# Alineamiento Estratégico y Gobernanza de Acceso

Por André Koot


*Por comentarios sobre este artículo, contacte nuestro Repositorio GitHub o reporte un problema.*

## Tabla de contenidos



## Resumen

Para que una organización tenga éxito en la era digital actual, debe contar con una sólida función de Tecnología de la Información (TI). Sin embargo, si esta función no trabaja codo a codo con los componentes de negocio de la organización tendrá un mal rendimiento. Varias organizaciones consideran la Administración de Identidades y Accesos (IAM, por sus siglas en inglés) como una responsabilidad de TI. Si bien algunas tareas y actividades relacionadas con la IAM son consideradas parte de las TI, otras no lo son. El éxito de los programas relacionados a la IAM puede verse limitado si no se entienden claramente las diferentes tareas y responsabilidades dentro del campo de la IAM.

Este artículo aborda la necesidad de tener un alineamiento estratégico explícito, también conocido como el alineamiento TI con el negocio, entre los esfuerzos TI en torno a la IAM (particularmente la gestión de acceso) y las necesidades de negocio de una organización. La falta de este tipo de alineamiento conduce a proyectos fallidos de IAM e inhibe el crecimiento de las empresas.

# Introducción

Muchos departamentos de Tecnología de la Información (TI) son designados responsables de la implementación de los sistemas IAM que dan soporte a una organización para que opere de forma eficiente y efectiva. Los sistemas de administración de identidades están diseñados para automatizar los procesos de incorporaciones, traslados y bajas (procesos de "JML", por sus siglas en inglés) de los empleados.[1] En cambio, los sistemas de administración de acceso están diseñados para solicitar y otorgar autorizaciones a sistemas de información e incluso el acceso físico a instalaciones tales como edificios o centros de datos. Para que la TI apoye los procesos y controles necesarios, debe incluir los impulsores de negocios de la organización. En general, la TI (y en particular la IAM) deben estar al servicio de la organización. La importancia del alineamiento estratégico es crítica y desafortunadamente el mismo es desafiante. Los diferentes lenguajes, culturas y prioridades cotidianas obstruyen la comprensión que tiene cada lado sobre qué debe pasar para que un negocio tenga éxito y porqué.

## Terminología

- Alineamiento: El índice de sincronización de los procesos y entornos.
- Gobernanza: Garantizar que los propietarios responsables tienen el control, de forma demostrable.
- Gobernanza y Administración de Identidades: Una solución para automatizar la administración de usuarios y las autorizaciones en los sistemas objetivo, construida sobre los procesos de clientes y de recursos humanos de la organización.
- Procesos de incorporaciones, traslados y bajas: Es el ciclo de vida de incorporación/traslado/baja de la identidad de un empleado y tiene en cuenta los tres estados del ciclo de vida de un empleado: la incorporación a la organización, el traslado dentro de la organización (cambio de área o departamento) y la partida o baja de la organización.[2]

## Acrónimos (por sus siglas en inglés):

- CEO: director ejecutivo; CFO director financiero; CRO director de riesgos; CTO director de tecnología; COO: director de operaciones
- RBAC: Control de Acceso Basado en Roles
- IGA: Gobernanza y Administración de Identidades
- Procesos JML: Procesos de incorporaciones, traslados y bajas

# Entendiendo el alineamiento estratégico

El alineamiento TI con el negocio, también conocido como alineamiento estratégico es estudiado desde los años 80. Siguiendo el modelo de Henderson y Venkatraman, el

[1] Cameron, A. & Grewe, O., (2022) "Un pantallazo sobre el ciclo de vida de la identidad digital (v2)" *Cuerpo de Conocimiento de IDPro* 1(7). doi: https://doi.org/10.55621/idpro.31

[2] Bago (Editor), E. & Glazer, I., (2021) "Introducción a la identidad - Parte 1: tiempo de administración (v2)", *Cuerpo de Conocimiento de IDPro* 1(5). doi: https://doi.org/10.55621/idpro.27

alineamiento estratégico combina una integración dinámica de la planificación TI con el desarrollo de negocio para dar forma o permitir una estrategia holística de negocios.[3]

Idealmente, la TI permite que la empresa funcione de forma efectiva y eficiente. La TI puede ayudar a resolver problemas de negocio al proveer formas de trabajo lógicas y estructuradas, integrando soluciones y permitiendo la integración de accesos y aplicaciones. Por ejemplo, la TI ayuda a automatizar tareas manuales, manteniendo registros, integrando diferentes componentes y sistemas de procesamiento de la información, siguiendo las mejores prácticas de seguridad. Cuando está alineada con los impulsores de negocio de la organización, la TI entiende mejor qué problemas deben ser solucionados y los negocios suelen ser más exitosos cuando sacan provecho de la eficacia que ofrece la TI.

