino Unido) y a su red de firmas miembro, cada una de las cuales es una entidad independiente. En www.deloitte.com/about se ofrece una descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Deloitte presta servicios de auditoría, asesoramiento fiscal y legal, consultoría y asesoramiento en transacciones corporativas a entidades que operan en un elevado número de sectores de actividad. La firma aporta su experiencia y alto nivel profesional ayudando a sus clientes a alcanzar sus objetivos empresariales en cualquier lugar del mundo. Para ello cuenta con el apoyo de una red global de firmas miembro presentes en más de 140 países y con aproximadamente 170.000 profesionales que han asumido el compromiso de ser modelo de excelencia.