GTAG®

GUÍA DE AUDITORÍA DE TECNOLOGÍA GLOBAL

Gestión de identidades y accesos

The Institute of Internal Auditors

¿Qué es la GTAG?

Las Guías de Auditoría de Tecnología Global (GTAG) preparadas por el Instituto de Auditores Internos (IIA) están escritas en un lenguaje directo de negocio para abordar en forma oportuna problemas relacionados con la gestión, el control y la seguridad de la tecnología de la información (TI). La colección GTAG se utiliza como un recurso disponible para los directores ejecutivos de auditoría sobre los distintos riesgos asociados a la tecnología y las prácticas recomendadas.

Guía 1: *Controles de tecnología de la información*

Guía 2: *Controles de gestión de parches y cambios: críticos para el éxito de la organización*

Guía 3: *Auditoría continua: implicancias para el aseguramiento, la supervisión y la evaluación de riesgos*

Guía 4: *Gestión de la auditoría de tecnología de la información*

Guía 5: *Gestión y auditoría de riesgos de privacidad*

Guía 6: *Gestión y auditoría de puntos vulnerables de tecnología de la información*

Guía 7: *Tercerización de la tecnología de la información*

Guía 8: *Auditar controles de aplicación*

Visite el sitio Web del IIA en www.theiia.org/technology para descargar toda la colección.

Gestión de identidades y accesos

Líder de proyecto

Sajay Rai, Ernst & Young LLP

Autores

Frank Bresz, Ernst & Young LLP

Tim Renshaw, Ernst & Young LLP

Jeffrey Rozek, Ernst & Young LLP

Torpey White, Goldenberg Rosenthal LLP

Noviembre 2007

Índice

1. Resumen ejecutivo

La gestión de identidades y accesos (IAM, en inglés) es el proceso que permite gestionar quién tiene acceso a qué información en el transcurso del tiempo. Esta actividad interfuncional implica la creación de distintas identidades para individuos y sistemas, así como también la asociación de cuentas a nivel de la aplicación y del sistema a estas identidades.

Los procesos de IAM se utilizan para iniciar, capturar, registrar y gestionar las identidades de usuarios y los permisos de acceso relacionados a la información confidencial de la organización. Estos usuarios no sólo son los empleados corporativos, sino también los proveedores, clientes, máquinas de planta, cuentas genéricas de administrador y tarjetas de identificación electrónicas de acceso físico. Los medios que utiliza la organización para facilitar la administración de cuentas de usuario y para implementar los controles adecuados en torno a la seguridad de los datos forman la base de la IAM.

Si bien muchos ejecutivos consideran a la IAM como una función de tecnología de la información (TI), este proceso afecta a todas las unidades de negocio de la organización. Por ejemplo, los ejecutivos deben asegurarse de que exista un proceso para la gestión del acceso a los recursos de la compañía y de que se aborden los riesgos inherentes del proceso. Las unidades de negocio deben saber qué es la IAM y cómo gestionarla de manera eficaz. Los departamentos de TI deben comprender cómo la IAM puede respaldar los procesos de negocio y luego deben proporcionar soluciones sólidas que cumplan con los objetivos corporativos sin exponer a la compañía a riesgos indebidos. Para satisfacer todas estas necesidades, se debe lograr una sólida comprensión de los conceptos fundamentales de la IAM.

Además, se debe obtener información de la gestión de negocios y TI para comprender el estado actual de los procesos de IAM de toda la compañía. Se puede desarrollar una estrategia basada en la precisión con que los procesos existentes se alinean con los objetivos de negocio, el grado de aceptación de riesgo y las necesidades de la organización.

Al desarrollar una estrategia de IAM, se debe tener en cuenta lo siguiente:

- Los riesgos asociados con la IAM y la manera en que se abordan.
- Las necesidades de la organización.
- La manera de comenzar a analizar la IAM dentro de la organización y cuál es la estructura de un proceso de IAM eficaz.
- El proceso para identificar a los usuarios y la cantidad de usuarios actuales en la organización.
- El proceso para autenticar a los usuarios.
- Los permisos de acceso otorgados a los usuarios.
- Si los usuarios están obteniendo acceso de forma indebida a los recursos de TI.
- El proceso para rastrear y registrar la actividad de los usuarios.

A medida que la organización cambia, también cambia el uso de los procesos de IAM. Por lo tanto, cuando se realizan cambios, la dirección debe tener cuidado de que el proceso de IAM no se torne demasiado engorroso y difícil de manejar o exponga a la organización a riesgos indebidos ocasionados por el uso inadecuado de los activos de TI.

El rol de los auditores internos

Dado que la IAM afecta a todas las partes de la organización, desde el acceso a la puerta de entrada de una planta hasta la recuperación de información corporativa bancaria y financiera, los directores ejecutivos de auditoría (DEA) suelen preguntarse cómo las organizaciones pueden controlar el acceso de manera más eficaz para lograr una mejor comprensión de la magnitud de la IAM. Por ejemplo, para controlar el acceso de manera eficaz, los gerentes primero deben conocer los puntos de entrada físicos y lógicos a través de los cuales se puede obtener acceso. Los procesos de IAM deficientes o poco controlados pueden ocasionar una falta de cumplimiento de las regulaciones organizativas y una incapacidad para determinar si se está haciendo un uso indebido de los datos de la compañía.

Como resultado, el DEA debe participar en el desarrollo de la estrategia de IAM de la organización. El DEA brinda una perspectiva única respecto de cómo los procesos de IAM pueden incrementar la eficacia de los controles de acceso y, a la vez, proporciona una mayor visibilidad para los auditores respecto del funcionamiento de estos controles.

El objetivo de esta Guía de Auditoría de Tecnología Global (GTAG, en inglés) es proporcionar percepciones acerca de lo que significa la IAM para una organización y sugerir áreas de auditoría interna para la investigación. Además de participar en el desarrollo de la estrategia, el DEA tiene la responsabilidad de preguntar a los gerentes de negocio y TI qué procesos de IAM se realizan actualmente y cómo se administran. Si bien este documento no se utiliza como recurso definitivo para la IAM, puede ayudar a los DEA y a otros auditores internos a comprender, analizar y supervisar los procesos de IAM de la organización.

2. Introducción

Durante años, las organizaciones se han enfrentado al complejo problema de gestionar identidades y credenciales para sus recursos tecnológicos. Lo que solía ser un simple problema que se circunscribía dentro de las paredes del centro de datos se ha convertido en un problema cada vez mayor y exponencialmente complejo que enfrentan las organizaciones de todos los tamaños.

Por ejemplo, muchas organizaciones grandes no pueden gestionar de manera eficaz las identidades y los permisos de acceso otorgados a los usuarios, especialmente en entornos de TI distribuidos. Durante los últimos años, los departamentos de TI han formado grupos de administración de sistemas (SA, en inglés) para gestionar la amplia gama de servidores, bases de datos y escritorios que utiliza la organización. No obstante, a pesar de la creación de grupos de SA, la gestión del acceso a los recursos de la organización sigue siendo un desafío.

Incluso con esta expansión, muchas veces los recursos humanos y los procesos manuales no pueden manejar las tareas complejas y los gastos fijos administrativos excesivos necesarios para gestionar las identidades de usuarios dentro de la organización. Además, en los últimos años, los requerimientos reglamentarios han agregado complejidad y un mayor escrutinio externo de los procesos de gestión de acceso. Estos requerimientos reglamentarios y las prácticas de negocio prudentes han llevado a las organizaciones a otorgarles acceso a las personas en un nivel lo más granular posible, forzando a los gerentes a determinar qué derechos específicos son necesarios, en lugar de otorgarles a los usuarios acceso a los recursos que, de hecho, no necesitan para realizar sus trabajos.

Si bien lo que se conoce como IAM se ha convertido en un término aceptado por la industria, existen muchas definiciones actualmente en uso, según la industria, el proveedor de productos o el consultor profesional. No obstante, la premisa básica sigue siendo la misma. Esta publicación no pretende establecer autoritariamente la definición correcta. En cambio, combina muchas de las definiciones que se han presentado en la industria de TI.

2.1 Impulsores de negocio

Según un reciente informe de pronósticos de International Data Group (IDG)[1], se espera que el gasto en IAM y sistemas relacionados crezca rápidamente. En Estados Unidos, este incremento es impulsado principalmente por la Ley Sarbanes-Oxley de 2002, la Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA, en inglés) de 1996, la Ley Gramm-Leach Bliley (GLBA, en inglés) de 1999, El Acuerdo de Basilea II y otras regulaciones específicas de la industria. Por ejemplo, la industria de servicios financieros está sujeta a pautas que especifican el uso de múltiples grupos de credenciales (es decir, autenticación de múltiples factores). Este informe de pronósticos predice que el mercado global de IAM crecerá, por lo menos, un 10% por año hasta llegar a US$ 5 mil millones en 2010. Así, en muchas organizaciones, la IAM se convertirá en un importante proyecto de TI.

Con este crecimiento, es importante examinar las distintas razones por las cuales las organizaciones se embarcan en proyectos de IAM. Estas incluyen:

- Mejora del cumplimiento de regulaciones.
- Reducción del riesgo de seguridad de la información.
- Reducción del costo operativo y de desarrollo de TI.
- Mejora de las eficiencias y la transparencia operativas.
- Mayor satisfacción del usuario.
- Incremento de la eficacia de las iniciativas de negocio clave.

2.1.1 Mejora del cumplimiento de regulaciones

Sin sobreestimar los efectos de las regulaciones mencionadas en el párrafo anterior, es importante observar que las leyes Sarbanes-Oxley, HIPAA, GLBA, Basel II y otras regulaciones han tenido un impacto significativo en las organizaciones de todo el mundo. No obstante, si bien las iniciativas de IAM han ayudado a cubrir las brechas relacionadas con los controles de acceso al sistema, no han tenido el alcance necesario. Muchas iniciativas de IAM de las compañías actúan meramente como subterfugios para el cumplimiento de las regulaciones. Si bien este enfoque para abordar la IAM puede ser aprobado en una auditoría, podría afectar a la organización en el futuro ya que el programa de IAM se torna demasiado complejo, inoperable y costoso. Además, las organizaciones deben ser conscientes de que los programas de IAM muchas veces recolectan información personal acerca de los usuarios de sistemas. Por lo tanto, estos programas deben estar cuidadosamente alineados con las leyes de privacidad y protección de datos, como la Norma de protección de datos de la Unión Europea de 1995.

2.1.2 Reducción del riesgo de seguridad de la información

Un impulsor clave para la implementación exitosa de la IAM es la mejor postura frente a los riesgos que se deriva de la implementación de mejores controles de identidades y acceso. Sabiendo quién tiene acceso a qué información y cómo el acceso se relaciona directamente con un trabajo o una función en particular, la IAM mejora la eficacia del entorno de control general de la organización.

En muchas organizaciones, la eliminación de derechos de acceso de usuarios o de derechos de acceso para una identidad digital puede demorar de tres a cuatro meses. Esto puede presentar un riesgo inaceptable para la organización, especialmente si una persona puede seguir obteniendo acceso a los sistemas y recursos de la compañía durante el período de eliminación de accesos. Por ejemplo, según observaciones informales, algunos usuarios, como contratistas, siguen teniendo derechos de acceso durante años, lo que genera el acceso no autorizado continuo a los sistemas y una exposición de la infraestructura de la organización a intentos de piratería evitables.

[1] Informe de IDG Nº 204639: Worldwide Identity and Access Management 2006-2010 Forecast Update With Submarket Segments, diciembre de 2006.

2.1.3 Reducción de los costos operativos y de desarrollo de TI

Irónicamente, la proliferación de sistemas automatizados puede afectar negativamente la eficiencia del trabajador debido a los distintos mecanismos de inicio de sesión utilizados. Como resultado, los trabajadores deben recordar o acarrear una variedad de credenciales que cambian frecuentemente. Por ejemplo, un empleado típico puede tener un nombre de usuario y una contraseña para su escritorio, otro nombre de usuario y otra contraseña para obtener acceso a otros sistemas, varios nombres de usuario y contraseñas más para las distintas aplicaciones de identificación y explorador, y un número de identificación personal (PIN, en inglés) con una contraseña de uso único para obtener acceso remoto.

Teniendo en cuenta la gran cantidad de credenciales, multiplicada por sus contraseñas que caducan frecuentemente, el mantenimiento de credenciales se puede tornar demasiado complejo y excesivamente desafiante para los usuarios. Por lo general, esto ocasiona la insatisfacción de los usuarios con el proceso y el olvido de contraseñas. Este escenario degrada la eficiencia del empleado y afecta significativamente a las funciones de soporte, como la mesa de ayuda, que administra estas credenciales y maneja las llamadas por olvido de contraseñas.