Para alcanzar los niveles necesarios de alineamiento estratégico, primero se deben tener en cuenta las dificultades que enfrenta. El lenguaje utilizado por las empresas para identificar "qué es importante" suele diferir bastante del lenguaje utilizado por la TI.

| Las empresas hablan de: | | La TI habla de: |
|---|---|---|
| La satisfacción del cliente | | Acuerdo de nivel de servicio del sistema (por ej. una disponibilidad del 99.999%) |
| Retorno de la inversión ("ROI", por sus siglas en inglés) | | Arquitectura de red (por ej. híbrida, en la nube, en las instalaciones) |
| Requisitos legales y normativas (por ej. El Reglamento General de Protección de Datos [RGPD], la Ley de privacidad del consumidor de california ["CCPA" por sus siglas en inglés]) | | Anuncios de vulnerabilidades y exposiciones comunes ("CVE", por sus siglas en inglés)[4] |
| Cuota de mercado | | Las últimas tecnologías de administración de contenedores<br>(por ej. Kubernetes) |
| Ganancias antes de intereses, impuestos, depreciación y amortización ("EBITDA", por sus siglas en inglés) | | Mecánicas de control de acceso (por ej., -rwxr-xr-x) |

[3] Henderson, John C., y N. Venkatraman. "Alineación estratégica: un modelo de proceso para integrar la tecnología de la información y las estrategias comerciales." (1989), https://dspace.mit.edu/bitstream/handle/1721.1/49138/strategicalignme1989hend.pdf, y Dampney, C. N. G., & Andrews, T. B. (1989). "Luchando por una ventaja competitiva sostenida: la creciente alineación de los sistemas de información y los negocios." División de tecnología de la información de Australia de CSIRO.

[4] https://cve.mitre.org/

| | | |
|---|---|---|
| Balance financiero final (por ej., el Libro mayor de contabilidad) | | Capacidades de red (por ej. bits por segundo, estructuras de base datos) |
| Tasas de interés | | Arquitectura de centro de datos y clústeres de computación |
| Confianza del consumidor y reputación del negocio | | P1 (incidentes de prioridad 1) |

(No existe una correlación horizontal implícita entre los términos de la columna izquierda y los de la columna derecha).

## Modelos de alineamiento

Existen diferentes metodologías que describen los puntos de comunicación necesarios para dar soporte al alineamiento estratégico. En 1993, Hendersen y Venkatraman, dos colegas de IBM, crearon el siguiente modelo de alineamiento estratégico.[5]

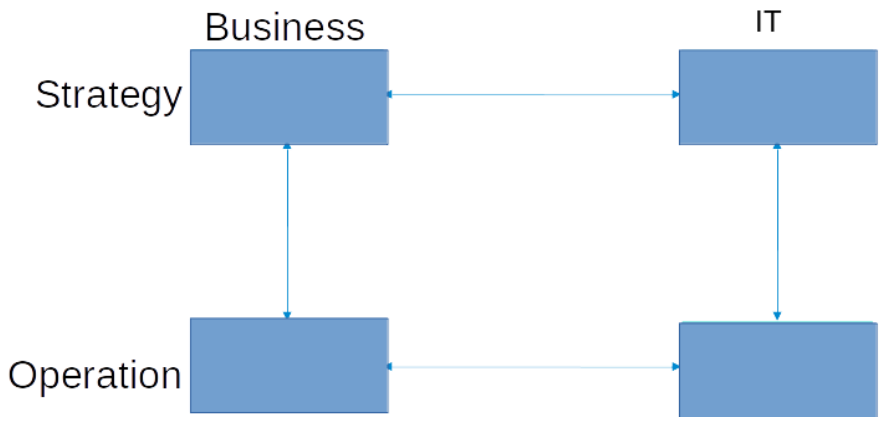


*Figura 1: Modelo simple para el alineamiento estratégico*

Este modelo sugiere que las partes interesadas de negocio y TI deben comunicarse tanto a nivel estratégico como operativo. Esta comunicación multidireccional garantiza que los procesos de negocio estén respaldados por las soluciones de TI apropiadas. Al unir las decisiones estratégicas con las decisiones operativas, la organización puede minimizar los cambios innecesarios en procesos y tecnologías. Sin embargo, para que este modelo de trabajo funcione, la organización debe contemplar que la forma de trabajo de la TI y el negocio, son diferentes, así como sus culturas, lenguajes y jergas. Estas diferencias dificultan el alineamiento estratégico.

