Planificación de la fuerza laboral de Administración de Identidades y Accesos

Coloca la identidad al centro de tu fuerza laboral de ciberseguridad.

Por Kenneth M. Myers
© 2022 IDPro, Kenneth M. Myers

Tabla de contenidos

Resumen

Este artículo propone un abordaje práctico para ayudar a los profesionales de la Administración de Identidades y Accesos (IAM) a aconsejar a los directivos de una empresa sobre la planificación de la administración de identidades y accesos de la fuerza laboral. Si bien normalmente la planificación de la fuerza laboral es una tarea del área de Recursos Humanos (RRHH), el profesional IAM, los gerentes a cargo de contratar personal y los equipos de RRHH deberían conocer las tareas, el conocimiento y las habilidades necesarias dentro de la industria IAM. Este modelo de competencias puede adaptarse a las necesidades de capacitación del personal de áreas específicas de la mayoría de las empresas ya que plasma las tareas, el conocimiento y las habilidades implicadas en cada una de las áreas que conforman los servicios de administración de las identidades y accesos.

Sirviéndose de las Infraestructuras IAM del gobierno federal de los Estados Unidos, este artículo se propone colaborar en la maduración y consolidación de la profesión de la administración de identidades y accesos a lo largo de las empresas, permitiendo que los profesionales de la IAM lleven adelante una experiencia IAM consistente.

Palabras clave: administración de identidades y accesos, ciberseguridad, planificación de la fuerza laboral, modelo de competencia, arquitectura de empresa, función laboral

Introducción

La Administración de Identidades y Accesos (IAM) es una profesión desafiante. En general, la primera interacción de un nuevo empleado o cliente con una organización es un proceso de identidad que muchas veces no es amigable. Estas interacciones pueden incluir:

1. Completar varias veces un formulario de solicitud de empleo para comprobar la identidad.
2. Crear un nombre de usuario y contraseña en casi todos los sitios web para autenticación.
3. Realizar varias solicitudes de acceso a los equipos de soporte técnico y a veces esperar varios días o semanas para su aprobación.

La administración de identidades y accesos es fundamental para las transacciones digitales. Cuando quienes están a cargo de las tareas diarias de identidad no son profesionales de la identidad, las organizaciones pueden enfrentarse a errores en la configuración, malas experiencias de usuario y potenciales filtraciones de la información. Más aún, las organizaciones que carecen de una visión integral de la seguridad y el control de accesos se exponen a un riesgo mayor. Para esclarecer las responsabilidades laborales y determinar las habilidades que son necesarias para cumplir cada función, las organizaciones deben usar un marco de ciberseguridad de la fuerza de trabajo en la planificación de su fuerza laboral.

- Un marco de la fuerza de trabajo es un conjunto de **tareas, conocimientos y habilidades (TKS, por sus siglas en inglés)** para que una persona pueda realizar su trabajo.
- La planificación de la fuerza de trabajo garantiza que una organización tenga las **habilidades correctas** para cumplir con sus objetivos técnicos y de negocio.

Si bien tanto la planificación de la fuerza de trabajo como su marco son tareas que corresponden esencialmente al equipo de recursos humanos, para que la planificación de la fuerza de trabajo sea exitosa los profesionales IAM deben participar activamente de la misma, proveyendo el TKS necesario para el marco de la fuerza de trabajo. Un marco de fuerza laboral se compone de varias partes.

1. Competencia - Un método para evaluar a una persona. La evaluación de competencias está comprendida en las descripciones TKS.
2. Tarea - una actividad dirigida hacia el logro de un objetivo.
3. Conocimiento - Un conjunto de conceptos recuperables dentro de la memoria. Completar una tarea puede requerir múltiples conceptos.
4. Habilidad - La capacidad de realizar una acción observable.

5. Función laboral - un método consistente para describir las competencias y TKS necesarias para llevar a cabo el trabajo del cual se es responsable.

Es importante aclarar algunos puntos:

1. Un modelo de competencia es un conjunto de TKS necesarias para ejecutar eficazmente un trabajo. Un modelo de competencia forma parte del marco de la fuerza de trabajo.
2. En términos de planificación de la fuerza laboral, un modelo de madurez es un método para medir las capacidades relacionadas con un nivel de pericia o grado de optimización superior.
3. Una función laboral no es lo mismo que el nombre de un cargo. Generalmente, el nombre de un cargo se define a nivel organizacional mientras que la función laboral es una forma consistente de describir un tipo de trabajo. El nombre de un cargo puede ser específico a una organización, pero la función laboral debería ser la misma en todas las organizaciones.

Un nivel de madurez puede incorporar un modelo de competencia para describir el conjunto de TKS de cada nivel de pericia, desde el nivel inicial al nivel superior.