La proliferación de sistemas automatizados también puede sumar importantes costos operativos ya que se reproducen los directorios y las bases de datos de identidades de usuarios. Esto genera un desempeño deficiente y un incremento de costos, que son, en su mayoría, costos ocultos. Por ejemplo, muchas organizaciones enfrentan las siguientes circunstancias:

- Una falta de flujos de trabajo de aprobación definidos y automatizados, que hace que el asistente administrativo deba suponerlo según su mejor criterio al iniciar el proceso de establecimiento y manejo de solicitudes de acceso.
- Un incremento en la cantidad de llamadas a la mesa de ayuda, que, en su mayoría, se relacionan con el soporte de identidades y acceso, como solicitudes de restablecimiento de contraseñas.
- Contratación de nuevos empleados que deben esperar una semana o más para obtener acceso de base a los sistemas de TI, como correo electrónico y recursos de red.
- Ausencia de documentación de requisitos de acceso por rol; por lo tanto, los usuarios deben realizar varias llamadas de seguimiento para obtener el acceso que necesitan.

2.1.4 Mejora de las eficiencias y la transparencia operativas

Contar con un proceso bien definido para la gestión de acceso a la información puede mejorar, en gran medida, la eficiencia operativa de una compañía. Muchas veces, las organizaciones luchan contra otorgarles a los usuarios el acceso que requieren para realizar sus funciones laborales. Por ejemplo, las solicitudes se envían a varios miembros del equipo de TI o administración que posiblemente no sepan qué acceso o información está solicitando el usuario o si este tiene una necesidad de negocio de obtener dicho acceso o información. Además, sin un proceso definido, es posible que las solicitudes se envíen incompletas o se realicen de manera incorrecta, lo que ocasiona más trabajo para el equipo de TI o administración.

Por lo tanto, la implementación de un proceso de IAM definido puede mejorar, en gran medida, la eficiencia del proceso. En las grandes organizaciones, el uso adecuado de tecnologías de IAM propicias puede garantizar que la solicitud se enrute a la persona correcta para su aprobación o a la configuración de sistema adecuada o al sistema de establecimiento automatizado. Además, las solicitudes de acceso que demoran semanas en completarse se pueden reducir a días y, a la vez, se puede mejorar la preparación de informes de cumplimiento para estas aprobaciones a través del uso de flujos de trabajo de aprobación definidos dentro del proceso de IAM establecido.

2.1.5 Mayor satisfacción del usuario

Además de las eficiencias operativas mencionadas anteriormente, la implementación de un proceso de IAM eficaz puede permitirles a los usuarios identificar el acceso que necesitan, enviar la solicitud a la persona encargada de la aprobación y obtener rápidamente acceso a la información de trabajo. Esto, a su vez, ayuda a reducir la frustración del usuario, que es especialmente importante a medida que se contratan nuevos empleados (por ejemplo, cuando a los nuevos miembros de un equipo se les proporciona acceso oportuno para realizar sus funciones laborales, se tornan productivos con mayor rapidez).

2.1.6 Incremento de la eficacia de las iniciativas de negocio clave

Muchas veces, ciertas iniciativas de negocio requieren que se cambien los derechos de acceso. Por lo general, estas iniciativas incluyen "joint ventures", socios de tercerización, ventas, fusiones y adquisiciones. Para las compañías que participan en estas actividades, la posibilidad de proporcionar acceso rápidamente a los niveles de información adecuados puede mejorar, en gran medida, el éxito de la actividad. A la inversa, sin un proceso bien definido, podría resultar difícil determinar si se otorgó o se eliminó el nivel correcto de acceso. Por ejemplo, durante una "joint venture" o una fusión, el acceso a la información adecuada y la extinción oportuna del acceso a ciertos recursos de la compañía resultan críticos.

2.2 Conceptos de la gestión de identidades y accesos

La gestión de identidades y accesos (IAM, en inglés) es un proceso complejo que consiste en diversas políticas, procedimientos, actividades y tecnologías que requieren la coordinación de muchos grupos de la compañía, como recursos humanos y TI. Esta guía ayudará a los DEA a comprender los distintos componentes de la IAM, permitiendo que este tema sea más fácil de entender. Para una definición más detallada de estos componentes, consulte el glosario que se encuentra al final de esta guía.

Fundamentalmente, la IAM intenta abordar tres preguntas importantes:

1. **¿Quién tiene acceso a qué información?** Un sistema sólido de gestión de identidades y accesos ayudará a la compañía no sólo a gestionar las identidades digitales, sino también a gestionar el acceso a recursos, aplicaciones e información que estas identidades requieren.
2. **¿El acceso es adecuado para el trabajo que se está realizando?** Este elemento incluye dos aspectos. En primer lugar, ¿el acceso es correcto y está definido adecuadamente para admitir una función laboral específica? En segundo lugar, ¿el acceso a un recurso determinado entra en conflicto con otros derechos de acceso, planteando así un problema potencial de separación de funciones?
3. **¿El acceso y la actividad se supervisan, se registran y se informan adecuadamente?** Además de beneficiar al usuario a través del logro de una mayor eficiencia, los procesos de IAM deben estar diseñados de tal manera que respalden el cumplimiento de regulaciones. Una de las mayores realidades reglamentarias de la Ley Sabarnes-Oxley y de otras regulaciones es que los derechos de acceso deben estar definidos, documentados, supervisados, registrados e informados adecuadamente.

2.3 Riesgos de adopción

La creación de un proceso de IAM plantea la posibilidad de cambios en el personal y en las actividades de negocio actuales y la necesidad de inversión de capital. La introducción de procesos de IAM en una organización puede exponerla a nuevos riesgos y, a la vez, mitigar riesgos existentes. La organización debe examinar y comprender estos riesgos a medida que implementa procesos de IAM nuevos o modificados. En especial, se debe tener en cuenta lo siguiente:

- **Complacencia de la organización.** Muchas organizaciones están felices de continuar realizando ciertos procesos de la misma manera que lo han hecho siempre, aun cuando el statu quo es ineficiente o inadecuado desde una perspectiva de control.
- **Participación.** Todo proyecto importante requiere tiempo adicional y el compromiso de varios recursos para garantizar el éxito del proyecto. Si la organización no dedica suficiente tiempo, se corre el riesgo de terminar inadecuadamente las actividades del proyecto.
- **Planificación.** Los proyectos exitosos requieren planes bien diseñados, hitos de entrega y procesos de determinación de alcance de la gestión de cambios para establecer las expectativas respecto de los compromisos de recursos y las líneas cronológicas.
- **Comunicación.** Los objetivos del proyecto de IAM, las actividades planificadas y los requerimientos de recursos se deben comunicar a las partes interesadas correspondientes. Sin esta comunicación, las personas que deben participar en el proyecto no podrán proporcionar el aporte adecuado.
- **Incorporación de todos los sistemas al proceso.** Los proyectos de IAM son complejos y suelen demorar un tiempo considerable en completarse. Intentar incorporar muchos sistemas informáticos en la estructura de IAM simultáneamente puede tornarse una tarea dificultosa y fallida. Priorizar las áreas de riesgo de negocio clave y los recursos de sistema afectados por el proceso son buenos objetivos para el alcance inicial.
- **Complejidad del proceso.** De acuerdo con el riesgo de complacencia, hacer que un proceso revisado sea demasiado complejo afectará su éxito. Por ejemplo, los usuarios podrían tratar de evadir el proceso o crear uno propio.
- **Crear un proceso demasiado débil.** Si el proceso de IAM está definido débilmente, es confuso o está abierto a las interpretaciones de los usuarios, alentará a otras personas a crear prácticas subvariantes que no utilizan eficazmente el proceso de IAM.
- **Falta de puesta en vigor.** Como parte de la implementación, gobierno y uso del proceso de IAM, las actividades de puesta en vigor correctas le permiten funcionar tal como se diseñó. Si a los usuarios se les permite emplear procesos variados o evadir los establecidos, se puede poner en peligro el éxito general del proyecto.

Si bien algunos de estos riesgos se pueden mitigar o eliminar, se deben identificar, comprender y priorizar antes de definir el proceso de IAM.

3. Definición de los conceptos clave

En las siguientes secciones se analizarán estos conceptos:

- **Identidad** — elemento o combinación de elementos utilizados para describir, de manera exclusiva, a una persona o máquina. Puede ser algo que usted conoce, como una contraseña o un número de identificación (ID) personal; algo que tiene, como una tarjeta de ID, un identificador de seguridad o un identificador de software; algo que forma parte de su persona, como una huella digital o un patrón de retina; o una combinación de estos elementos.
- **Acceso** — información que representa los derechos otorgados a la identidad. Estos derechos de acceso a la información se pueden otorgar para permitir que los usuarios realicen funciones transaccionales en diversos niveles. Algunos ejemplos de funciones transaccionales son copia, transferencia, adición, cambio, eliminación, revisión, aprobación, sólo lectura y cancelación.
- **Habilitaciones** — grupo de derechos de acceso para realizar funciones transaccionales. Nota: El término "habilitaciones" se utiliza ocasionalmente y como sinónimo de derechos de acceso.

Cuando se analiza el concepto de identidades, por lo general, muchos ejecutivos piensan en usuarios humanos. No obstante, es importante recordar que también existen cuentas de servicio, identidades de máquinas y otras identidades no humanas que se deben gestionar. La imposibilidad de controlar cualquiera de estas identidades y el acceso que tienen puede ser perjudicial para el esquema de control general de una organización.

Para que las identidades lleguen a formar parte del ADN de la organización y de su sistema de gestión de accesos, deben atravesar varias etapas. Estas etapas son:

- **Establecimiento.** El establecimiento se refiere a la creación, cambio, extinción, validación, aprobación, propagación y comunicación de una identidad. El tiempo para completar este proceso varía en función de las necesidades específicas de la organización. Además, este proceso debe estar regido por una declaración de política específica de la compañía, de aplicación universal, que redacta y mantiene el departamento de TI con aportes de otras unidades de negocio.
- **Gestión de identidad.** La gestión de identidad debe formar parte de las actividades continuas de la compañía. Incluye el establecimiento de una estrategia de IAM, la administración de los cambios en la declaración de política de IAM, el establecimiento de parámetros de identidades y contraseñas, la gestión de sistemas y procesos de IAM manuales o automatizados y las actividades periódicas de supervisión, auditoría, conciliación y preparación de informes respecto de los sistemas de IAM.
- **Puesta en vigor.** La puesta en vigor incluye la autenticación, la autorización y el registro de las identidades como se utilizan dentro de los sistemas de TI de la organización. La puesta en vigor de los derechos de acceso principalmente se realiza a través de procesos o mecanismos automatizados.

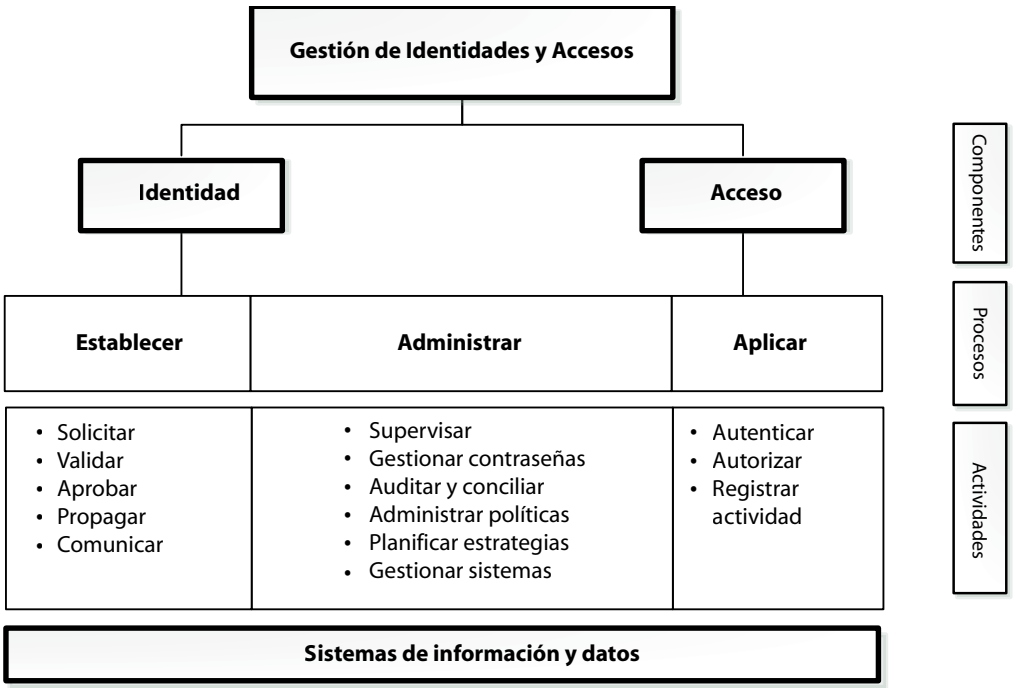

Figura 1. Relaciones entre los componentes de IAM y los conceptos clave

3.1 Gestión de identidades versus gestión de habilitaciones

3.1.1 Proceso de gestión de identidades y accesos

Un proceso de IAM debe estar diseñado para iniciar, modificar, rastrear, registrar y cancelar los identificadores específicos asociados con cada cuenta, ya sea humana o no humana, mediante el uso de los recursos de TI de la organización. Luego, la organización debe utilizar su proceso de IAM para gestionar estos identificadores y su respectiva asociación con las cuentas de usuario. Como resultado, el proceso de IAM debe estar diseñado para incorporar las aplicaciones que necesita una cuenta de usuario para obtener acceso y la forma en que los identificadores se asocian con el usuario, si varían según las aplicaciones. La Figura 1 demuestra cómo los componentes de la gestión de identidades y accesos se relacionan entre sí.