Una característica clave de este modelo (y de los otros modelos presentados) es que la comunicación entre dominios/células sólo puede ocurrir en líneas horizontales y verticales, pero nunca diagonales. Esto significa que la comunicación se da únicamente en relaciones formalizadas lo cual previene la interrupción de procedimientos formales y maduros.

---

[5] Alineación estratégica, Henderson y Venkatraman, 1993, reimpresión en https://www.researchgate.net/figure/The-Henderson-and-Venkatraman-strategic-alignment-model-Reprinted-from-Henderson-JC_fig2_220220710

*El caso del director ejecutivo:*
*Mi antiguo director ejecutivo estaba tentado a comprar un teléfono inteligente. Si todos los jóvenes vendedores usaban estos dispositivos ¿por qué no el director ejecutivo? Pero él también quería acceder al correo electrónico de su compañía en el mismo teléfono inteligente. Su expectativa no hubiese sido un problema de no ser que en el 2008 las empresas no respaldaban estos dispositivos de forma tradicional. El director ejecutivo le encargó directamente a un ingeniero TI que lo hiciera posible: le pidió poder instalar la aplicación, conectar al servidor de mail, crear un canal seguro para la Internet, agregar certificados, etc. Este cambio no convencional interrumpió por tres meses las operaciones TI.*

En el modelo de Información de Ámsterdam del profesor Rik Maes, el Dr. Maes agregó componentes adicionales para implementar una estructura y gestión de la información.[6] :

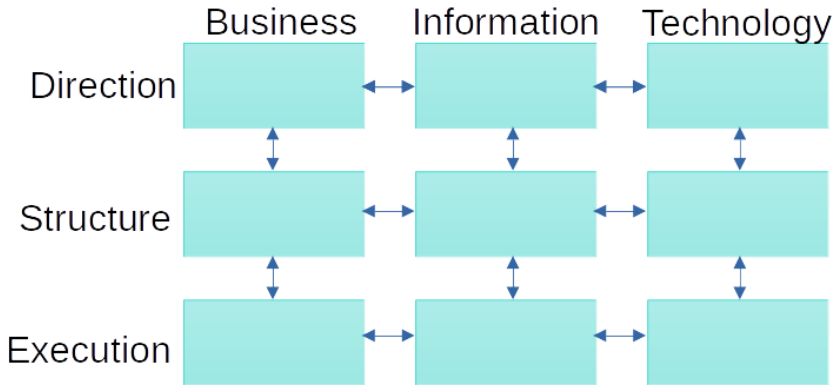

*Figura 2: el Modelo de información de Ámsterdam para el alineamiento estratégico*

La columna del medio, de gestión de la información, traduce los requisitos de negocio a soluciones TI (traducción de izquierda-a-derecha). También traduce las características y la funcionalidad de los componentes TI (plataformas, servicios, aplicaciones) a oportunidades de negocios (la traducción de derecha-a-izquierda). La función de gestión de información debe superar los problemas indicados arriba, como las diferencias culturales y de lenguaje. El administrador de información (o CIO, por sus siglas en inglés) debe comprender y saber cómo dialogar tanto con gente de negocios como con el personal TI. El administrador de información debe ser capaz de conectar con toda la organización y hacer las veces de eslabón perdido dentro del alineamiento TI con el negocio.