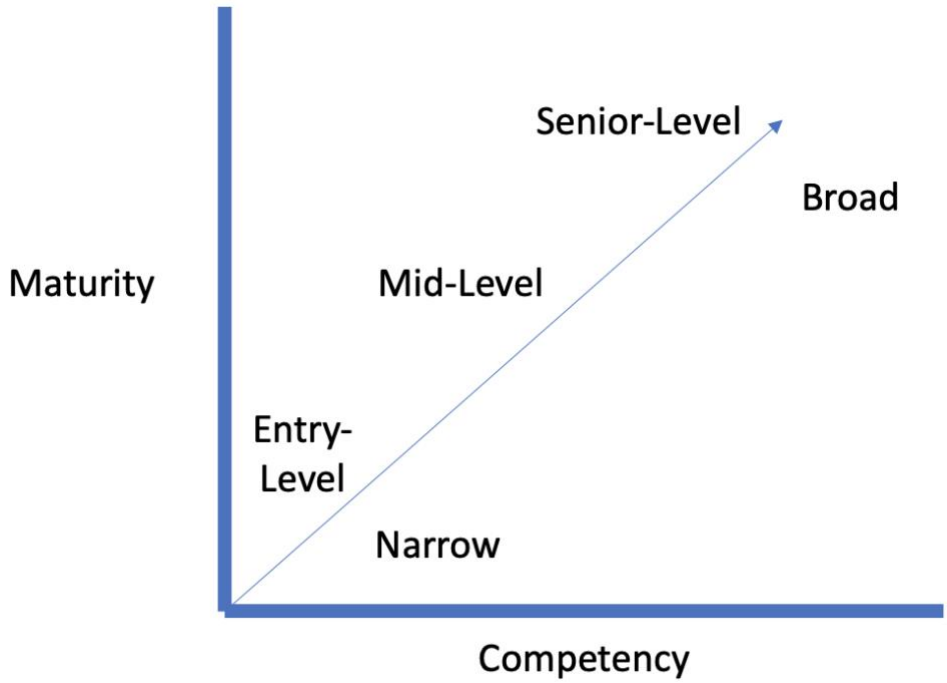

Figura 1. Ejemplo de la interrelación de un modelo de competencia y un modelo de madurez

El presente artículo propone un abordaje práctico para ayudar a los profesionales de la Administración de Identidades y Accesos (IAM) a aconsejar a los directivos de una empresa sobre la planificación de la administración de identidades y accesos de la fuerza laboral. La

siguiente sección resume por qué la profesión IAM necesita su propio modelo de competencia y su propia planificación de la fuerza laboral.

Terminología

- **Gestión de accesos** – Utiliza información de identidad para proveer control de acceso a recursos protegidos como sistemas informáticos, bases de datos o espacios físicos.
- **Atributos** – Pares de claves/valores relevantes para la identidad digital (nombre de usuario, nombre, apellido, etc.)
- **Autenticador** – Son los medios utilizados para confirmar la identidad de un usuario, procesador o dispositivo, como el nombre de usuario o contraseña, un pin de un solo uso o una tarjeta inteligente.
- **Enlazar** – Asociar un autenticador con una identidad.
- **Modelo de competencia** – Conjunto de tareas, conocimiento y habilidades (TKS) necesarias para una ejecución eficaz de un trabajo. Un modelo de competencia forma parte de un marco de fuerza de trabajo.
- **Credencial** - Una credencial permite la autenticación de una entidad enlazando la identidad a un autenticador.
- **Administración de credenciales** – Refiere a cómo emitir, administrar y revocar autenticadores enlazados a identidades. La administración de credenciales se corresponde a grandes rasgos con el término IDPro "Servicios de credenciales". Aquí utilizamos el término administración de credenciales de forma que tenga correlato con los términos de la iniciativa de Identidad Federal, Credenciales y Control de Acceso (FICAM).[1]
- **Administración de Identidades y Accesos** – La disciplina que permite a los individuos correctos acceder a los recursos correctos, en los momentos correctos y por las razones correctas. [2]
- **Planificación de la Administración de Identidades y Accesos de la Fuerza de Trabajo** – Son las actividades que aseguran que una organización tiene las aptitudes necesarias para llevar a cabo los objetivos técnicos y de negocio.
- **Administración de Identidades** – Es un conjunto de políticas, procedimientos, tecnología y otros recursos usados para mantener la información de identidades.
- **Administración de Identidades, credenciales y accesos** – Programas, procesos, tecnologías y personal usados para crear representaciones confiables de identidades digitales de individuos y entidades no humanas, para enlazar esas identidades a credenciales que puedan servir como intermediario en operaciones

[1] Flanagan (Editor), H., (2021) "Terminología en el Cuerpo de Conocimiento de IDPro", *Cuerpo de Conocimiento de IDPro* 1(8). doi: https://doi.org/10.55621/idpro.41.
[2] Gartner. (2021). *Glosario Gartner Glossary*. Extraído de Gartner: https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam.

de acceso y para valerse de las credenciales a fin de proveer un acceso autorizado a los recursos de una organización. [3]

- **Marco de la Fuerza de Trabajo** – Es un resumen de las categorías de trabajo, funciones y modelos de competencia necesarios para ejecutar la planificación de la fuerza laboral.
- **Planificación de la Fuerza de Trabajo** – Son las actividades que aseguran que una organización tiene las habilidades necesarias para llevar a cabo los objetivos técnicos y de negocio.