3.1.2 Gestión de las habilitaciones

Como parte del proceso de IAM, la gestión de habilitaciones debe estar diseñada para iniciar, modificar, rastrear, registrar y cancelar las habilitaciones o los permisos de acceso asignados a las cuentas de usuario. Independientemente de la metodología que emplea la organización para agrupar las cuentas de usuario en funciones similares (por ejemplo, grupos de trabajo, roles o perfiles), las habilitaciones de cada usuario se deben gestionar correctamente. Por lo tanto, la organización debe realizar revisiones periódicas de los derechos de acceso para detectar situaciones en las que los usuarios acumulan habilitaciones a medida que se mueven dentro de la organización o situaciones en las que se les asignan habilitaciones inadecuadas a los usuarios. Para realizar revisiones de los derechos de acceso, las unidades de negocio deben solicitar informes de derechos de acceso y comunicar, al departamento de TI, los cambios necesarios a través de los mecanismos de IAM adecuados.

Un componente de un proceso de gestión de habilitaciones diseñado correctamente es el análisis de la separación de funciones. Esto puede evitar la asignación de combinaciones de habilitaciones que le proporcionen a una persona el acceso inadecuado a través de un proceso de negocio o puede detectar conflictos existentes.

3.2 Componentes de la gestión de identidades y accesos

3.2.1 Tipos de identidades

Las identidades adoptan diferentes formas dentro de una organización y, en un proceso de gestión de identidades, se deben considerar todos los tipos.

Los tipos de identidades incluyen, entre otros, todos o alguno de los siguientes:

- Empleados que utilizan recursos de TI.
- Proveedores (por ejemplo, subcontratistas).
- Dispositivos de TI (por ejemplo, dispositivos de hardware que realizan funciones similares a un usuario, como aplicaciones fijas y móviles).
- Cuentas de servicio de aplicaciones (por ejemplo, cuentas predefinidas proporcionadas por el proveedor de software).
- Cuentas de máquina (por ejemplo, dispositivos de hardware de TI que realizan funciones dentro y a través de entornos o aplicaciones de TI, como una máquina de planta).
- Cuentas funcionales o por lote (por ejemplo, las cuentas utilizadas para ejecutar procesos por lote, como lotes de generación de informes durante la noche).

Al auditar las identidades presentes en la organización, los auditores deben determinar si los identificadores específicos y de aplicación universal están asociados con cada tipo de identidad. Esto permite aplicar diferentes reglas a los procesos de gestión y revisión asociados con los distintos tipos de cuentas. Por ejemplo, una cuenta por lote puede estar sujeta a distintas políticas y puede requerir un tipo de revisión diferente que una cuenta de usuario.

3.2.2 Incorporación

Una vez que se determina la necesidad de una identidad, se debe crear la identidad en el entorno de TI. El proceso, ya sea manual o automatizado, que se utiliza para crear esta identidad se denomina incorporación, que implica la creación de un perfil de identidad y la información necesaria requerida para describir la identidad.

3.2.3 Separación

La separación es el proceso opuesto a la incorporación. Durante este proceso, las identidades que ya no requieren derechos de acceso al entorno de TI se identifican, se inhabilitan o desactivan, se revisan para garantizar que estén inactivas y se eliminan del entorno de TI después de un período predeterminado.

3.3 Derechos de acceso y habilitaciones

3.3.1 Cambios de habilitaciones de accesos de identidades

Establecimiento y cambios de derechos de acceso

Cuando a un usuario se le otorga una identidad a través del proceso de establecimiento, la evaluación de los derechos de acceso otorgados o cambiados debe formar parte de la aprobación del propietario de negocio y de la revisión del departamento de TI respecto de la solicitud de acceso. Si bien el departamento de TI no debe hacerse responsable de la aprobación de identidades de usuarios, debe participar en el proceso dado que cuenta con una mejor comprensión de cómo los derechos de acceso otorgados sobre los distintos sistemas de TI interactúan entre sí.

Derechos de acceso de cuentas que no pertenecen a personas
Muchas aplicaciones, bases de datos y herramientas requieren el uso de cuentas funcionales. Por lo general, estas cuentas no se utilizan para que un usuario específico realice la autenticación sino para la comunicación entre dos distintos componentes del sistema. Por ejemplo, la mayoría de los sistemas de gestión de bases de datos (DBMS, en inglés) requieren, para su funcionamiento, que los sistemas en los que se alojan tengan cuentas específicas creadas y activadas. Por lo tanto, la organización debe contar con un método adecuado para solicitar la generación de estas cuentas, limitar su acceso sólo a las habilitaciones correctas, supervisar quién tiene acceso a las credenciales de autenticación de cuentas y revocar las cuentas cuando ya no son necesarias.

3.3.2 Otorgar derechos de acceso a cuentas privilegiadas

Otorgar a una identidad el acceso a cuentas privilegiadas
Las cuentas privilegiadas normalmente están asignadas a la persona del departamento de TI responsable de administrar los sistemas de TI, incluidos los dispositivos y aplicaciones de red, y la infraestructura general de TI. Por lo general, la organización les confía a estos usuarios un nivel de acceso que les permite realizar cambios de alto nivel y, algunas veces, sin documentar en el entorno de TI. Para evitar un acceso innecesario o inadecuado a estas cuentas, la organización debe incluir una sección en su declaración de política de IAM que trate sobre el establecimiento, la administración y la puesta en vigor adecuados.

Supervisar cuentas privilegiadas
En todas las organizaciones existen cuentas privilegiadas. En muchas compañías, estas cuentas se colocan en manos de personas confiables debido al riesgo que representan. A pesar del nivel de confianza depositado en estas personas, la gestión de TI correspondiente debe realizar periódicamente algunos de los siguientes pasos:

- Revisar la lista de usuarios que tienen acceso privilegiado.
- Revisar, siempre que sea posible, las actividades de las cuentas privilegiadas.
- Revisar la actividad en línea de estas cuentas privilegiadas para detectar transmisiones inadecuadas de datos confidenciales salientes o la introducción inadecuada de aplicaciones no aprobadas.

3.3.3 Separación de funciones

Conflictos
Durante el proceso de establecimiento, las personas encargadas de la aprobación de solicitudes de acceso deben evaluar si la solicitud ocasionará un conflicto de separación de funciones. Además, al establecer o cambiar la identidad de un usuario, el departamento de TI puede observar un potencial conflicto de separación de funciones. En este caso, el departamento de TI debe notificarle el problema al propietario de negocio o a la persona encargada de la aprobación. La realización de un análisis de separación de funciones antes de otorgar acceso adicional a una cuenta puede ser un proceso automatizado y se puede utilizar como un control preventivo.

Supervisión periódica de los derechos de acceso
Como parte del proceso de supervisión de IAM, la organización de establecer una metodología para revisar periódicamente los derechos de acceso otorgados a todas las identidades que residen en su entorno de TI. Si bien el departamento de TI facilita esta revisión, debe ser llevada a cabo principalmente por la organización con aprobaciones recibidas de cada propietario de negocio responsable. Además, las identidades de cuentas privilegiadas y de TI deben ser revisadas por un gerente o propietario del sistema adecuado.

3.4 Proceso de establecimiento

En la Figura 2 se presenta una progresión del flujo de trabajo lógico que aborda el proceso de establecimiento.

3.4.1 Solicitud de acceso

El proceso para solicitar la creación, eliminación o modificación de una identidad se debe definir en un procedimiento que detalle lo siguiente:

- Cómo se deben realizar las solicitudes para los distintos tipos de identidades (por ejemplo, medio manual, medio electrónico o llamadas al soporte informático).
- Hacia dónde se deben enrutar las solicitudes.
- Plazos específicos para realizar solicitudes.
- Expectativas de consumación.

3.4.2 Aprobación

Una solicitud de identidad debe estar sujeta a un proceso de aprobación de varios pasos. La aprobación inicial de la solicitud debe ser otorgada por la persona autorizada, responsable directo de la supervisión de las actividades del solicitante. Además, la aprobación se debe llevar a cabo antes de enviar la solicitud al departamento de TI. Una vez otorgado el primer nivel de aprobación, podría ser necesario un segundo nivel de aprobación que debe ser otorgado por el propietario de la aplicación. Una vez garantizadas las aprobaciones correspondientes, la solicitud se debe enrutar al departamento de TI o al sistema correspondiente para su consumación.

3.4.3 Propagación y creación de identidades

Una vez aprobada la creación de la identidad en cumplimiento con las políticas de la organización, la identidad será creada por un miembro del departamento de TI o por una aplicación automatizada controlada dentro del departamento de TI. Al crear la identidad, se debe tener en cuenta lo siguiente:

- La función del solicitante dentro de la organización.

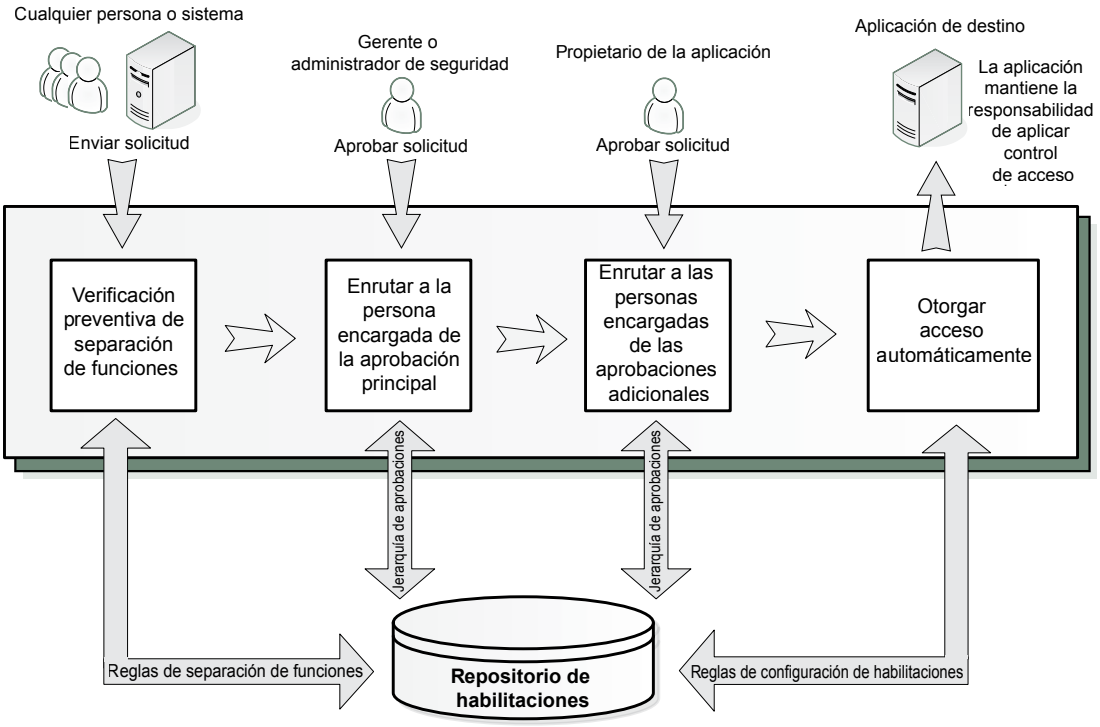

Figura 2. Diagrama de un flujo lógico de establecimiento automatizado.