La capa horizontal del medio incorporada por este Modelo también tiene una función específica de 'traducción':

Esta capa puede ser vista como la capa de arquitectura. Traduce conceptos estratégicos a operaciones cotidianas. Al ver las diferentes columnas dentro de esta capa de izquierda a derecha, podemos identificar los siguientes conceptos arquitectónicos:

---

[6] El modelo de información de Ámsterdam, 1999, re-edición en https://www.researchgate.net/publication/242321998_A_Generic_Framework_for_Information_Management

- Arquitectura de negocios (organigrama/gráfica de organización y modelos de procesos de negocios, incluyendo la Segregación de Funciones (“SoD”, por sus siglas en inglés), el abuso de los controles de prevención de la información, etc.).
- Arquitectura de la información (modelos de datos, flujos e interfaces).
- La arquitectura TI (incluyendo servidores y redes, contenedorización, en la nube, y arquitectura de seguridad).

Dentro de este modelo podemos ubicar al CEO, CFO y COO en el área superior izquierda. Estas personas son las responsables de definir la estrategia de negocio, dirección y curso de la organización. El jefe de TI o CTO (director de tecnología) estaría ubicado en el área superior derecha, como responsable de las estrategias TI, como por ejemplo la estrategia de aprovisionamiento y la estrategia de gestión de proveedores. Esta tarea deja al CIO en control de la columna del medio, siendo responsable del alineamiento TI con el negocio.

En este modelo, la gobernanza y la dirección de negocio está a cargo de los actores del área superior izquierda.

## IAM y alineamiento

Hasta ahora nos hemos enfocado en la relación negocio/TI de forma general. Dado que la IAM es considerada parte de la TI, nos encontramos que los desafíos del alineamiento estratégico están en el corazón mismo de la mayoría de los fracasos de proyectos IAM. En muchos casos, la IAM es fundamentalmente una función TI. La IAM incluye tareas básicas de “*techies*” como el reseteo de contraseñas, administración de cuentas, aprovisionamiento de usuarios y más. En cambio, la IAM está asociada a las necesidades de negocio más que cualquier otro aspecto de la TI. Los procesos de autorización, en particular, reducen las diferencias entre las operaciones de TI y los requisitos de negocios.

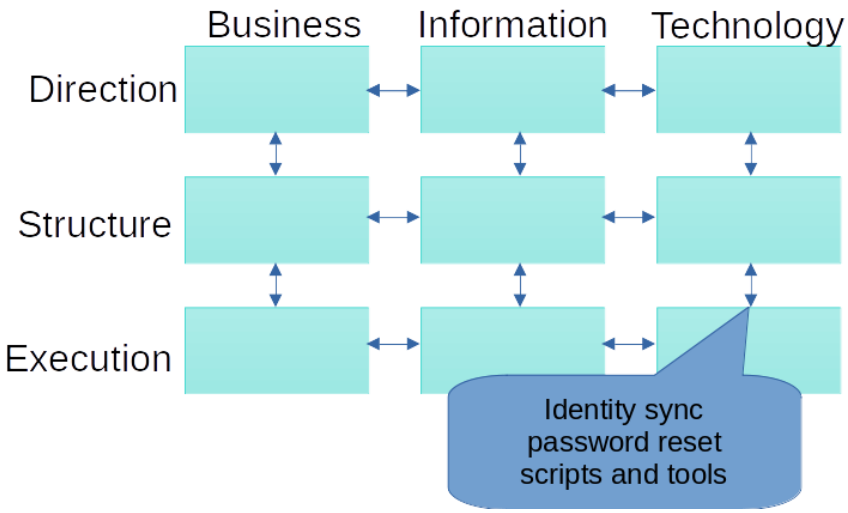


*Figura 3: El Modelo de información de Ámsterdam - La IAM como función TI*

La IAM comenzó como una responsabilidad de la TI. Crear interfaces, conectores, protocolos y agregar certificados pertenecía al terreno de la IAM y la TI. El desencadenante de todas las transacciones de identidad solía ser el departamento de recursos humanos, pero en operaciones diarias la administración de identidades pertenecía a la TI como parte de su

tarea general de automatización de procesos de negocio. Esto no ha cambiado. La mayor parte de la administración de identidades en una organización aún se considera como siendo de TI: área inferior derecha.

Por otro lado, la gestión de autorizaciones no se planifica tan fácilmente. La autorización involucra "El acto de determinar el derecho de un usuario para acceder a una funcionalidad con una aplicación de computadora y el nivel en el cual ese acceso debe ser otorgado. En la mayoría de los casos, una "autoridad" define y provee el acceso, pero en algunos casos el acceso es concedido por derechos inherentes (como en el caso de un paciente accediendo a su propio registro médico)." [7] La autorización está directamente relacionada con las prácticas de negocios, pero aun así suelen ser implementadas por el equipo IAM.