Acrónimos (por sus siglas en inglés)

- CISM - *Certified Information Security Manager* - Gestor Certificado de Seguridad de la Información
- FICAM – *Federal Identity, Credential, and Access Management - Identidad Federal*, Credenciales y Control de Acceso
- IAM – *Identity and Access Management* - Administración de Identidades y Accesos
- ICAM – *Identity, Credential, and Access Management* - Administración de Identidades, Credenciales y Accesos
- MFA – *Multi-factor authentication* - Autenticación de Múltiples Factores
- NICE – *National Initiative for Cybersecurity Education* - Iniciativa Nacional para la Educación en Ciberseguridad
- NIST – *National Institute of Standards and Technology* - Instituto Nacional de Estándares y Tecnología
- TKS – *Tasks, Knowledge, and Skills* - Tareas, Conocimientos y Habilidades

[3] NIST. (2021b). *Glosario - ICAM*. Extraído del Centro de Recursos para la Seguridad Informática: https://csrc.nist.gov/glossary/term/Identity_Credential_and_Access_Management

Planteamiento del problema

Si bien existen numerosos marcos e investigaciones sobre la planificación general de la fuerza laboral cibernética, hay una carencia de información específica sobre la planificación de la fuerza de trabajo IAM. El gobierno federal de los Estados Unidos pone a disposición gratuitamente numerosos documentos sobre el desarrollo de la planificación de la fuerza de trabajo de ciberseguridad en organizaciones grandes con diversas fuerzas de trabajo de ciberseguridad y arquitecturas de empresa. La Oficina de administración de personal, organización principal de recursos humanos del gobierno federal de los Estados Unidos, define la administración de identidades como una competencia técnica de la ciberseguridad y marca la Iniciativa Nacional para la Educación en Ciberseguridad (NICE) del Instituto Nacional de Estándares y Tecnología (NIST) como la fuente principal para identificar y definir funciones de la ciberseguridad. [4] Sin embargo, el marco NICE de NIST no incluye funciones específicas de la IAM.[5]

Por fuera del gobierno de los Estados Unidos, diversos marcos pueden ser adaptados para el uso general. Además, hay una variedad de material de capacitación ofrecido por distribuidores/vendedores como:

- *"Mastering Identity and Access Management with Microsoft Azure"*[6]
- *"Identity, Authentication, and Access Management in OpenStack"*[7]
- *"Oracle Identity and Access Management"*[8]
- *"Securing the Perimeter* (usando Gluu)"[9]

El hecho de que el foco esté puesto en capacitaciones desarrolladas por distribuidores/vendedores es uno de los motivos por los cuales el desarrollo del conocimiento se basa en productos específicos en lugar de basarse en los estándares y las

---

[4] OPM. (2015). *Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need.* Extraído de CHCOC: https://chcoc.gov/sites/default/files/Attachment%20to%20Memo%20-%20Guidance%20for%20Identifying%20Addressing%20Reporting%20Cyb.._.pdf.

[5] Petersen, R., Santos, D., Smith, M., Wetzel, K., & Witte, G. (noviembre de 2020). Iniciativa Nacional para la Educación en Ciberseguridad (NICE) Marco para la Ciberseguridad de la Fuerza Laboral. Extraído del Centro de Recursos de Seguridad Informática: https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

[6] Nickel, J. (febrero de 2019). *Mastering Identity and Access Management with Microsoft Azure.* Editorial Packt.

[7] Martinelli, S., Nash, H, and Topol, B. (diciembre de 2015). *Identity, Authentication, and Access Management in OpenStack*. O'Reilly Media.

[8] Ramey, K. (diciembre de 2016). *Pro Oracle Identity and Access Management Suite*. Apress.

[9] Schwartz, M. and Machulak, M. (diciembre de 2018). *Securing the Perimeter*. Apress

tecnologías preexistentes que habilitan la IAM. La encuesta de IDPro *2021 IDPro Skills, Programs, and Diversity Survey* también enfatizó este descubrimiento en el contexto del Efecto Dunning-Kruger.

- La encuesta encontró que el 16% de los encuestados están interesados en capacitaciones de vendedores neutros que otorguen certificaciones. IDPro cubre esta necesidad con la nueva certificación de vendedor neutro: *Certified Identity Professional*.
- La encuesta encontró un Efecto Dunning Kruger para describir porqué un profesional experto en un producto específico de un vendedor podría creer que es experto en la totalidad de la IAM.

Las principales certificaciones en ciberseguridad consideran que la Identificación y Autenticación o la Administración de Identidades y Accesos es un dominio de conocimiento e incluyen un resumen de los principios de autenticación y autorización. Abordar la IAM como un subtema dentro de la ciberseguridad resulta insuficiente para que los profesionales aprendan lo necesario para trabajar eficazmente en su área. La siguiente sección resume por qué los profesionales IAM deben involucrarse en la planificación de la fuerza laboral.

¿Por qué es necesaria la planificación de la fuerza laboral IAM?

Este artículo sostiene que las organizaciones necesitan una planificación de la fuerza laboral IAM con el fin de capacitar a su equipo IAM y de disminuir los potenciales vectores de ataque relacionados con la IAM. Sin el conocimiento y entrenamiento necesarios, los procedimientos IAM pueden ser implementados por personas que solo tienen una comprensión básica de cuáles son las mejores prácticas de IAM, resultando en vectores de ataque frecuentes. Por ejemplo, de acuerdo con el Informe de las Investigaciones de Filtración de Información Verizon de 2021 las principales vulnerabilidades de seguridad fueron el *phishing* y las credenciales robadas.[10] Uno de los principales mecanismos para prevenir el *phishing* y el robo de credenciales es la implementación de la autenticación de múltiples factores (MFA). La MFA es una de las mejores prácticas conocidas entre los profesionales IAM, pero, ¿acaso los desarrolladores de software o los administradores de sistema están familiarizados con ella? Podemos ayudar a sanar esta brecha creando e incrementando una fuerza laboral profesional IAM mediante la planificación de la fuerza laboral y un modelo de competencia.