- Cómo se utilizará la identidad.
- Si el acceso otorgado al propietario de la identidad se basará en roles, reglas o necesidades específicas del usuario.
- Si la identidad se puede replicar a partir de un rol existente o será necesario crear un nuevo rol para satisfacer las necesidades del usuario.

La creación de la identidad requiere una comprensión de la forma en que se utilizará la identidad, las aplicaciones de software que utilizará la identidad y las restricciones de calendario a las que puede estar sujeta la identidad o de las que se debe liberar. Además, la identidad se debe crear con una contraseña correspondiente que contiene restricciones específicas de la aplicación y en cumplimiento con la declaración de política de la organización.

Al otorgar una identidad a una persona, muchos departamentos de TI asignan una contraseña temporal que el usuario debe cambiar durante el intento inicial de inicio de sesión.

Durante esta parte del proceso de IAM, las habilitaciones o derechos de acceso asignados a la identidad se deben evaluar junto con el rol funcional de la identidad en la organización para determinar si pueden surgir problemas de conflicto de interés respecto de la separación de funciones.

3.4.4 Comunicación

Como parte de su declaración de política, la organización debe definir la forma de comunicar la creación, eliminación y modificación de identidades de usuarios. La organización también debe establecer una ubicación o departamento centralizado, separado de TI, para iniciar las comunicaciones de identidades a TI.

Además, el departamento de TI debe utilizar un mecanismo para recibir y enviar comunicaciones relacionadas con la creación, eliminación o modificación de una identidad. Los medios de comunicación pueden adoptar la forma de un mensaje automatizado, un mensaje verbal o una documentación en papel.

Cualquier comunicación relacionada con la identidad debe cumplir con la política de confidencialidad de datos de la organización. Al comunicar la creación o modificación de una identidad a través de medios electrónicos o en papel, el personal debe conocer las restricciones y los requisitos de confidencialidad de datos relacionados con la información de configuración de la identidad. Por ejemplo, es posible que las comunicaciones que contienen una contraseña se deban enviar en sobres sellados, mensajes de correo electrónico encriptados u otros métodos seguros. La organización también debe requerir que los usuarios cambien la contraseña luego de su primer uso para evitar el uso indebido de la identidad y para mitigar los riesgos asociados con su intercepción por una parte no autorizada.

3.4.5 Registro

Un repositorio de habilitaciones es un sistema que rastrea los privilegios otorgados a los usuarios a través del tiempo y registra las solicitudes de acceso, las aprobaciones, las fechas de inicio y fin, y los detalles relacionados con el acceso específico que se otorga. Estos datos se pueden utilizar al auditar el acceso, realizar revisiones de habilitaciones de usuarios y determinar si las actividades de acceso fueron aprobadas.

Los datos generados por el registro se deben mantener durante un período definido y luego se deben destruir. El período de

retención se debe basar en la naturaleza del acceso registrado, en los requerimientos reglamentarios y de auditoría, en las políticas corporativas y en las restricciones de almacenamiento de datos.

3.5 Proceso de administración de identidades y derechos de acceso

3.5.1 Auditoría periódica y conciliación de identidades y habilitaciones

Auditorías periódicas

Para evaluar el diseño y la eficacia del sistema de IAM de una organización, es necesario realizar una auditoría periódica del proceso. La frecuencia de la auditoría se debe determinar como parte del proceso de planificación de auditoría anual, que surge de la evaluación de riesgos anual de la auditoría interna. Las auditorías deben consistir en:

- Una identificación de la máxima a la mínima concentración de identidades de riesgo.
- Un reexamen del diseño del proceso de IAM.
- Un examen de la eficacia operativa del proceso de IAM.
- Una revisión del proceso de establecimiento, que abarca la evaluación de una muestra de identidades que representa una sección transversal de aquellas que estuvieron activas durante una parte del período de auditoría.
- Un examen de la eficacia de la actividad de puesta en vigor de la IAM.
- Un examen de la eficacia de la actividad administrativa de la IAM.

Separación de funciones

Los procesos y metodologías de IAM no deben ser los únicos controles utilizados para evitar que las identidades de usuarios obtengan acceso inadecuado. En consecuencia, la organización debe incorporar algún método de verificación o conciliación de identidades de usuario y sus derechos de acceso correspondientes respecto de los derechos de acceso reales para los cuales se aprobaron originalmente estas identidades. Este proceso de conciliación debe revelar algunos de los siguientes puntos:

- Las identidades de usuarios poseen derechos de acceso que coinciden con los derechos que deben poseer según la aprobación.
- Los derechos de acceso de algunas identidades de usuarios no se revisaron ni se aprobaron con la frecuencia esperada.
- Las identidades de usuarios poseen derechos de acceso que no coinciden con los derechos que deben poseer según la aprobación.
- Las identidades de usuarios asociadas con usuarios cesantes o desactivados todavía residen en el entorno de TI.
- No se solicitó ni se aprobó el acceso de usuarios para los que se necesitan emitir identidades y otorgar derechos de acceso.

Si el proceso de verificación y conciliación revela identidades y derechos de acceso que no están alineados, la organización debe contar con un método para informar estos problemas, determinar acciones correctivas y adquirir las aprobaciones necesarias para corregir estas deficiencias.

Revisiones de habilitaciones

Los procesos de IAM maduros pueden facilitar las actividades de revisión de acceso que realizan los gerentes y los propietarios de la aplicación. Los gerentes pueden revisar el acceso otorgado a sus empleados directos, mientras que los propietarios de la aplicación pueden revisar el acceso otorgado a todas las personas que utilizan la aplicación para identificar y revocar un acceso potencialmente inadecuado. Este proceso de revisión se debe realizar, por lo menos, una vez al año o con mayor frecuencia para las aplicaciones críticas o las personas de alto riesgo.

3.5.2 Administración de la declaración de política

La organización debe contar con un medio para revisar y repasar periódicamente la declaración de política de IAM y garantizar que esta refleja los procesos y las actividades actuales relevantes.

3.5.3 Estrategia de IAM

El departamento de TI o un grupo estratégico de la organización debe establecer un plan integral para iniciar, cambiar y sostener políticas, componentes, procesos y actividades de IAM. El plan debe abordar la forma en que la organización continuará con el proceso de IAM, así como también los riesgos de IAM presentes y futuros; si los procesos de IAM y las actividades relacionadas consistirán en soluciones manuales o electrónicas y si todas las áreas de la organización se incorporarán en el proceso de IAM.

3.5.4 Administración del sistema de IAM

Una vez que se hayan establecido los procesos de IAM dentro de la organización, se deben mantener a través de algunos medios (manualmente, electrónicamente o una combinación de ambos). El mantenimiento del proceso de IAM implica principalmente la administración de la infraestructura relacionada. Esta abarca elementos como la determinación de:

- Dónde se centralizan los procesos de IAM.
- Si la tecnología se utilizará para administrar los procesos de IAM y, si es así, dónde se alojará esta tecnología.
- Quiénes serán los propietarios de TI y de la línea de negocio de la IAM.
- Cómo se documentarán y se registrarán los cambios.

3.5.5 Administración de contraseñas de usuarios finales

Una vez creada una identidad, por lo general, se le asigna una contraseña inicial. Esta contraseña inicial se puede generar manualmente o electrónicamente y se comunica al usuario mediante el departamento de TI. Por lo tanto, si bien la IAM se aplica a las identidades y a los derechos de acceso de los usuarios,

también se deben considerar la emisión y el mantenimiento de las contraseñas de usuarios. Los parámetros, las estructuras y el uso adecuado de las contraseñas se deben detallar en la política de seguridad de la organización.

El mantenimiento de las contraseñas de usuarios es un componente fundamental de un proceso de IAM eficaz. El mantenimiento de contraseñas incluye la realización de las siguientes tareas:

- Emitir contraseñas iniciales.
- Comunicar contraseñas a usuarios.
- Restablecer contraseñas para usuarios bloqueados.
- Revisar las actividades de las contraseñas que cumplen con las pautas de la política de la organización.
- Revisar contraseñas fáciles de adivinar, que pueden ocasionar un potencial uso indebido de los activos de TI de la organización.

3.5.6 Consideraciones acerca del almacenamiento y del manejo

El proceso de IAM también debe abordar la forma en que la organización almacenará, informará, protegerá y gestionará las identidades y los derechos de acceso. Al almacenar las identidades y los derechos de acceso, la organización debe conocer dónde residirán; cómo se visualizarán y se informarán (por ejemplo, enmascarados o en texto claro); durante cuánto tiempo se almacenarán y cómo se almacenarán las identidades desactivadas, inhabilitadas y eliminadas.

3.5.7 Preparación de informes

Se deben crear y utilizar distintos tipos de informes dentro del proceso de establecimiento. Muchos de los informes que normalmente se crean se utilizan con fines operativos, como los informes de las actividades de rendimiento del sistema, de las tareas y de las funciones de gestión de colas y los eventos de conciliación.

Los informes de auditoría son aquellos que describen:

- Listas de identidades y su acceso asociado.
- La persona que aprueba el acceso para la información específica.
- La gestión de cuentas de grupo y supervisión.
- La cantidad de usuarios que obtienen acceso a una aplicación o recurso de información en particular.

Además, los procesos y los sistemas de respaldo deben ser capaces de proporcionar informes que detallen las aprobaciones de accesos y las revisiones, ya que estas son las áreas de mayor debilidad que se descubren al auditar el proceso de gestión de identidades y accesos de la organización.

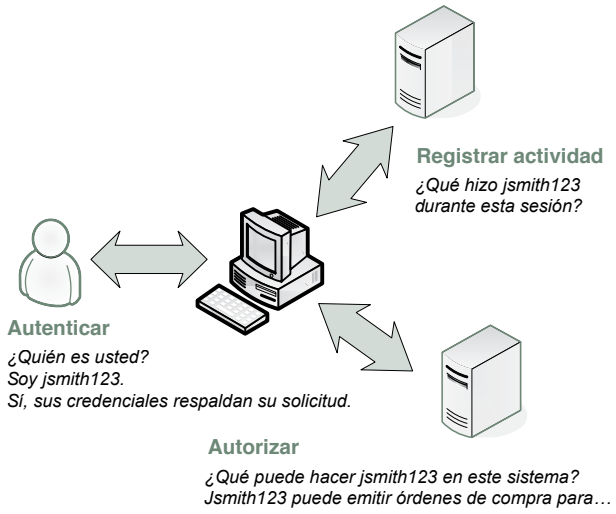

Figura 3. Puesta en vigor de los derechos de acceso del usuario

3.6 Proceso de puesta en vigor

3.6.1 Autenticación y autorización

La puesta en vigor de identidades con sus respectivos derechos de acceso se lleva a cabo durante el inicio de sesión del usuario en la aplicación, como se demuestra en la Figura 3. Durante el inicio de sesión, la aplicación realiza una verificación para validar la identidad del usuario. Este proceso se denomina autenticación y puede adoptar distintas formas. Por ejemplo, los sistemas pueden requerir autenticación mediante el uso de una característica específica del usuario (por ejemplo, la ID de la huella digital o el reconocimiento de voz), algo que tiene el usuario (por ejemplo, una tarjeta inteligente, una credencial de identificación o una llave de acceso) o algo que el usuario conoce (por ejemplo, una contraseña o una frase secreta).

Una vez reconocida y validada la identidad, la aplicación autorizará al usuario a realizar las funciones en la aplicación según los derechos de acceso asociados con la identidad del usuario. La autorización de la identidad del usuario se debe basar en los derechos de acceso otorgados al usuario durante el proceso de establecimiento. Muchas veces, la autorización de la identidad de un usuario puede no estar asociada a los derechos de acceso que se le intentaron otorgar durante el proceso de establecimiento. Por lo tanto, la supervisión y verificación de los derechos de acceso son partes importantes del proceso de IAM.