Al usar el modelo de información de Ámsterdam podemos identificar dónde están definidas de forma prominente las autorizaciones. Las autorizaciones facilitan la realización de tareas dentro de una organización y por lo tanto son cruciales en la fase de ejecución. Las autorizaciones se derivan de la estructura de organización y el proceso de negocio. Por lo tanto, la implementación de la gestión de autorizaciones debe realizarse dentro del área de estructura de negocio del modelo. Las reglas de segregación de funciones, por ejemplo, se definen dentro de un proceso de negocio: a una persona se le impide ejecutar una serie de tareas consecutivas ya que podría generar un riesgo de fraude, abuso de permisos o filtración de datos. Las tareas son definidas dentro del proceso. Esto quiere decir que el propietario del proceso (centro a la izquierda) tiene la responsabilidad de definir las políticas específicas de control de acceso.

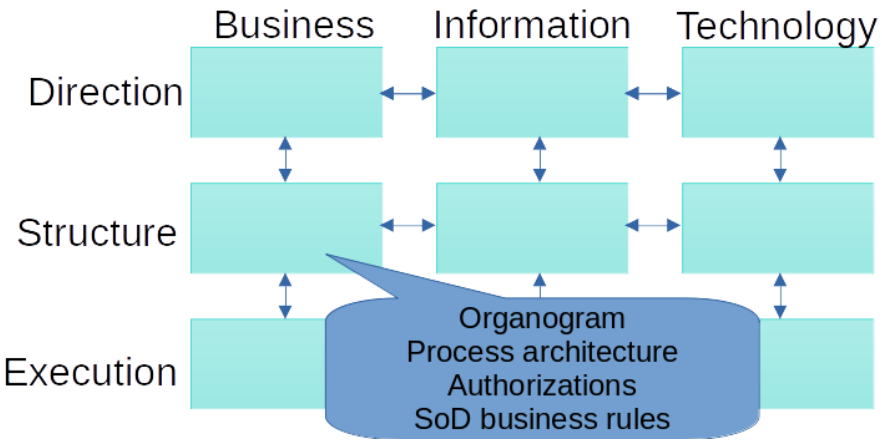


*Figura 4: El modelo de información de Ámsterdam - La autorización como función de negocio*

La TI no gestiona ni es propietaria de las autorizaciones dentro de la estructura de negocio. Son responsabilidad de los propietarios de "empresas", específicamente propietarios de procesos, jefes directos o propietarios de datos.

Gestionar autorizaciones (definirlas, otorgarlas y anularlas) es una de las tareas más complejas para cualquier organización. Aquí es donde el concepto de Control de Acceso Basado en Roles (RBAC, por sus siglas en inglés) se vuelve útil. El concepto fue creado en la

[7] Flanagan (Editor), H., (2022) "Terminología en el Cuerpo de Conocimiento de IDPro", *Cuerpo de Conocimiento de IDPro* 1(9). doi: https://doi.org/10.55621/idpro.41.

era de las unidades centrales con soluciones como la Instalación de Control de Acceso a Recursos (RACF, por sus siglas en inglés) de IBM y el sistema de Instalación de Control de Acceso 2 (ACF2, por sus siglas en inglés). En la era de las redes de áreas locales, RBAC se convirtió en la solución para gestionar estas autorizaciones complejas. En los noventa comenzaron a surgir soluciones específicas de administración de identidades y las soluciones de autorización que exploran el concepto de RBAC surgieron hacia los años 2000. Estas soluciones evolucionaron con el tiempo, ofreciendo eventualmente la gobernanza de identidad al incorporar procesos de confirmación/recertificación.