La implementación de MFA es una de las principales técnicas de reducción de daños, pero no toda la MFA es igual.[11] Un profesional no capacitado puede recomendar una opción resistente al *phishing* más sólida que un nombre de usuario y contraseña. Un profesional

[10] Verizon Enterprise. (2021). *Informe de las investigaciones de filtración de información 2021.* Extraído de: https://enterprise.verizon.com/resources/reports/dbir/2021/

[11] Grassi, P., Garcia, M., & Fenton, J. (2017). *800-63-3; Digital Identity Guidelines.* Extraído de la Publicación Especial NIST: https://doi.org/10.6028/NIST.SP.800-63-3

más experimentado puede recomendar una combinación de opciones resistentes al *phishing* y no resistentes al *phishing*, mostrando el riesgo y costo de cada una. La sección a continuación resume cómo los profesionales IAM pueden involucrarse en la planificación de la fuerza laboral.

Define tu equipo IAM

La arquitectura FICAM es una arquitectura de referencia del gobierno de los Estados Unidos que fue diseñada para las agencias federales.[12] (Encuentre una representación de la arquitectura FICAM en la Figura 2). Este artículo toma como punto de partida la arquitectura federal ICAM para la planificación de la fuerza laboral IAM que incluye la creación de un modelo de competencia. El marco de la fuerza laboral y el modelo de competencia son una guía gestionada generalmente por la oficina de recursos humanos pero desarrollada por los profesionales IAM.

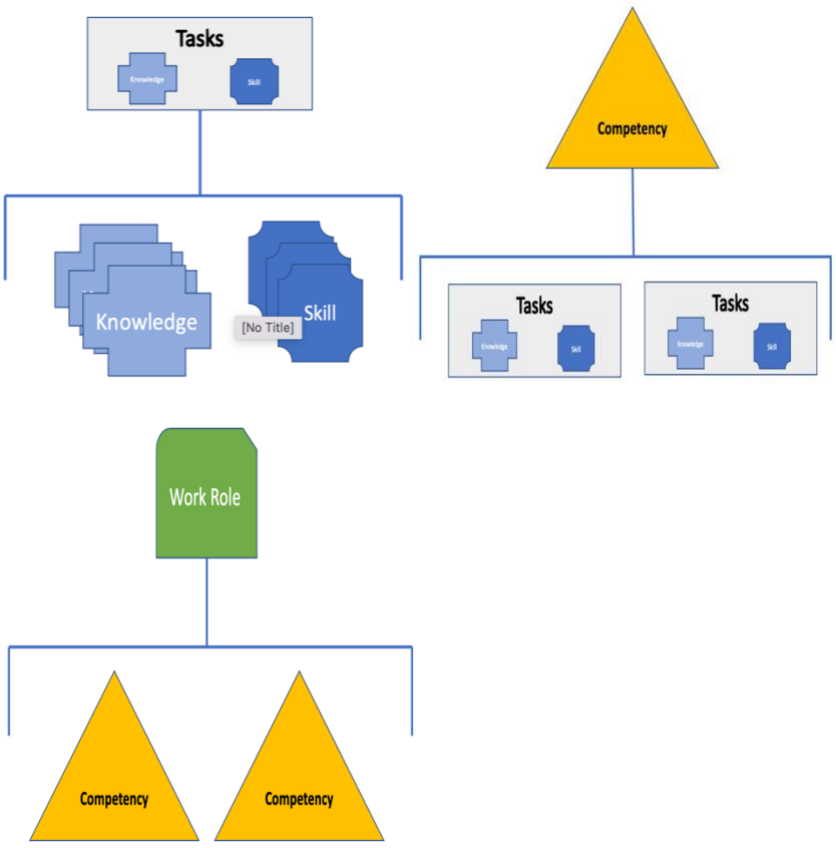

Figura 2. Conocimiento y habilidades se combinan para abarcar una tarea. Múltiples tareas abarcan una competencia. Múltiples competencias definen una función laboral.

[12] GSA. (2020). *Arquitectura federal ICAM*. Extraída de los manuales de estrategia FICAM: https://playbooks.idmanagement.gov/

Si bien la arquitectura FICAM fue desarrollada para el gobierno de los Estados Unidos, muchas de sus capacidades y servicios sirven para todas las organizaciones ya que todas las organizaciones deberían administrar identidades, credenciales y accesos. Las organizaciones pueden adoptar y adaptar este abordaje a su arquitectura específica de la identidad.