3.6.2 Registro

El registro de las identidades de usuarios, sus derechos de acceso y las funciones que realizan en la aplicación le proporciona a la organización un medio para examinar varios elementos:

- ¿Las identidades de usuarios y sus derechos de acceso coinciden con los derechos de acceso aprobados para la identidad de usuario?
- ¿Las identidades de usuarios y sus derechos de acceso están desalineados con los derechos de acceso necesarios

para que la identidad de usuario lleve a cabo sus responsabilidades funcionales?
- ¿Las identidades de usuarios realizan todas las funciones otorgadas a través del proceso de establecimiento?
- ¿Las identidades de usuarios presentan frecuentemente solicitudes de cambio de contraseña?
- ¿Las identidades de usuario acceden o intentan acceder a las aplicaciones fuera del horario normal de trabajo?
- ¿Hay intentos no autorizados para realizar ciertas funciones por parte de usuarios registrados o no registrados?

3.7 Uso de la tecnología en IAM

3.7.1 ¿Qué tipos de tecnología existen?

Al administrar actividades de IAM, la mayoría de los procesos de establecimiento y puesta en vigor se puede automatizar a través del uso de herramientas de software de aplicación de IAM. Estas herramientas abarcan desde aplicaciones que pueden ser instaladas y utilizadas fácilmente por organizaciones con pequeños departamentos de TI (por ejemplo, menos de 10 personas) hasta aplicaciones que requieren la personalización para su uso por parte de organizaciones con departamentos de TI grandes o globales.

3.7.2 Ventajas y desventajas del uso de tecnología

Si bien el uso de tecnología facilita absolutamente la IAM, existen ventajas y desventajas respecto de este uso. Las ventajas son:

- Tiempos de respuesta más rápidos.
- Evidencia de actividades fácilmente recuperable.
- Flujos de trabajo automatizados para aprobaciones y comunicaciones.
- Una mejor gestión de grandes volúmenes de datos.
- La posibilidad de administrar y supervisar sistemas de manera centralizada.

Las desventajas son:

- Falta de propiedad.
- Falta de comprensión de la manera de utilizar las herramientas.
- Herramientas que pueden no adaptarse al tamaño o a la complejidad de la organización.

3.7.3 ¿Cómo se utiliza la tecnología?

El uso de tecnología durante el proceso de IAM se puede aplicar para reemplazar actividades manuales o para compensar la falta de algunas actividades de IAM. La dirección de negocios debe comprender la tecnología que se utiliza y la razón por la cual se utiliza, mientras que el departamento de TI debe instalar y mantener las herramientas para respaldar las necesidades de negocio.

Se pueden utilizar herramientas para realizar cualquiera de las siguientes actividades:

- Generar formularios de solicitud de acceso.
- Enrutar formularios de solicitud de acceso a las personas encargadas de su aprobación.
- Realizar una revisión preliminar de conflictos de separación de funciones.
- Comunicar la creación, modificación y extinción de identidades.
- Realizar la autenticación y autorización de identidades para las aplicaciones.
- Generar registros de las identidades y de su uso.
- Generar contraseñas.

3.7.4 Conceptos adicionales

Inicio de sesión único

Existen muchas formas de realizar la autenticación de una identidad dentro de un sistema de IAM. El inicio de sesión único es un medio automatizado de autenticar una identidad para todos los recursos de TI para los cuales se han otorgado derechos de acceso a la identidad, sin requerir que la identidad proporcione más de una serie de factores de autenticación (es decir, una ID de usuario y una contraseña).

Inicio de sesión remoto

En muchas organizaciones, se otorgan derechos de acceso a identidades, particularmente a las humanas, para que se autentiquen ellas mismas al acceder a los recursos de TI desde una ubicación externa a la organización. Este tipo de acceso remoto y autenticación se puede llevar a cabo de varias maneras; algunas más seguras que otras. Los ejemplos de estos mecanismos son:

- Redes privadas virtuales, que son conexiones de dispositivos en red entre las oficinas de la organización y el sitio remoto de la identidad.
- Portales Web, que son conexiones a través de una interfaz basada en Internet con las oficinas de la organización.
- Módems de acceso telefónico, que son conexiones entre el sitio de la identidad y el sitio de la organización que utilizan líneas telefónicas comunes, similares a una llamada telefónica de voz.

Estos tipos de conexión remota tienen sus propias ventajas y desventajas. Por ejemplo, el acceso a través de un portal Web es el más universal ya que permite a los usuarios obtener acceso al sistema desde prácticamente cualquier sistema que tenga acceso a Internet; no obstante, se corre el riesgo de que la información confidencial o de propiedad se vea comprometida por el sistema no controlado en el que se encuentra el explorador Web. Los módems de acceso telefónico proporcionan conexiones directas un poco más seguras con la red interna pero con un rendimiento mucho más lento que las otras opciones de conexión que utilizan conexiones de Internet de alta velocidad. Estos son sólo dos ejemplos de los tantos factores que se deben evaluar al determinar qué usuarios pueden conectarse de forma remota con el entorno de TI y qué métodos se deben utilizar para establecer dicha conexión.

4. El rol de los auditores internos

Los auditores internos desempeñan un papel importante en ayudar a las organizaciones a desarrollar procesos de IAM eficaces y supervisar su implementación. Antes de realizar una auditoría de IAM, los auditores deben comprender la estructura de IAM existente en la organización, como la arquitectura de negocio de la compañía y las políticas de IAM, además de las leyes, regulaciones y mandatos que se deben cumplir. Al realizar la auditoría, los auditores internos deben documentar los procesos de identidad y autorización de la organización, así como también los repositorios y los componentes del ciclo de vida, y evaluar los controles de actividades de IAM existentes.

4.1 Procesos de IAM actuales

El primer paso en el proceso de IAM es determinar si la compañía tiene un programa de IAM. Para determinar esto, se pueden hacer las siguientes preguntas:

- ¿Existen políticas para la gestión y administración de identidades de usuarios y actividades de acceso?
- ¿Existe alguna estrategia para abordar los riesgos asociados con el proceso de IAM?
- ¿Existe algún modelo de referencia que puede utilizar la organización durante el proceso de administración?

Al responder estas preguntas, es importante identificar si ya existe documentación que, de alguna manera, aborde estos temas.

Además, al abordar la postura de IAM de una compañía, los auditores internos deben identificar ciertos elementos clave. La siguiente figura muestra que estos elementos no se centran totalmente en la tecnología pero incluyen:

- Alinear unidades de negocio y gestión.
- Comprender las leyes y regulaciones existentes.
- Establecer presupuestos.
- Desarrollar planes de implementación alcanzables.
- Definir cómo la tecnología puede permitir un entorno de control más eficaz.

4.1.1 Arquitectura de negocio

La arquitectura de negocio de IAM se refiere a los procesos y la lógica de flujo de trabajo que se implementan junto con un producto de software de IAM. La definición y documentación de esta arquitectura es un paso crítico hacia la gestión de los riesgos de negocio actuales y futuros. Como se muestra en la Figura 4, la IAM no se refiere estrictamente al uso de herramientas técnicas que aplican reglas. En cambio, está orientada al proceso y varía sustancialmente de una organización a otra. Por ejemplo, al igual que con cualquier proceso de negocio, los controles automatizados y manuales se pueden utilizar simultáneamente. Como resultado, es importante que la organización comprenda los controles que participan en la gestión de identidades y accesos.

Además, es fundamental que la organización comprenda los roles y las responsabilidades de las personas responsables de la gestión del entorno de control y del mantenimiento de los

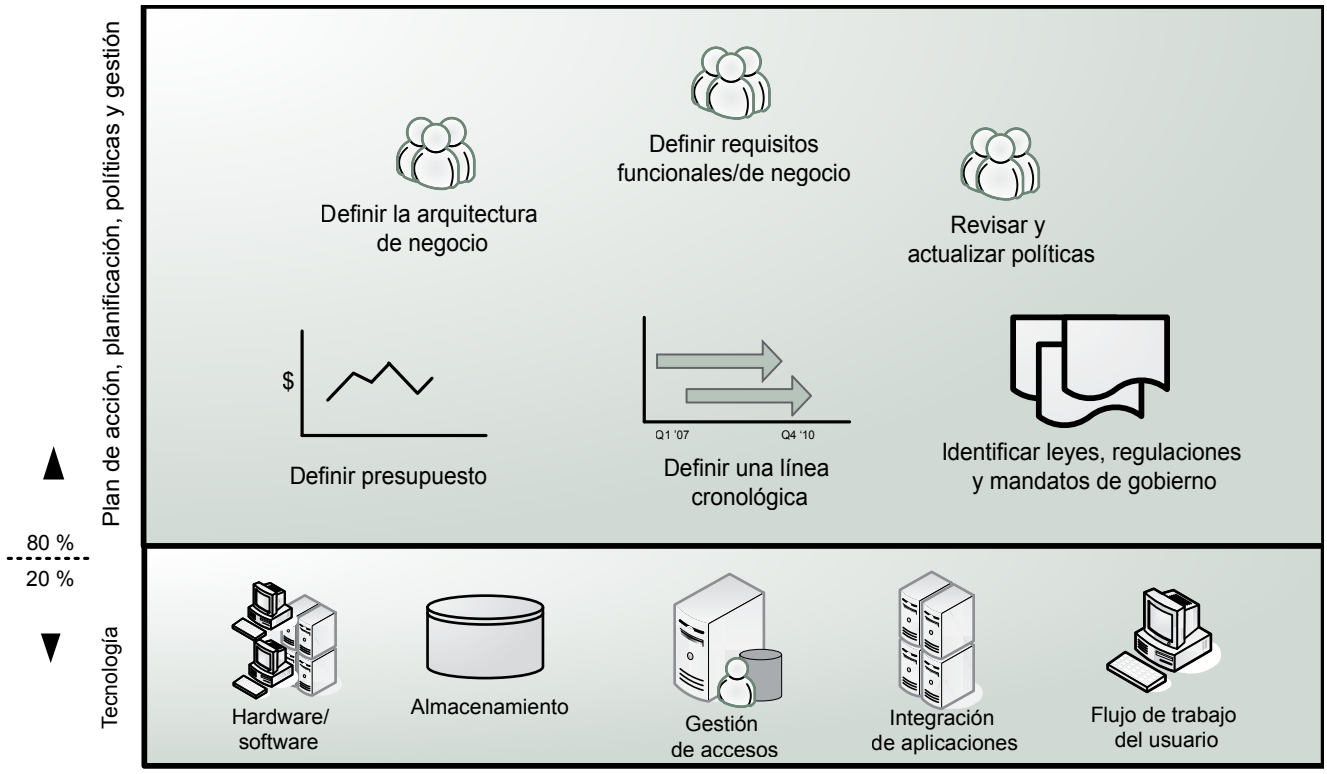

Figura 4. Naturaleza orientada al proceso de IAM

controles. Dado que muchos controles están automatizados o realizan funciones de TI, la dirección muchas veces supone que estos controles son responsabilidad del departamento de TI. No obstante, los gerentes de negocio y los propietarios de datos deben hacerse responsables del proceso de aprobación.

De igual importancia es el compromiso de la alta dirección, en especial, su comprensión respecto de que la IAM requiere la participación del liderazgo de negocio para respaldar adecuadamente los procesos en toda la compañía. Por ejemplo, si la alta dirección no le presta la atención adecuada a la IAM, probablemente la imagen de la organización no respalde la importancia de la IAM.

4.1.2 Políticas

Una vez que la arquitectura de negocio se documenta o, al menos, se comprende dentro de la organización, se deben revisar las políticas y procedimientos existentes que respaldan esta arquitectura y gobiernan la gestión de acceso. Si bien estas políticas muchas veces son de alto nivel y pueden describir el compromiso de una organización para gestionar la información de forma segura, es de igual importancia que las normas, procedimientos, reglas y pautas respalden cada política. Este conjunto de documentación se conoce como el marco de política corporativa.

Además, si bien la jerga y el tipo de documentación serán únicos para cada compañía, es importante que el marco de política proporcione a todos los empleados información suficiente acerca de cómo las identidades y los derechos de accesos de usuarios se gestionarán, revisarán y aprobarán. Por otro lado, el marco de política debe explicar cómo los procesos de negocio, las aplicaciones, los sistemas y los repositorios de datos nuevos se pueden configurar para alinearse con el marco de política y para asegurar que las nuevas políticas no expongan a la organización a un riesgo excesivo.

4.1.3 Leyes, regulaciones y mandatos

Es importante que la organización mantenga una eficiencia operativa y asegure que se implementen los procesos adecuados para permitir que el negocio cumpla con las distintas leyes, regulaciones y mandatos nacionales y locales. No basta con comprender estas leyes y regulaciones; las organizaciones deben determinar cómo las aplicarán a los procesos de IAM.