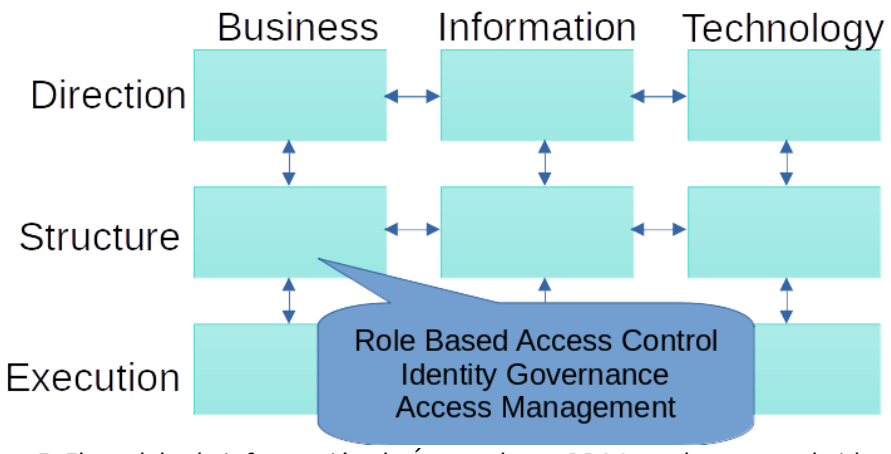


*Figura 5: El modelo de información de Ámsterdam - RBAC y gobernanza de identidad*

Hoy en día vemos a los vendedores moverse más hacia el centro. Los vendedores tradicionales de software de administración de identidades añaden soluciones de gestión de autorizaciones y los vendedores tradicionales de gobernanza de identidad incorporan la identidad y capacidades de gestión en el flujo de trabajo. También existen "nuevos" participantes en el mercado que ofrecen soluciones en la nube de gobernanza y administración de identidades.

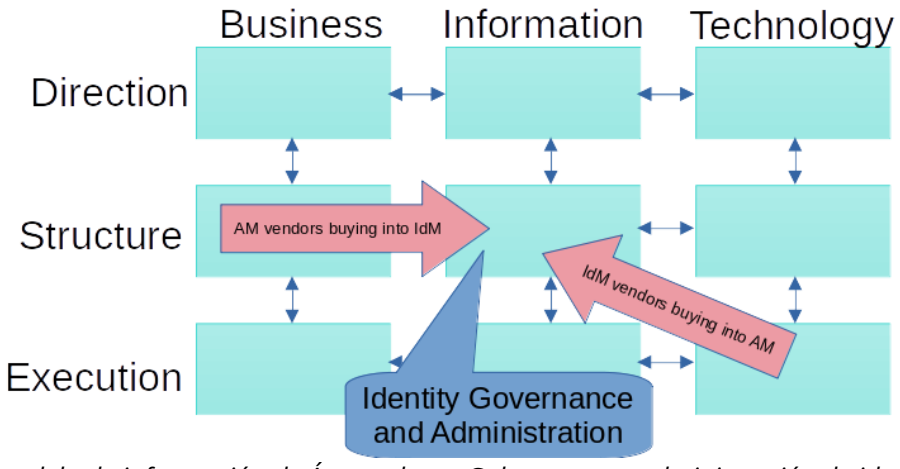


*Figura 6: El modelo de información de Ámsterdam - Gobernanza y administración de identidades (IGA)*

Al evaluar los modelos de Control de Acceso Basado en Atributos y Control de Acceso Basado en Políticas podemos ver en ambos el mismo cambio de responsabilidad en el alineamiento estratégico. Existen varias políticas de control de acceso centradas en TI, como el requisito

para usar certificados de TLS y redes de confianza cero. Pero también hay otras políticas de acceso que están dirigidas al negocio. Políticas como SoD o gestión de consentimiento relacionado a la privacidad mantienen una relación con el sector de estructura de negocio dentro del modelo.

## Un caso de estudio ampliado

Los sistemas de información fueron principalmente desarrollados para apoyar el proceso de gestión de identidad y la gestión de autorización; las soluciones IGA de la generación actual cumplen con su rol de forma admirable al apoyar los negocios con identidades confiables (basado en el ciclo de vida de identidad de recursos humanos) y autorizaciones fiables. Y aun así existe el problema de IAM siendo vista como una responsabilidad de TI. Permítanme explicar esto con el siguiente caso:

> *Caso de estudio - obligación vs. responsabilidad*
> *Una institución financiera apoya su gobernanza de identidad y requisitos de RBAC al usar una solución IGA moderna. El sistema está integrado dentro de un panorama TI y se conecta a varias aplicaciones de negocio destinadas al aprovisionamiento y la conciliación.*
>
> *Un auditor externo reportó al CEO un problema de alto riesgo relacionado con las autorizaciones en el sistema de contabilidad financiera.*
>
> *El CEO (arriba a la izq.) le reenvió el hallazgo al CTO (arriba a la der.). Dado que el problema estaba relacionado con un sistema, estimó que le correspondía a TI resolverlo. El CTO a su vez se lo reenvió al propietario del producto IGA en el departamento de servicio de envíos TI (abajo a la der.). El propietario del producto desafortunadamente no pudo resolver el problema.*
>
> *¿Qué salió mal?*