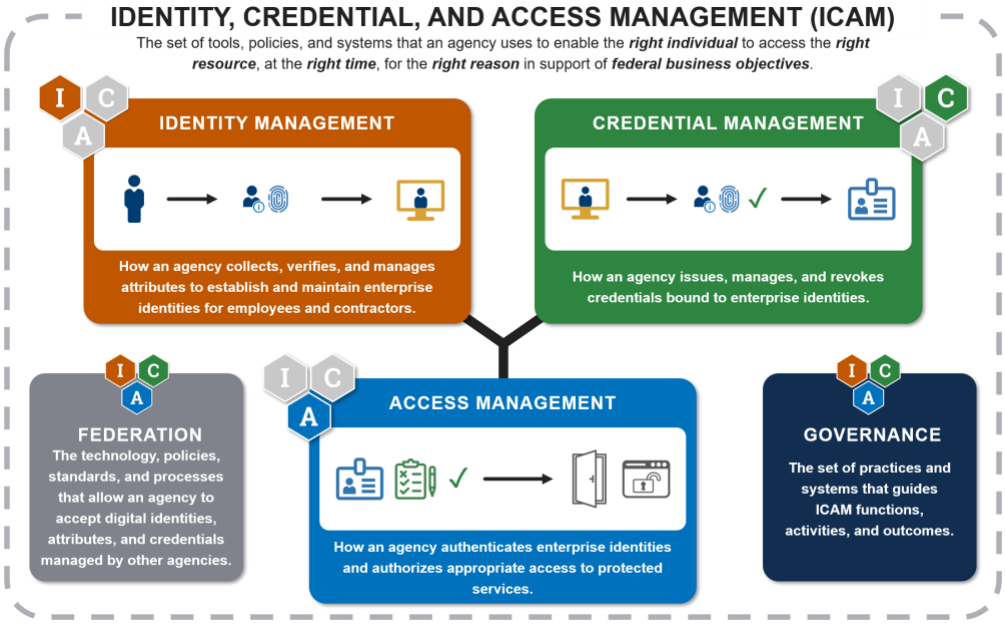

Figura 3. Arquitectura FICAM

La arquitectura FICAM define cinco áreas de dominio:

1. administración de la identidad
2. administración de credenciales
3. administración del acceso
4. (programática) gobernanza
5. federación

Luego de definir tu arquitectura IAM, el siguiente paso será utilizar el marco NIST NICE para convertir las capacidades de la arquitectura FICAM en TKS. El marco NIST NICE utiliza una fórmula simple para desarrollar enunciados fáciles de leer y comprender.

- Tarea – una actividad dirigida hacia el logro de un objetivo.
- Conocimiento - Un conjunto de conceptos recuperables dentro de la memoria. Completar una tarea puede requerir múltiples conceptos.
- Habilidad - La capacidad de realizar una acción observable. Existe una relación de muchos a uno o de uno a muchos entre la descripción de habilidades y la realización de las tareas.

El Cuadro 1 que se encuentra a continuación tiene un ejemplo de un modelo de competencia ICAM comprendido en el marco de gobernanza de la identidad.[13] Este modelo de competencia ICAM es solo un ejemplo y puede modificarse o adaptarse para cubrir las necesidades de tu organización. Una diferencia notable entre la arquitectura FICAM y otras arquitecturas IAM es la inclusión de la comprobación de la identidad como parte del servicio de administración de identidades. En una empresa, la comprobación de la identidad puede ser o bien una tarea de recursos humanos como parte de la contratación de un empleado o bien de una tercera aplicación de negocio en el caso de la incorporación de un cliente. La Arquitectura FICAM se enfoca principalmente en casos de uso de identidad de la fuerza laboral por lo cual para incorporar TSK de clientes o de no-humanos será necesario investigar más allá.

	Administración de Identidades	**Administración de Credenciales**	**Administración de Accesos**
Tarea	1. Realizar actividades de comprobación de identidades 2. Desarrollar un plan de mantenimiento del directorio de identidades 3. Revisar la prevalencia y fidelidad de la información 4. Instalar, actualizar y mantener servicios de directorio de identidades 5. Gestionar el modelado de funciones y grupos 6. Crear y automatizar flujos de trabajo para el aprovisionamiento, la gestión de derechos y administración de los registros de identidades	1. Vincular a los usuarios a un proceso de acreditación 2. Vincular un autenticador a una identidad 3. Llevar a cabo acciones de administración del ciclo de vida de credenciales como activar, renovar, resetear, suspender, revocar o terminar. 4. Emitir credenciales de Infraestructura de Clave Pública (PKI) y otro tipo de credenciales	1. Configurar y administrar servicios de inicio de sesión único 2. Configurar directorios y agentes de integración con Inicio de Sesión Único 3. Identificar métodos e integrar aplicaciones con Inicio de Sesión Único 4. Ejecutar y gestionar decisiones y puntos de aplicación de políticas 5. Configurar aplicaciones
Conocimiento	1. Conocimiento de la administración del ciclo de vida de la identidad 2. Conocimiento de métodos de comprobación de la	1. Conocimiento de la administración del ciclo de vida de credenciales 2. Conocimiento de tipos de	1. Conocimiento de modelos de autorización 2. Conocimiento de técnicas de

[13] GSA. (2021). Marco de gobernanza de identidades: https://playbooks.idmanagement.gov/docs/playbook-identity-governance-framework.pdf

	identidad, sus fortalezas y debilidades 3. Conocimiento de tecnologías y servicios de directorios de identidades 4. Conocimiento de técnicas de agregación de identidad 5. Conocimiento de legislación de privacidad y su impacto en la recopilación y mantenimiento de datos 6. Conocimiento de la gestión de derechos y flujos de trabajo	autenticadores, sus fortalezas y debilidades 3. Conocimiento de técnicas de vinculación de autenticación	autenticación de red y en la nube 3. Conocimiento de la administración del ciclo de vida de políticas de acceso 4. Conocimiento de la administración de privilegios de acceso 5. Conocimiento de enrutamiento de red
Habilidad	1. Habilidad de identificar un proceso de comprobación de la identidad con un nivel de garantía de la identidad 2. Habilidad de configurar y mantener un servicio de directorio de identidad 3. Habilidad de diagnosticar problemas de conexión del directorio 4. Habilidad para administrar el ciclo de vida de la identidad 5. Habilidad para elaborar y ejecutar revisiones de accesos y re-certificaciones 6. Habilidad de gestionar derechos	1. Habilidad de identificar un autenticador con un nivel de garantía del autenticador 2. Habilidad de vincular autenticadores a registros de directorio entre varios autenticadores 3. Habilidad de administrar el ciclo de vida de credenciales	1. Habilidad de determinar un modelo apropiado de autorización basado en el caso de uso 2. Habilidad de implementar técnicas de autenticación en múltiples entornos 3. Habilidad de administrar los requisitos de acceso utilizando las decisiones y puntos de aplicación de las políticas 4. Habilidad de implementar y gestionar herramientas de administración de accesos con privilegios