En muchos casos, los tipos de datos que se pueden recabar y transferir más allá de los límites del país están definidos estrictamente. Por ejemplo, los países que cuentan con leyes de protección de datos y que deben cumplir con la Norma de protección de datos pueden limitar el tipo de información de los empleados que se puede transmitir a los sistemas y administradores fuera del país de origen del usuario. No obstante, dado que esta información personal puede ser necesaria para realizar revisiones de habilitaciones y otorgar a los usuarios acceso a sistemas alojados en otros países, se deben establecer procedimientos legales que respondan a esta situación y a situaciones similares. Como resultado, al auditar el marco de política que gobierna el manejo de información personal en la organización, se debe establecer un proceso de revisión para determinar si las leyes aplicables se cumplen correctamente.

4.1.4 Presupuesto

La financiación de las iniciativas de IAM debe abordar la implementación de nuevos procedimientos y tecnologías de respaldo, así como también operaciones continuas basadas en nuevos procesos de IAM. Posiblemente se requiera un tiempo y una financiación significativos para generar un cambio organizativo e implementar las herramientas de tecnología que respalden la IAM. Esta financiación puede incluir hardware, software y consultores o contratistas para implementar la tecnología. Una vez implementada la tecnología, se necesita una financiación continua para los aranceles de licencias y el personal de soporte interno y externo. Según el ciclo de presupuesto de la organización, posiblemente sea necesario desarrollar un caso de negocio e introducirlo en el proceso de presupuesto anual.

4.1.5 Línea cronológica (calendario)

Si se ha desarrollado o se está desarrollando un programa de IAM, se debe realizar una evaluación del calendario de su implementación y de su alineación con las necesidades de informes de la gestión de programas que tenga la organización. Si se deben cumplir requerimientos específicos de preparación de informes, es importante que estas fechas sean comunicadas y gestionadas de manera conjunta por el programa de IAM y otras oficinas de gestión de programas. Además, es probable que los programas complejos encuentren problemas relacionados con la línea cronológica. La revisión de estos programas y su habilidad de gestionar correctamente cambios en el calendario le permite al equipo de auditoría determinar la probabilidad que tiene el proyecto de cumplir satisfactoriamente con las fechas y los hitos objetivo futuros.

4.1.6 Requisitos de negocio

Ya sea que exista o no un programa de IAM formal, es importante que todos los sistemas tengan la capacidad de cumplir con los requisitos de desempeño de negocio. Si hay un programa, es necesaria la aplicación de un proceso directo que determine si se recopilaron y revisaron los requisitos de negocio de las partes interesadas antes de iniciar la implementación del programa. En función de la etapa actual del programa, la organización debe ser capaz de revisar si los sistemas existentes proporcionan la funcionalidad requerida para que el programa de IAM funcione correctamente. Si no hay un programa de IAM formal, esto podría resultar más difícil. Posiblemente los requisitos de negocio no se documenten correctamente ni se comuniquen debidamente al personal encargado de la gestión del entorno de TI.

Con el surgimiento de la Ley Sarbanes-Oxley y regulaciones similares en todo el mundo, muchas organizaciones han establecido controles más estrictos sobre los procesos de administración de accesos. Como resultado, debe haber pautas disponibles dentro de la organización con respecto a lo que se requiere para cumplir

con los requisitos reglamentarios. Por último, todos los requisitos deben incluir la capacidad de responder estas preguntas:

- ¿Quién tiene acceso lógico a la información?
- ¿El nivel de acceso es adecuado?
- ¿Quién aprobó el acceso?

4.2 Auditoría de IAM

Ya sea que exista o no un programa definido, los auditores internos deben examinar los procesos de gestión de identidades y accesos que se aplican en la organización.

4.2.1 Evaluación de IAM

Antes de desarrollar un enfoque de auditoría de IAM o ayudar en la creación de procesos de IAM, se deben revisar las políticas y los procedimientos de gestión de identidades existentes. Una vez identificados los procesos actuales, los auditores internos pueden ayudar a la dirección mediante la realización de una evaluación de riesgos que le permitirá a la organización desarrollar un proceso de gestión de identidades eficaz.

Además de realizar una evaluación de riesgos, los auditores internos pueden ayudar a la dirección o al equipo de gestión de identidades a determinar de dónde deben provenir los miembros de equipo nuevos o adicionales dentro de la organización. Los auditores internos pueden ser miembros de equipo valiosos en este aspecto ya que tienen una visibilidad de todos los niveles de la organización y comprenden qué áreas deben contar con un mayor enfoque de gestión de identidades.

Documentar identidades

Como parte del proceso, los auditores deben identificar claramente las distintas identidades de usuarios que existen dentro de la organización. (Consulte la página 6 para obtener una lista de los tipos de identidades). En cada categoría de usuarios y, en particular, en las organizaciones complejas, varios de estos grupos pueden tener subgrupos. Los grupos que, en general, tienen múltiples subgrupos incluyen los proveedores y las cuentas por lote.

Definir los componentes del ciclo de vida de una identidad

Los componentes del ciclo de vida de una identidad abarcan el establecimiento, la administración y la puesta en vigor. Para definir los componentes del ciclo de vida de una identidad, los auditores deben determinar el proceso, los controles y la documentación que se relacionan con el proceso de establecimiento. Por ejemplo, si los procesos son manuales, ¿qué orientación o capacitación han recibido los administradores? Si los procesos son automatizados, ¿se genera algún tipo de retroalimentación para identificar si estos están funcionando?

Determinar los controles dentro del proceso de ciclo de vida de una identidad

Como sucede con cualquier proceso, es fundamental identificar los controles que lo afectan. Dentro del proceso de ciclo de vida de una identidad, existen varias áreas de control clave que deben ser revisadas. Los controles pueden incluir procesos de aprobación para la creación de identidades, procesos de revocación de accesos, revisiones de habilitaciones y registro de accesos.

Antes de crear una identidad, alguien de la organización debe aprobarla. Por ejemplo, es probable que un gerente apruebe la contratación de un nuevo empleado. Este gerente de contratación trabajará con recursos humanos para ayudar a establecer la identidad de la persona en el sistema. Por lo general, en este proceso se recopila información personal, se determina si la persona ha trabajado anteriormente para la compañía y, finalmente, se crean cuentas informáticas para la persona. Cada paso de este proceso se debe revisar para determinar que existan los controles adecuados durante el ciclo de vida de la identidad, ya que se debe controlar la creación de identidades para evitar la introducción de usuarios desconocidos en el entorno.

Además, la organización necesita desactivar o eliminar correctamente las identidades de usuarios que ya no son necesarias. Por lo tanto, las políticas deben identificar claramente cómo se debe proceder cuando la persona deja la organización. También se deben realizar revisiones para confirmar que se haya llevado a cabo la acción adecuada.

Determinar repositorios de identidades

Para identificar repositorios, los auditores deben determinar dónde se almacena la información acerca de las identidades. Por lo general, esto incluirá áreas como recursos humanos, repositorios de bases de datos de contratistas, bases de datos de proveedores de servicios tercerizados y bases de datos de fuerza de ventas externas.

Para las cuentas que no pertenecen a personas, incluidas las cuentas de sistema, podría resultar más difícil documentar la información acerca de cómo fueron creadas, quién tiene acceso a ellas y qué información acerca de las cuentas se almacena y se mantiene. No obstante, debe existir una metodología para documentar los tipos de cuentas que se encuentran en uso.

Documentar los controles para los repositorios de identidades

Una vez identificados los repositorios de identidades, se deben evaluar los controles utilizados para proteger los datos que residen en esos repositorios. Esta tarea requerirá varias revisiones detalladas que abarcan múltiples controles. No obstante, las revisiones se pueden realizar de la misma manera que las revisiones tradicionales de sistemas, bases de datos y aplicaciones. Por ejemplo:

- ¿Las máquinas que almacenan la información son seguras?
- ¿Según qué normas son seguras?
- ¿La organización mantiene normas respecto de cómo gestionar y operar estos sistemas?

- ¿Los sistemas están sujetos a las mismas normas que las aplicaciones financieras en general?
- ¿El acceso a los sistemas, herramientas y repositorios de datos de IAM se gestiona a través del sistema de IAM o a través de otros medios?

4.2.2 Evaluación de la gestión de habilitaciones

Documentar habilitaciones

Los procesos eficaces de gestión de habilitaciones deben documentar las habilitaciones que se otorgan a los usuarios de plataformas, aplicaciones y funciones dentro de las aplicaciones, entre otros. Como parte de su rol, los auditores deben determinar cómo se agrupan las habilitaciones y qué permisos tienen los usuarios, los dispositivos de TI, las cuentas de servicio, las cuentas de máquina y las cuentas por lote.

Documentar el ciclo de vida de la autorización

Los auditores deben determinar y documentar las diferencias entre el ciclo de vida de la autorización y el ciclo de vida de la identidad. Por lo general, de alguna manera, se deben identificar los siguientes pasos principales: creación de la autorización, asignación de la autorización y eliminación de la autorización.

Además, los auditores deben tener en cuenta que los programas de IAM de gran magnitud pueden tener procesos establecidos para la creación de nuevas habilitaciones, para la agrupación y para su asignación a las personas o funciones dentro de la organización, mientras que las organizaciones pequeñas pueden utilizar formularios en papel u hojas de cálculo para solicitar y rastrear accesos. Independientemente del método utilizado, es necesario que en la organización haya una persona encargada de aprobar el acceso y garantizar que sea otorgado al sistema o a la aplicación.

Determinar los controles del ciclo de vida de la autorización

La aprobación del acceso es uno de los controles clave en el ciclo de vida de la gestión de habilitaciones. Se debe prestar suma atención a este proceso, según la naturaleza de la organización. Por ejemplo, en compañías más pequeñas, la concesión de derechos de acceso muchas veces es una decisión directa. No obstante, en organizaciones más grandes, puede resultar difícil determinar qué acceso necesita realmente una persona para realizar su trabajo. Además, debido a la estructura compleja de preparación de informes y gestión de muchas organizaciones, puede resultar difícil para la persona encargada de la aprobación conocer la clase de acceso que requiere un individuo para realizar una determinada función laboral. Por último, se deben aplicar controles para garantizar que los sistemas se configuren sólo después de recibir una aprobación correcta.

Determinar los repositorios de habilitaciones

Los repositorios de habilitaciones tienen una variedad de mecanismos de puesta en vigor que deben ser configurados correctamente. Para este fin, muchas aplicaciones son capaces de gestionar habilitaciones en forma independiente. Muchas veces, esta actividad incluye la ejecución de funciones de autenticación y autorización. Por ejemplo, las aplicaciones pueden aprovechar un mecanismo de autenticación central, como un directorio, o un mecanismo de autorización central, como un portal o tecnología de gestión de accesos de Web.

Muchos procesos de negocio dependen de varias aplicaciones y utilizan distintos mecanismos para la puesta en vigor de autenticaciones y autorizaciones. Independientemente del mecanismo de autorización utilizado, los auditores deben identificar dónde se almacena y cómo se gestiona la información de habilitaciones.

Documentar los controles para los repositorios de habilitaciones

El aspecto más importante que se debe revisar al documentar los controles para los repositorios de habilitaciones es si el sistema auditado contiene las habilitaciones correctas. Por ejemplo, los auditores deben determinar si el repositorio de habilitaciones refleja adecuadamente las habilitaciones que ya se encuentran establecidas. Muchas veces, pueden existir discrepancias entre lo que es y lo que debería ser. Así, determinar dónde radican las debilidades puede ser un desafío.

Como sucede con la información del repositorio de identidades, todos los sistemas estándar, las bases de datos y las normas de seguridad de las aplicaciones deben ser revisadas. Al igual que en la revisión de controles de repositorios de identidades, se deben realizar revisiones de las configuraciones de máquina de la misma manera que se realizan otras revisiones de configuraciones.

Identificar cómo se realizan la conciliación y la supervisión

La función principal de la conciliación es verificar que el acceso real esté alineado con el acceso aprobado, como se describió anteriormente. Muchas organizaciones han implementado procesos específicos para la revisión y conciliación de accesos. Las siguientes tres preguntas abordan varios elementos clave del proceso que se deben revisar:

1) ¿Se realiza una conciliación repetida y confiable?

Los auditores deben revisar la ejecución de los procesos de conciliación para determinar si son sostenibles y repetidos. Además, los auditores deben revisar estos procesos para determinar su confiabilidad, es decir, ¿el proceso realmente genera una mejora medible en el estado del control de acceso lógico?