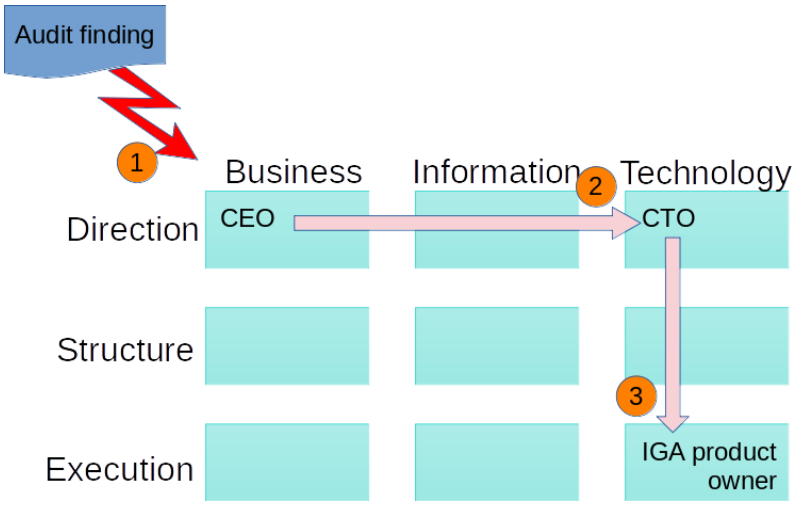


*Figura 7: El modelo de información de Ámsterdam- comunicación IAM predeterminada*

> *El propietario del producto es responsable del sistema IGA pero no de las decisiones de autorizaciones en sí; éste no puede solucionar los problemas encontrados por el*

*auditor. En resumidas cuentas, el propietario tiene la responsabilidad, pero no la obligación de las autorizaciones. En su lugar, le corresponde al propietario del proceso de negocio financiero resolver el problema.*

*Nótese que basado en el modelo de información de Ámsterdam, no existe comunicación directa entre el propietario del producto IGA, quien trabaja en el nivel operativo dentro de TI (abajo a la der.) y el propietario del proceso de negocio (centro a la izq.) en la capa arquitectónica del negocio. Esta comunicación sería un vínculo diagonal e interferiría con las operaciones regulares y correctamente estructuradas.*

*El consejo sería que el propietario del producto vuelva a escalar verticalmente el problema hacia el CTO sobre la base de que no es responsable de las decisiones de autorizaciones. El CTO debería aconsejar entonces al CEO a que le asigne la solución del problema al propietario del proceso de negocio:*

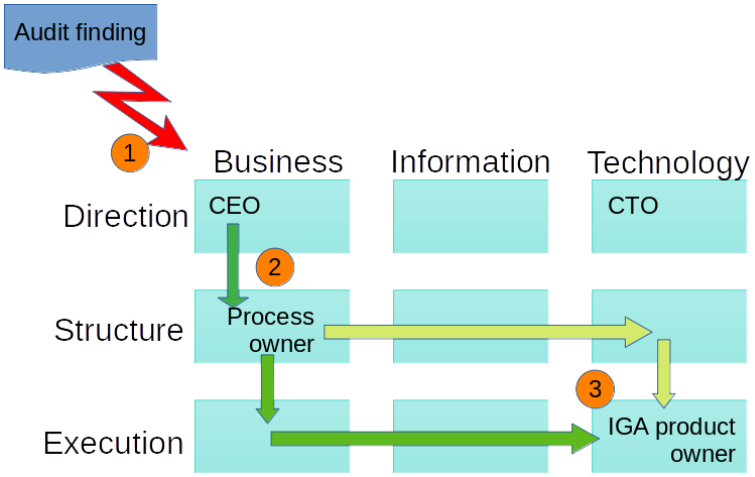


*Figura 8: El modelo de información de Ámsterdam - Camino correcto de comunicación*

*(Se podrían seguir diferentes caminos de comunicación necesaria para llevar a cabo las adaptaciones requeridas del modelo de autorización en el sistema IGA.)*

## El camino futuro

¿Cómo resuelven estos modelos el problema de la falta de participación de las partes interesadas dentro de las organizaciones? ¿Puede acaso el alineamiento estratégico resolver el desafío de la gobernanza?