Cuadro 1. Modelo de competencia alineado con la arquitectura FICAM

Con este modelo de competencia, una organización puede definir las funciones necesarias para la realización de tareas. La lista a continuación describe los roles organizacionales más comunes para operar una infraestructura de identidad de una empresa. Las organizaciones más pequeñas pueden tener menos funciones donde cada una abarca más tareas, mientras que organizaciones más grandes tienen más funciones donde cada una

lleva a cabo tareas más específicas. El cuadro a continuación ofrece un ejemplo sobre cómo una tarea de identidad difiere entre una organización grande con múltiples divisiones y una organización pequeña con menos divisiones. Por ejemplo:

Tarea	**Organizaciones grandes con múltiples divisiones**	**Organizaciones pequeñas con dos o menos divisiones**
Realizar actividades de comprobación de la identidad	Toda comprobación de la identidad es tercerizada a un tercero mediante un administrador de sistemas que configura una federación con un tercero.	La comprobación de identidad de la fuerza laboral es generalmente realizada por el personal de recursos humanos. En aplicaciones de negocio, puede realizar preguntas personalizadas basadas en conocimientos a terceros.
Emitir autenticadores y otros tipos de credenciales	Múltiples administradores para cada tipo de credencial. Puede tener un equipo dedicado únicamente a PKI.	Un grupo pequeño de administradores realiza la tarea para todas las credenciales.
Configurar la integración de directorio y agente con Inicio de Sesión Único	Puede involucrar múltiples equipos y administradores dependiendo de la ubicación del directorio y de qué oficina es su propietaria (por ej., en la nube, empresa o aplicación)	Puede involucrar un solo equipo o administrador.
Proveer cuentas a servicios de punto de conexión (*endpoint services*) y aplicaciones	Una solución integrada con el equipo de recursos humanos y *endpoints* para mantener sincronizados los atributos y derechos.	Varios administradores de sistema realizan las tareas manualmente.

Cuadro 2. Muestra de tareas IAM basada en el tamaño de la organización

La siguiente sección aborda las funciones laborales sugeridas por NIST NICE y ofrece un ejemplo de desarrollo de un equipo IAM.

Desarrolla tu equipo IAM

Las Tareas, Conocimientos y Habilidades específicas de la IAM existen para definir una competencia IAM general. Esta competencia IAM puede incorporarse a las funciones laborales NIST NICE. Las siete funciones laborales clave de la mayoría de los programas IAM, modeladas según el marco NIST NICE, son:

1. Director de programa – Es una función directiva para liderar, coordinar, comunicar e incorporar los resultados del programa. Esta función es responsable del éxito general del programa, garantizando que esté alineado con las prioridades de la organización. Un administrador de programa es el responsable general del programa de identidad de la empresa. Dependiendo de los nombres dentro de la estructura organizacional, esta función puede llamarse director, jefe de la división o vicepresidente asociado. Para asegurar un soporte corporativo adecuado, esta persona debería responder directamente ante un ejecutivo.
2. Administrador de sistemas – Una función meramente operativa que instala, configura, identifica y resuelve problemas, y mantiene las configuraciones del servidor (*hardware* y *software*) para garantizar su confidencialidad, integridad y disponibilidad. Un administrador de sistemas generalmente gestiona cuentas, *firewalls* y parches. Son responsables del control de accesos, de la administración de credenciales y de la creación y administración de cuentas. Su función puede ser compartida con otros departamentos por fuera de la IAM. Es probable que el nombre del trabajo se asocie a vendedores específicos (Administrador "Nombre del Vendedor) o a una función (Administrador de Directorio).
3. Desarrollador de *Software* – En general es una función de diseño de sistema o de operación de sistema. Esta función es responsable de desarrollar y escribir aplicaciones informáticas, *software* o programas utilitarios específicos nuevos (o de modificar los existentes) siguiendo las mejores prácticas de garantía de *software*. Es probable que los desarrolladores de *software* programen una página de inicio de sesión o una aserción de federación para expandir las tareas de desarrollo de *software*.
4. Especialista de redes – Una función meramente operativa que planifica, implementa y opera servicios/sistemas de red, incluyendo *hardware* y entornos virtuales. Un especialista de red puede oficiar de administrador de sistemas o ser responsable de establecer y mantener servicios de autenticación y autorización de red. A menudo, este especialista se comparte con otros departamentos por fuera de la IAM.
5. Arquitecto de empresa – Fundamentalmente es una función de diseño de sistema responsable de desarrollar y mantener procesos de negocio, sistema e información para dar soporte a las necesidades de la misión de la empresa. Esto incluye desarrollar normas y requisitos de tecnología de la información (TI) que describen las arquitecturas objetivo y de planificación de base. Un arquitecto de identidad de empresa puede oficiar de arquitecto de seguridad, o su función puede denominarse arquitecto de seguridad.