No basta con revisar el acceso lógico y determinar si es adecuado. Muchas organizaciones grandes han encontrado revisiones ficticias en las que la persona responsable de realizar la revisión sella una aprobación en el informe de habilitaciones como resultado de su incapacidad de manejar la cantidad de usuarios que debe revisar.

Dado que el proceso de revisión se podría considerar como una forma de validación de identificación, la persona que realiza la

revisión debe tener cierto conocimiento de la persona que está refrendando (es decir, debe afirmar que la persona necesita obtener acceso a una aplicación). Si las personas que validan el acceso no pueden conocer a todos los usuarios, debe implementarse un proceso más eficaz. En esta situación, una posibilidad sería que los gerentes de niveles inferiores realicen las revisiones de sus empleados directos, en lugar de que sean realizadas por ejecutivos de rango superior que casi nunca interactúan con los empleados.

2) ¿Con qué frecuencia se realizan las conciliaciones?
Muchas organizaciones realizan revisiones de conciliaciones dos veces al año. No obstante, una vez aplicada la automatización, el proceso se podría realizar prácticamente una vez al día y las excepciones se podrían reparar o informar automáticamente a las personas encargadas de gestionar el acceso.

3) ¿Cómo se manejan las conciliaciones?
Para responder esta pregunta, los auditores podrían preguntar lo siguiente:

- ¿Qué sucede cuando se lleva a cabo un evento de conciliación (es decir, qué sucede cuando lo que es no coincide con lo que debería ser)?
- ¿El evento simplemente se registra para su posterior revisión?
- ¿Los sistemas se reconfiguran automáticamente para alinearse con lo que debería ser?
- ¿Qué pasos se llevan a cabo para identificar la causa raíz del problema?
- ¿El evento sólo es un problema tecnológico o una persona realizó un cambio no autorizado en el sistema?

Apéndice A: Lista de verificación de revisión de IAM

Al auditar la gestión de identidades y accesos (IAM, en inglés), el desglose de la información en tres áreas temáticas (administración, establecimiento y puesta en vigor) permite realizar una revisión completa del entorno y responder ciertas preguntas clave. La siguiente lista de verificación es un panorama general de alto nivel y no pretende ser un programa de auditoría integral ni abordar todos los riesgos relacionados con la IAM.

Áreas temáticas:

- **Administración** — ¿Qué se ha establecido para desarrollar y mantener una estrategia de IAM adecuada, políticas, procedimientos y operaciones continuas?
- **Establecimiento** — ¿Cómo se otorga, supervisa y elimina el acceso dentro del entorno?
- **Puesta en vigor** — ¿Existen medidas adecuadas para impedir, evitar y detectar los intentos de evasión de los procesos de IAM?

Pregunta o tema de auditoría	Estado
1.1 ¿Existe una estrategia de IAM? Un elemento crítico de un proceso de IAM eficaz es la presencia de un enfoque coherente para gestionar la infraestructura de tecnología de la información (TI) de respaldo. Contar con una estrategia consecuente a través de la organización permitirá que todos los departamentos gestionen personas, sus identidades y los accesos que necesiten utilizando procesos similares, si bien, no necesariamente la misma tecnología. • Pregunte por las estrategias de IAM actuales en la organización. • Si existen, determine cómo se gestionan y quién las gestiona.	
1.2 ¿La dirección y las demás personas relevantes comprenden correctamente los riesgos asociados con el proceso de IAM? ¿La estrategia aborda los riesgos? Contar con una estrategia no garantiza que se cubran todos los riesgos que podría presentar la IAM. Es importante que la estrategia contenga elementos que identifiquen todos los riesgos relevantes. • Determine si se realizó una evaluación de riesgos de los procesos de IAM establecidos. • Determine cómo se identifican y abordan los riesgos.	
1.3 ¿La organización crea o modifica un proceso de IAM sólo para satisfacer las cuestiones reglamentarias? Es fundamental que los procesos de IAM se integren con asuntos y estrategias de negocio más amplios. Existen muchos beneficios de contar con un entorno de IAM sólido, por ejemplo, tener un entorno de control interno más eficaz. • Determine las necesidades de la organización con respecto a IAM. • Determine si los procesos de IAM se amplían en la organización o sólo cumplen con un requerimiento de terceros externos.	
1.4 ¿Las regulaciones que rigen la organización se comprenden correctamente? Se están creando nuevas regulaciones y, para las grandes organizaciones multinacionales, puede resultar difícil identificar todos los requisitos reglamentarios que deben cumplir. • ¿Cómo la organización determina los requisitos reglamentarios que debe cumplir? • ¿Cómo la organización se mantiene actualizada respecto de estas regulaciones? • ¿Cómo la organización captura, almacena y recupera esta información?	

Pregunta o tema de auditoría	Estado
1.5 ¿Existen métodos definidos para abordar adecuadamente los problemas relacionados con la separación de funciones? Si bien muchas áreas del negocio han definido reglas para gestionar los problemas relacionados con la separación de funciones, por lo general, no están documentadas ni se comprenden correctamente. La pregunta principal que debe hacerse es si los gerentes u otras personas responsables de la aprobación de accesos son capaces o no de reconocer cuándo se presenta alguna debilidad de separación de funciones. • ¿Los conflictos de separación de funciones están identificados dentro del proceso de IAM? • ¿Cómo se tratan estos conflictos? ¿Quién trata con ellos? • ¿Existen mecanismos para capturar o identificar estos conflictos antes de que se otorgue el acceso?	
1.6 ¿El entorno de IAM se centraliza o se distribuye correctamente para reflejar la estructura de la organización? Una situación técnica ideal sería tener una solución de software única con procesos coherentes claramente documentados y gestionados a través de una herramienta de implementación única. No obstante, debido a los desafíos asociados con la integración de sistemas heredados y la modificación de procesos utilizados para otorgar aprobaciones, estas tecnologías no pueden estar a la altura de su potencial. • Si existen múltiples soluciones de IAM, ¿cómo se gestionan para identificar, evitar o detectar permisos no autorizados o innecesarios otorgados a los usuarios?	
1.7 ¿Cómo se establecen las políticas de contraseñas? Y estas, ¿son suficientes para la organización? Las políticas que rigen los procesos de IAM son componentes fundamentales de cualquier solución eficaz. Por lo tanto, es importante comprender cómo se establecen las políticas, cómo se comunican y cómo los elementos tecnológicos del entorno respaldan su cumplimiento. • ¿Qué parámetros de contraseñas se han establecido para las aplicaciones de toda la compañía? • ¿Se aplican de manera coherente? • ¿Cómo se controlan los cambios realizados en estos parámetros?	

Pregunta o tema de auditoría	Estado
2.1 ¿La organización cuenta con procesos coherentes para gestionar el acceso al sistema? Varios aspectos del establecimiento generan preguntas. Estas preguntas, que se deben hacer y en última instancia se deben responder, se relacionan con el conocimiento de las personas respecto de los procesos, la documentación generada y la adhesión a los procesos especificados. • Determine si existen políticas y procedimientos relacionados con la IAM en la organización. • Determine si las políticas y procedimientos se han comunicado a las personas correspondientes en la organización.	
2.2 ¿Los auditores pueden identificar, de manera exclusiva, a las personas a las que se les otorga acceso a los sistemas de la organización basándose en las credenciales de registro que se les asignan? Un elemento crítico dentro del proceso de establecimiento es la capacidad de identificar correctamente a las personas para las que se gestiona el acceso. • ¿Existen identificadores exclusivos para los usuarios de recursos de TI? • ¿Cómo se rastrean y se registran estos identificadores?	
2.3 ¿Se degrada la productividad de los empleados debido a que es demasiado difícil obtener y mantener el acceso al sistema? Como se describió anteriormente, los impulsores clave de la adopción de un sistema de IAM son los requisitos reglamentarios que exigen mejores controles. Existen beneficios claros para la implementación de estos tipos de sistemas. No obstante, los procesos manuales que, por lo general, se emplean para gestionar el acceso no son capaces de proporcionar acceso inmediato a estos sistemas. • ¿Cómo se gestiona el proceso de IAM en la organización? • ¿Existen beneficios si una parte del proceso de IAM se torna autosuficiente para los usuarios (por ejemplo, el restablecimiento de contraseñas o el uso de una aplicación de soporte informático frente a un número de llamada?	
2.4 ¿Quién debe aprobar el acceso de un usuario en el entorno? Esta es una pregunta importante que se debe responder. Otra pregunta es si debe haber varias personas que participen en el proceso de concesión de aprobaciones. • Determine los métodos utilizados para aprobar las solicitudes de acceso de usuarios. • Determine si la aprobación se basa en la unidad de negocio o departamento de TI. • Determine cómo se aprueban los conflictos de separación de funciones.	
2.5 ¿Puede la organización demostrar que sólo las personas adecuadas tienen acceso a la información? Esta es una pregunta crítica para que responda un auditor. No obstante, puede resultar difícil demostrar que la organización tiene control sobre el acceso de usuarios. • ¿Con qué frecuencia la organización revisa el acceso otorgado a sus usuarios? • Si se realiza una revisión, ¿cómo se identifica, registra y aborda el acceso inadecuado?	

Pregunta o tema de auditoría	Estado
2.6 ¿Existen controles adecuados para evitar que las personas agreguen accesos a los sistemas y aplicaciones fuera del proceso aprobado? Contar con un proceso que gestione las identidades y accesos a los sistemas y aplicaciones sería una situación ideal. No obstante, ¿cómo las organizaciones pueden garantizar que las personas no evadan el proceso y agreguen sus propias cuentas o las cuentas de otros sin la debida autorización o sin cumplir con los procesos definidos? • Determine qué persona de la organización tiene la capacidad de agregar, modificar o eliminar usuarios de las aplicaciones utilizadas en el entorno. • Determine si existe alguna revisión periódica de usuarios que rastree sus permisos de acceso y los formularios de solicitudes de acceso.	
2.7 Cuando las personas dejan la organización, ¿se identifica qué acceso al sistema tenían estas personas? ¿Se revoca el acceso de manera oportuna? Uno de los principales hallazgos en la auditoría de IAM es la persistencia de cuentas que siguen teniendo acceso mucho tiempo después de que los propietarios de las cuentas dejaron la organización. El desafío consiste en identificar todo acceso asociado con un usuario específico. • ¿Cuenta la organización con un proceso para desactivar o eliminar permisos de acceso de usuarios cuando ya no son necesarios? • ¿Cómo la organización garantiza que se hayan desactivado o eliminado todos los nombres de cuenta asociados con una determinada persona?	
2.8 ¿Qué hace la organización con respecto a las cuentas que no pertenecen a personas? Las cuentas que no pertenecen a personas constituyen un desafío por varios motivos, de los cuales, uno de los más importantes es determinar los controles asociados con estos tipos de cuentas. • ¿Qué funciones realiza la cuenta? • ¿La cuenta es necesaria y debe estar activa? • ¿Quién tiene acceso a la cuenta? • ¿Existe una contraseña compartida para la cuenta? • ¿Cuántas personas conocen la contraseña? • ¿Cómo lleva el control de las acciones realizadas por la cuenta?	
2.9 ¿Qué hace la organización con respecto a las cuentas privilegiadas? Las cuentas privilegiadas proporcionan un grupo único de desafíos. Estas cuentas son necesarias para gestionar el entorno y para proporcionar soporte constante, oportuno y de alta calidad. No obstante, las cuentas privilegiadas también tienen la capacidad de evadir muchos de los controles establecidos para gestionar el acceso de las cuentas típicas. • Determine las personas de la organización que poseen permisos de acceso privilegiado a las aplicaciones utilizadas en la organización. • ¿Cómo se solicitan, aprueban y otorgan los permisos de acceso privilegiado? • ¿Con qué frecuencia se revisan los permisos de acceso otorgados?	

Pregunta o tema de auditoría	Estado
3.1 ¿Qué solidez tienen los controles establecidos para evitar que las personas evadan los controles de autenticación o autorización? Uno de los desafíos más urgentes para las aplicaciones es la puesta en vigor del acceso y la forma en que las aplicaciones individuales gestionan la autenticación y la autorización. • Determine el medio de autenticación utilizado para las aplicaciones existentes. • Determine si el medio de autenticación presenta oportunidades para que los usuarios evadan el proceso de autenticación (por ejemplo, contraseñas débiles o almacenadas).	
3.2 ¿Existe un enfoque uniforme para aplicar el acceso? El liderazgo de TI debe definir cómo se manejará este problema y cómo los sistemas aplicarán las decisiones tomadas. • Las contraseñas, ¿están sincronizadas entre las aplicaciones utilizadas en la organización? • Si se utilizan de alguna manera, ¿cómo se gestionan los mecanismos de sincronización? • Sin sincronización, ¿qué mecanismos se aplican para evitar que los usuarios accedan a aplicaciones a las cuales no se les ha otorgado acceso?	
3.3 ¿Cómo se registra, recopila y revisa la información? Es importante comprender qué tipos de eventos se registran, dónde se capturan y con qué frecuencia se revisan. • Determine si la organización utiliza un registro de eventos para la IAM. • Si se utilizan registros de eventos, determine cuándo y cómo se revisan. • Si se revisan los registros y se descubren discrepancias, ¿cómo se resuelven estos problemas?	