Primero que nada, esta teoría demuestra que el control de acceso o la gestión de autorizaciones no son responsabilidad de TI. El 'negocio' es el responsable de estructurar e implementar los modelos de autorización y gestión de autorizaciones. Cuando mucho, TI es capaz de dar soporte a la empresa únicamente en la implementación de las herramientas que puedan colaborar con los mismos.

Esto hace que la implementación de la IAM sea un nuevo desafío. La implementación no es solamente un proyecto TI. Una solución de administración de identidades puede implementarse como si fuera un proyecto TI, pero la gestión de autorizaciones no es un

proyecto. La gestión de autorizaciones es la eterna responsabilidad de los gerentes y los propietarios de las empresas.

Esto nos lleva a la siguiente conclusión: un proyecto de IAM no puede existir como un proyecto TI. Implementar la gestión de autorizaciones resulta en (o requiere) un cambio organizativo y está por lo tanto relacionado con la gobernanza y el control de responsabilidades de negocio habituales.

La gobernanza de acceso es lo que conecta la gobernanza de negocio y el desafío del control con las soluciones TI usadas para apoyar a la organización para que lleve a cabo su misión. La forma más sencilla de activar el negocio es encontrar a alguien que tome una decisión sobre el tema SoD o con una de las partes interesadas del proceso de aprobación de solicitudes de acceso.

> *Caso de estudio: reglas SoD*
> *Una institución financiera utiliza una solución IGA moderna para administrar cuentas y autorizaciones en Active Directory y sistemas de información misceláneos. Este sistema depende del concepto SoD. Al usar los controles SoD se hace imposible asignarle al mismo empleado dos o más roles opuestos. Existen más de 1200 reglas SoD en el sistema IGA.*
>
> *Al preguntar al propietario del producto del departamento TI quién había definido estas reglas SoD, no supo responder. Mientras que el propietario del producto es responsable del correcto funcionamiento del sistema, la responsabilidad de las reglas SoD está por fuera de su área de responsabilidad. Quizás, ni siquiera conozca a todas las partes involucradas en la toma de estas decisiones.*
>
> *En un mundo ideal, las reglas SoD no se aplicarían sin un propietario de negocio responsable y claramente identificado. En este caso, la institución financiera tiene un gran proyecto de negocio por delante para asegurarse de que los propietarios de procesos indicados hayan revisado cada regla.*

Una buena práctica es la creación de roles y reglas (de negocio) pero solamente si una persona del sector de negocios puede ser designada como la parte interesada responsable del rol o la regla. La gobernanza no es solamente depender de los departamentos TI para solucionar problemas sino tener a alguien que sea responsable de la administración de negocios y de la implementación de los controles para gestionarlo.

## Conclusión

Para que una organización tenga éxito en esta era digital, debe contar con una función TI fuerte. No obstante, para que esta función TI sea óptima debe estar fuertemente asociada a los componentes de negocio de la organización. En otras palabras, para que un negocio sea exitoso, las distintas partes del negocio deben empujar hacia el mismo lado.

Los proyectos IAM sólo pueden triunfar si existe un sólido alineamiento TI con el negocio. Los desafíos de las responsabilidades de una organización en relación con la gestión de autorizaciones ponen en evidencia que la IAM, más que cualquier otra función TI, debe comprender las necesidades de negocio y cubrirlas en los sistemas de identidad.

Garantizar el alineamiento estratégico TI con el negocio es responsabilidad de ambas partes dentro de la organización que deben ser conscientes de las barreras culturales y de las jergas dentro de cada grupo y trabajar para superarlas.

## Agradecimientos

El autor agradece a Heather Flanagan, editora principal de IDPro por convertir los fragmentos originales (escritos en un inglés apenas comprensible) a un texto legible.

## Biografía del autor

André Koot es consultor principal en SonicBee en Ámsterdam, Países Bajos. Es miembro del Comité del Cuerpo de Conocimiento de IDPro. André cuenta con más de 30 años de experiencia en seguridad de la información y con más de 20 años de experiencia en la administración de identidades y accesos. Anteriormente se desempeñó en las áreas de contabilidad financiera y economía de negocios.