6. Analista de seguridad de sistemas – A menudo es una función de diseño de sistema o de operación de sistema responsable de analizar y desarrollar la integración, testeo, operaciones y mantenimiento de la seguridad de sistemas. Un analista puede ser una función técnica o no-técnica que colabora con propietarios de aplicaciones y otros equipos de la empresa para traducir los requisitos del negocio en procesos y flujos de trabajo IAM. Algunas de sus tareas pueden incluir la minería de roles, requisitos de acceso, mapeo de atributos y tareas IAM similares.
7. Especialista de testeo y evaluación de sistemas – Habitualmente es una función de diseño de sistema o de operación de sistema responsable de planificar, preparar y ejecutar testeos de sistemas para evaluar los resultados en función de especificaciones y requisitos, y analizar/reportar los resultados de la prueba. Desarrollan y ejecutan testeos de *software* y procedimientos IAM antes de que sean implementados en un entorno de producción. Esta función puede denominarse *QA* o *Tester*.

Para ayudar a integrar los procesos de identidad digital en la gestión de riesgos general de la empresa, el equipo ICAM de una organización debería reportarse ante un ejecutivo de dirección o cuerpo de gobernanza.

Fases del desarrollo de equipo

La mayoría de las organizaciones siguen un patrón similar que se alinea con las fases de desarrollo de equipo de Tuckman: Formación, Enfrentamiento, Normalización, Desempeño y Finalización/Disolución.[14] En este artículo nos enfocamos en las tres primeras fases para desarrollar un equipo IAM que tenga un buen desempeño.

Formación

En la etapa de formación, una organización conoce las posibilidades y desafíos que implican no tener una función destinada a la IAM. Para comenzar, la organización acuerda crear un puesto destinado a esto para luego eventualmente ampliar la función IAM. La mayoría de las organizaciones descubre que necesita una persona central que sea el enlace o liaison entre las diversas funciones de identidad dentro de la organización. Habitualmente, esta decisión se precipita a raíz de eventos corporativos como un hallazgo de auditoría, un incidente cibernético o un cambio en la seguridad. Normalmente, esta función se alinea con el **director de programa** y responde ante el director de información (CIO, por sus siglas en inglés), el director de seguridad de la información (CISO, por sus siglas en inglés) o ante un nivel por debajo de una posición ejecutiva. En esta etapa, la función principal del director de programa es identificar, monitorear y reportar los procesos de identidad de alto riesgo y recomendar métodos para mitigarlo. En esta etapa, es posible que aún no tengan un equipo o responsabilidades asignadas.

[14] Stein, J. (n.d.). *Using the Stages of Team Development*. Extraído de los Recursos Humanos del MIT: https://hr.mit.edu/learning-topics/teams/articles/stages-development

Enfrentamiento

En la etapa de enfrentamiento, las responsabilidades IAM se establecen con una mayor aceptación dentro de la organización. La coordinación de apoyo directivo colabora para que la división operativa esté de acuerdo en perder cierto control de la IAM por el bien mayor del rendimiento de la organización y potencial ahorro de costos. En esta etapa, las responsabilidades del **director de programa** se han expandido permitiéndole crear un equipo primario de identidad con los **administradores de sistema** o **desarrolladores de *software*** existentes, en función de la arquitectura de empresa de la organización. Estos administradores pueden especializarse en un único producto o en una tecnología específica como directorios o autenticación. Centralizar la responsabilidad y el equipo puede venir de la mano de un cambio en el abordaje tecnológico. El director de programa puede identificar la necesidad de incorporar puestos adicionales como un arquitecto de identidad, también conocido como arquitecto de empresa, para desarrollar las normas y requisitos para el estadio objetivo de la infraestructura de identidad. En organizaciones más pequeñas, los administradores de sistema senior pueden oficiar de arquitectos porque son quienes están más familiarizados con los sistemas, vendedores y la misión de la organización y pueden proponer un estado objetivo. Las organizaciones más grandes pueden decidir separar un arquitecto de sus habituales tareas técnicas diarias para que se enfoque en una planificación a largo plazo.

Normalización

En la etapa de normalización, se establece la función IAM con un equipo destinado a ello y se determinan criterios de responsabilidad. En esta etapa, el equipo trabaja productivamente en conjunto. Es posible que el director de programa identifique la necesidad de ampliar la colaboración organizacional a un grupo extendido de miembros corporativos que incluya personal de seguridad física, del departamento legal, de privacidad, de recursos humanos tecnología de la información y de oficinas de cumplimiento normativo. Este grupo de miembros puede crear un cuerpo de gobernanza o un comité directivo para colaborar en la planificación del estado objetivo de la organización o para dar soporte organizacional para incrementar el rendimiento de la inversión en sistemas de identidad. Para, por ejemplo:

- Colaborar con recursos humanos para dar soporte a la comprobación de identidad remota.
- Colaborar con la seguridad física para integrar las decisiones de control de acceso físico a las herramientas de administración de accesos de la empresa.
- Colaborar con la oficina de cumplimiento normativo para automatizar el reporte de cumplimiento.

Dependiendo de determinadas necesidades y directivas organizacionales, una organización puede aproximarse o entrar en la etapa de desempeño. La identidad es un componente vital para llevar a cabo procesos de negocio eficaces, así como para

desarrollar un área de riesgos organizacionales. Es posible que los directores de programa deban adaptarse a iniciativas nuevas como la migración a la nube o la arquitectura de confianza cero.