Apéndice B: Información adicional

Se puede obtener información adicional de las siguientes fuentes externas:

- Canaudit, www.canaudit.com.
- Revista *Chief Information Officer* (CIO) , www.cio.com.
- Revista *Chief Security Officer* (CSO) , www.csoonline.com.
- Objetivos de Control de Información y Tecnologías relacionadas (CobiT), www.isaca.org/cobit.
- Consejo Federal de Inspección de Instituciones Financieras (FFIEC), www.ffiec.gov.
- IBM Corp., www.ibm.com/software/tivoli.
- ISACA, www.isaca.org.
- El Instituto de Auditores Internos, www.theiia.org.
- Microsoft Corp., www.microsoft.com/technet/security/guidance/identitymanagement.
- Oracle, www.oracle.com/products/middleware/identity-management/identity-management.html.
- Junta de Supervisión de Firmas de Contabilidad Pública (PCAOB), www.pcaobus.org.
- Instituto de Administración de Sistemas, Auditoría, Red y Seguridad (SANS), www.sans.org.

Glosario

Acceso(s): Derecho o permiso que se otorga a una identidad. Estos derechos de acceso a la información se pueden otorgar para permitir que los usuarios realicen funciones transaccionales en diversos niveles.

Autenticación: Proceso que intenta comparar una identidad con los valores almacenados en un repositorio de identidades. Es una forma de validar que los usuarios realmente sean quiénes afirman ser.

Autorización: Proceso utilizado para determinar qué tipos de actividades se permiten. Comúnmente, una vez que el usuario ha sido autenticado, puede obtener autorización para realizar distintos tipos de actividades o se le pueden otorgar ciertos derechos de acceso.

Autorización confidencial: Recuso o acceso identificado para presentar potencialmente un nivel de riesgo de seguridad a la organización, si se establece o cuando se establece. Los ejemplos incluyen autoridades especiales, grupos de administradores de dominios y acceso a la cuenta raíz.

Establecimiento: Proceso utilizado para crear una identidad, asociar identidades con accesos y configurar los sistemas en consecuencia.

Evento de ciclo de vida: Evento que sucede durante el ciclo de vida de un usuario y que puede activar un proceso del sistema de IAM (por ejemplo, la cesación o transferencia).

Habilitaciones: Acceso a una funcionalidad específica en un sistema o aplicación que se otorga a un usuario específico. La mayoría de las personas de una organización poseen múltiples habilitaciones otorgadas para acceder a varios sistemas.

Identidad: Secuencia o conjunto de características único que identifica, de manera exclusiva, a una persona.

ID de usuario: Identificador o ID de inicio de sesión correspondiente a un recurso específico que se utiliza para gestionar el acceso a ese recurso.

Incorporación: Proceso que permite identificar a una persona para incorporarla a una organización como empleado o contratista, proporcionándole las herramientas necesarias para realizar su trabajo y creando una identidad, cuentas y acceso adecuados para sus funciones.

Modelo de seguridad: Regla de seguridad incorporada a una aplicación que conecta el nivel inferior de seguridad (es decir, la configuración de seguridad) con el nivel superior de seguridad (es decir, los grupos de seguridad). Los grupos de seguridad son asignados a los usuarios.

Recurso: Objeto del sistema de IAM que puede ser solicitado por un usuario. Puede ser una aplicación, un componente de la infraestructura de tecnología (por ejemplo, un sistema) o una autorización o acceso específico (por ejemplo, grupo o perfil).

Repositorio de gestión de identidades y accesos (IAM): Instalación de almacenamiento de datos que aloja todos los datos actuales e históricos relacionados con el sistema de IAM.

Separación: Proceso a través del cual una persona deja una función como empelado o contratista de la organización, devuelve los activos físicos que se le asignaron, se le revocan los derechos de acceso físico y se le cancelan los derechos de acceso lógico (es decir, a aplicaciones y sistemas).

Separación de funciones: Mecanismo de control por medio del cual un proceso se divide en sus componentes constitutivos y la responsabilidad de ejecutar cada componente se divide entre las distintas personas. La separación de funciones segmenta el proceso de manera que ninguna persona tenga una capacidad excesiva de ejecutar transacciones o cubra unilateralmente las irregularidades sin detección.

Sistema de IAM: Sistema que consiste en uno o más subsistemas y componentes que facilitan el establecimiento, la gestión y la revocación de identidades y accesos a recursos.

Transferencia: Evento del ciclo de vida por medio del cual un usuario cambia sus responsabilidades o funciones laborales.

Acerca de los autores

Frank Bresz, CISSP
Frank Bresz es director ejecutivo de la oficina de servicios financieros de Ernst & Young, en la que es responsable de la estrategia de seguridad de los sistemas de información y de las operaciones de programas estratégicos. Bresz ha trabajado con los clientes para desarrollar sus programas de seguridad de la información y se ha concentrado en alinear la visión del programa de seguridad con las regulaciones existentes y pendientes.

Bresz tiene más de 22 años de experiencia en operaciones de seguridad de la información y centros de datos, y tiene una sólida trayectoria en el desarrollo de grandes programas de gestión de identidades y accesos (IAM, en inglés) como parte de iniciativas más amplias de seguridad de la información. Antes de trabajar en Ernst & Young, fue responsable de la gestión de tecnología de la información (TI) durante 10 años y trabajó muchos años en Sybase en el desarrollo de aplicaciones basadas en Web.

Bresz obtuvo su título universitario en ciencias de la computación en la Universidad de Pittsburgh. Es profesional certificado de seguridad de sistemas de información.

Sajay Rai, CISSP, CISM
Sajay Rai es socio en la práctica de servicios de consultoría de riesgos de Ernst & Young. Tiene más de 30 años de experiencia en TI, en especial, en las disciplinas de seguridad de la información, continuidad del negocio y gestión de riesgos. Rai trabajó anteriormente en IBM como director general de la práctica nacional de continuidad del negocio y consultoría de contingencia. Desempeñó un papel fundamental en el inicio de la práctica de consultoría de seguridad de la información de la compañía y en la gestión de la práctica de consultoría de TI en América Latina.

Rai es coautor del libro recientemente publicado, *Defending the Digital Frontier: A Security Agenda*, que brinda orientación a los ejecutivos de negocios y TI sobre cómo desarrollar un programa de seguridad de la información eficaz y eficiente. Ha sido mencionado en *Crain's Cleveland Business Who's Who in Technology*.

Rai obtuvo una maestría en gestión de la información en Washington University y un título universitario en ciencias de la computación en Fontbonne College. Es profesional certificado de seguridad de sistemas de información y administrador certificado de seguridad de la información.

Tim Renshaw, CISSP
Tim Renshaw es asesor senior en la oficina de servicios financieros de Ernst & Young. Tiene experiencia en gestión de programas y TI en industrias farmacéuticas y servicios financieros. Renshaw ha desarrollado estrategias de implementación de IAM para varias instituciones mundiales de servicios financieros y ha trabajado con los clientes en la industria de servicios financieros para desarrollar programas de evaluación de riesgos y planes estratégicos de seguridad de la información. Además, ha establecido y administrado oficinas de gestión de programas de TI, ha realizado revisiones independientes de proyectos de implementación de tecnología en toda la empresa y ha respaldado iniciativas de reingeniería de procesos de negocio.

Renshaw obtuvo su título universitario en sistemas de información y en economía en la Universidad Carnegie Mellon. Es profesional certificado de seguridad de sistemas de información.

Jeffrey Rozek, CISSP
Jeffrey Rozek es gerente senior en la práctica de servicios de consultoría de riesgos globales en Ernst & Young, donde se especializa en seguridad de la información. Tiene aproximadamente 15 años de experiencia en seguridad y sistemas de información en industrias de servicios financieros, telecomunicaciones, fabricación y servicios públicos. Rozek ha conducido varios proyectos de seguridad, que incluyen implementaciones de gran escala, multinacionales y en varios idiomas, y se ha concentrado en proporcionar soluciones de control, autenticación y autorización de accesos. Ha trabajado en varias compañías de Fortune 100 en la evaluación y el desarrollo de enfoques generales de riesgos y seguridad y modelos de madurez. Además, ha ayudado a clientes en el desarrollo, diseño e implementación de arquitecturas de seguridad técnica.

Rozek obtuvo su título universitario en contabilidad en John Carroll University y es profesional certificado de seguridad de sistemas de información.

Torpey White, CPA, CISA

Torpey White es director de la práctica de consultoría de gestión de Goldenberg Rosenthal, donde brinda servicios de asesoría y certificación a organizaciones de Fortune 1000, de mercado intermedio y sin fines de lucro. White tiene experiencia en evaluaciones de control interno, revisiones operativas, examinaciones de Declaración sobre Normas de Auditoría Nº 70, administración de proyectos de la Ley Sarbanes-Oxley de 2002 Sección 404 de Estados Unidos, auditoría interna, asistencia contable, informes y análisis financieros, análisis de procesos de negocio y documentación y reingeniería de procesos de negocio.

White tiene 20 años de experiencia y ha trabajado para organizaciones de distintas industrias, que incluyen organizaciones en sectores de desarrollo de software, servicios públicos, concesionarios y subastas de automóviles, hipismo, servicios de salud, organizaciones sin fines de lucro e industria liviana. Además, se dedica a la gestión y desarrollo de planes de auditoría interna, implementaciones de sistemas financieros, presupuestos y pronósticos, soporte de sistemas heredados, soporte de adquisiciones e implementaciones de proyectos especiales.

White obtuvo sus títulos universitarios en contabilidad y finanzas en la Universidad de LaSalle. Es contador público certificado y auditor certificado de sistemas de información.

Los revisores

El IIA agradece a las siguientes personas y organizaciones que brindaron valiosos comentarios y agregaron gran valor a esta guía:

- Ken Askelson, JCPenney, Estados Unidos.
- Lily Bi, IIA.
- Lawrence P. Brown, The Options Clearing Corp., Estados Unidos.
- Tim Carless, Chrysler Financial, Estados Unidos.
- Christopher Fox, ASA, eDelta, Nueva York, Estados Unidos.
- Nelson Gibbs, Deloitte & Touché LLP, Estados Unidos.
- Steve Hunt, Enterprise Controls Consulting LP, Estados Unidos.
- Stuart McCubbrey, General Motors Corp., Estados Unidos.
- Heriot Prentice, IIA.
- James M. Reinhard, Simon Property Group Inc., Estados Unidos.
- Paula Stockwell, IBM Corp., Estados Unidos.
- Jay R. Taylor, General Motors Corp., Estados Unidos.
- Hajime Yoshitake, Nihon Unisys Ltd., Japón.

GTAG®

Gestión de identidades y accesos

La gestión de identidades y accesos (IAM, en inglés) es un proceso interfuncional que ayuda a las organizaciones a gestionar quién tiene acceso a qué información durante un período determinado. Este proceso se utiliza para iniciar, capturar, registrar y gestionar las identidades de usuarios y los permisos de acceso relacionados a la información confidencial de la organización. Los procesos de IAM deficientes o poco controlados pueden ocasionar una falta de cumplimiento de las regulaciones organizativas y una incapacidad para determinar si se está haciendo un uso indebido de los datos de la compañía.

Los directores ejecutivos de auditoría (DEA) deben participar en el desarrollo de la estrategia de IAM de la organización, así como también evaluar la implementación de la estrategia y la eficacia de los controles de acceso en toda la compañía. El objetivo de esta Guía de Auditoría de Tecnología Global (GTAG, en inglés) es proporcionar percepciones acerca de lo que significa la IAM para una organización y sugerir áreas de auditoría interna para la investigación. Puede ayudar a los DEA y a otros auditores internos a comprender, analizar y supervisar los procesos de IAM de la organización.

Visite www.theiia.org/guidance/technology/gtag/gtag9 para calificar esta GTAG o enviar comentarios.

The Institute of Internal Auditors

www.theiia.org