Conclusión

Las organizaciones necesitan una infraestructura de la fuerza laboral IAM para garantizar la contratación y capacitación de su fuerza laboral de identidad. Los ataques de ciberseguridad predominantes son ataques basados en la identidad. Este artículo presenta un modelo de planificación de la fuerza laboral IAM basado en TKS y alineado con una arquitectura IAM de empresa de una organización grande. Luego alinea las tareas con la manera en la que una organización típica identifica y dota de personal a su fuerza laboral IAM. El modelo de competencia puede usarse o adaptarse a la medida de necesidades específicas para definir funciones IAM consistentes a lo largo de las organizaciones.

Biografía del autor

Kenneth Myers es candidato doctoral en la Universidad Marymount y especialista en información y seguridad TI en la Administración General de Servicios de los Estados Unidos. Puede encontrarlo en kmm57090@marymount.edu o https://idmken.github.io.

Lecturas complementarias

OMB. (2019). *Enabling Mission Delivery through Improved Identity, Credential, and Access* Management. Extraído de OMB: https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf.

Sharma, A., Sharma, S., and Dave, M. (2015). *Identity and Access Management - A Comprehensive Study*. 2015 *International Conference on Green Computing and Internet of Things,* 1, 1481-1485. https://doi-ieeecomputersociety-org.proxymu.wrlc.org/10.1109/ICGCIoT.2015.7380701.

Schneider, F. B., & Mulligan, D. K. (2011). Una tesis doctoral. *IEEE Security & Privacy Magazine, 9(4)*, 3–4. Extraído de https://doi.org/10.1109/msp.2011.76.

NIST. (2021c). Glosario - *Phishing*. Extraído del Centro de Recursos para la Seguridad Informática: https://csrc.nist.gov/glossary/term/phishing

NSA. (2020). *Detecting Abuse of Authentication Mechanisms.* Extraído de *Cybersecurity Advisory*: https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF.

Reiner, S. (2020, 12 29). *Golden SAML revisited: The solorigate connection*. Extraído del blog CyberArk: https://www.cyberark.com/resources/threat-research-blog/golden-saml-revisited-the-solorigate-connection

Tan, Y., Li, W., Yin, J., & and Deng, Y. (2020). A universal decentralized authentication and authorization protocol based on Blockchain. *2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, (pp. 7-14).

Li, W., & Mitchell, C. J. (2020). *User Access Privacy in OAuth 2.0 and OpenID Connect*. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, (pp. 664–672).

ACM, IEEE, AIS, S., & IFIP. (2017). *Cybersecurity Curricular Guideline.* Extraído de CSEC 2017: https://cybered.hosting.acm.org/wp/.

ISC2. (2021). *CISSP – the world's premier cybersecurity certification*. Extraído de ISC2: https://www.isc2.org/Certifications/CISSP.

CompTIA. (2021). *Security+ (plus) certification*. Extraído de las certificaciones CompTIA IT: https://www.comptia.org/certifications/security.

Universidad de Bristol. (2020). *CyBOK Version 1.0.* Extraído del Cuerpo de Conocimiento de Ciberseguridad: https://www.cybok.org/knowledgebase/.

Cuerpo de Conocimiento de IDPro. (2022). Extraído de IDPro: https://idpro.org/body-of-knowledge/.

Rose, S., Borchert, O., Mitchell, S., & & Connelly, S. (2020). *Zero trust architecture.* Extraído de la Publicación Especial NIST: https://doi.org/10.6028/nist.sp.800-207.

NIST. (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity.* Extraído del Marco de Ciberseguridad NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

DHS. (2018). *PRIVMGMT: The First Step Toward CDM Phase 2 Capabilities.* Extraído de Continuous Diagnostic and Mitigation (CDM): https://us-cert.cisa.gov/sites/default/files/cdm_files/FNR_CPM_OTH_NovWebinarSlides.pdf.

Kim, K., Smith, J., Yang, T. A., & Kim, D. J. (2018). *An Exploratory Analysis on Cybersecurity Ecosystem Utilizing the NICE Framework*. *2018 National Cyber Summit (NCS)*. Publicado. https://doi.org/10.1109/ncs.2018.00006.

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). *Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security,* 24-35.

Bicak, A., Liu, M., & Murphy, D. (2015). *Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. Information Systems Education Journal (ISEDJ)*, 99-110.

Hoag, J. (2013). Evolution of a cybersecurity curriculum. *Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13*, (pp. 94-99).

Ran, F. X., & Sanders, J. (2020). Instruction quality or working condition? The effects of Part-Time faculty on student academic outcomes in community college introductory courses. *AERA Open*.

Furnell, S. (2020). The cybersecurity workforce and skills. *Computers and Security*, 100.

Gordon, A. (2016). *The Hybrid Cloud Security Professional*. *IEEE Cloud Computing, 3*(1), 82-86.

CIISec. (2019). *CIISec Roles Framework, Version 0.3.* Extraído de *Charted Institute of Information Security:* https://www.ciisec.org/CIISEC/Resources/Capability_Methodology/Roles_Framework/CIISEC/Resources/Roles_Framework.aspx.

NIST. (2021a). Glosario - Credencial. Extraído del Centro de Recursos para la Seguridad Informática: https://csrc.nist.gov/glossary/term/credential.