Autenticación y Autorización (v2)

Por Mark Morowczynski (Microsoft) y Michael Epping (Microsoft)

Actualizado por el Comité del Cuerpo de Conocimiento de IDPro para la v2

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

Tabla de Contenidos

Resumen **2**

Introducción **2**

Terminología 2

¿Qué es la identificación? **5**

¿Qué es la autenticación? **5**

¿Qué es la autorización? **7**

El rol de los proveedores de identidad y la federación **9**

Conclusión **10**

Biografía de los Autores **10**

Registro de cambios **11**

Resumen

Este artículo describe los elementos fundamentales de la autenticación y autorización, dos elementos claves de la Identidad y la Administración de Acceso. También aborda la federación y los Proveedores de Identidad, herramientas comunes para ejecutar la autenticación y autorización dentro de una organización.

Introducción

Este artículo describe la autenticación y la autorización, dos elementos cruciales para llevar a cabo una estrategia óptima de Identidad y Administración de Acceso. Generalmente las organizaciones suelen contar con varias herramientas de autenticación y autorización, tanto en su servidor local como en la nube. Se describen los conceptos de base de cada una, y se exploran y usan las formas comunes de autenticación y autorización.

Terminología

Varios de estos términos han sido tomados de la "Terminología en el Cuerpo de Conocimiento de IDPro".[1]

Término	Definición
Listas de Control de Acceso	Las Listas de Control de Acceso son definiciones sobre quién o qué tiene el acceso permitido o denegado a determinado recurso. Por ejemplo, un archivo compartido puede tener una Lista de Control de Acceso que permita a los usuarios del departamento de marketing leer y escribir, a los usuarios del departamento TI solo leer y denegar el acceso a todos los otros usuarios.
Control de Acceso Basado en Atributos ("ABAC", por sus siglas en inglés)	Es un patrón de sistemas de control de acceso que involucra definiciones dinámicas de los permisos basados en información (como atributos o proclamaciones), como por ejemplo códigos de trabajo, departamento o grupo de miembros.
Autenticación	La autenticación es un proceso de demostración por el cual se determina que el usuario con identidad digital que está solicitando acceso es el legítimo propietario de esa identidad. Dependiendo del caso de uso, una identidad puede representar a un humano o una entidad no humana; puede ser un individuo o una organización y puede ser verificada en el mundo real con algunas salvedades, incluyendo la posibilidad de no ser verificada en el mundo real.

[1] "Terminología en el Cuerpo de Conocimiento de IDPro," Cuerpo de Conocimiento de IDPro, actualizado el 30 de Setiembre de 2021, https://bok.idpro.org/article/id/41/.

Autorización	Es el acto de determinar el derecho de un usuario para acceder a una funcionalidad con una aplicación de computadora y el nivel en el cual ese acceso debe ser otorgado. En la mayoría de los casos, una "autoridad" define y provee el acceso, pero en algunos casos el acceso es concedido por derechos inherentes (como en el caso de un paciente accediendo a su propio registro médico).
Directorio	Un directorio es un repositorio central de identidades de usuarios y de los atributos que las componen. Una identidad de usuario podría ser John Smith siendo John el atributo de nombre, Smith el atributo de apellido, director el atributo de cargo y marketing el atributo de departamento. Los atributos en el directorio pueden ser usados para tomar decisiones de autorización en cuanto a qué acceso debe tener determinado usuario para acceder a aplicaciones.
Identificación	Establece inequívocamente al usuario de un sistema o de una aplicación.
Federación de identidades	Una Federación de identidades es un grupo de proveedores de informática o de red que acuerda operar utilizando los protocolos estándares y los acuerdos de confianza. En una situación de Inicio de Sesión Único (SSO, por sus siglas en inglés), la federación de identidades ocurre cuando un Proveedor de Identidades (IdP, por sus siglas en inglés) y un Proveedor de Servicio (SP, por sus siglas en inglés) acuerdan comunicarse mediante un protocolo estándar específico. El usuario de la empresa preferirá iniciar sesión en la aplicación usando sus credenciales de la empresa antes que crear nuevas y específicas credenciales en la aplicación. Al usar un solo conjunto de credenciales, los usuarios tienen que administrar solamente una credencial. Los problemas relacionados con las credenciales -como el reseteo de contraseña- pueden ser gestionados en una ubicación central y las aplicaciones pueden confiar en que los sistemas de empresa apropiados (como los sistemas de recursos humanos) son una fuente confiable en lo que refiere al estado y afiliación de un usuario. La f ederación de identidades puede tomar diversas formas. En el ámbito académico, las federaciones multilaterales en las que un tercero de confianza gestiona los metadatos de varios IdPs y SPs, son muy comunes. [1]
Administración de Identidades y Accesos (IAM, por sus siglas en inglés)	La IAM es la disciplina utilizada para garantizar que el acceso correcto está designado para el usuario correcto y para los recursos correctos, por las razones correctas.

Autoridad de Información de Identidades (IIA, por sus siglas en inglés)	Representa una o más fuentes de datos usadas por la Administración de Identidades (IDM, por sus siglas en inglés) como base para el conjunto maestro de registros de identidades de entidades principales o sujetos. Cada IIA puede proveer un subconjunto de registros y de atributos. A veces la IIA se diferencia del Proveedor de Información de Identidades o IIP. La IIA se usa para incluir el servicio que de hecho provee la información, así como la autoridad raíz. Esto se corresponde a "Fuente de Información de Identidades" en ISO/IEC 24760-2 y a "Fuentes de Identidades" en Internet2.
Proveedor de Identidades (IdP, por sus siglas en inglés)	Un Proveedor de Identidades (IdP) envía información sobre un usuario a una aplicación. Generalmente, esta información está guardada en el almacén de datos del usuario con lo cual un proveedor de identidades tomará esa información y la transformará para pasarla al proveedor de servicio, es decir la aplicación. La organización OASIS, que es la responsable de las especificaciones SAML, define que un IdP es un "tipo de SP que crea, mantiene y gestiona la información de identidad de entidades principales y provee autenticación a otros SP dentro de la federación, como es el caso de los navegadores de Internet."
Autenticación de Múltiples Factores (MFA, por sus siglas en inglés)	Es un método por el cual la identidad de un usuario es validada al nivel de confianza requerido de acuerdo con una política de seguridad para un recurso que es accedido utilizando más de un factor (algo que sabes —como tu contraseña—, algo que tienes —como tu teléfono inteligente—, algo que eres —como tu huella digital—).
Terceros confiables (RP, *Relying Party*)	Es un componente, sistema o aplicación que usa el Proveedor de Identidades (IdP, por sus siglas en inglés) para identificar a sus usuarios. El RP tiene sus propios recursos y lógica. Nótese que el término "servicio de confianza" (*relying service*) es utilizado en los estándares ISO/IEC para abarcar todos los tipos de componentes que usan servicios de identidad, incluyendo sistemas, subsistemas y aplicaciones, independientemente del dominio u operador. Aquí usaremos el término "terceros confiables" (RP) de la manera que es más comúnmente empleada. A grandes rasgos, un RP se corresponde con el término "Agency *Endpoint*" del modelo FICAM o con el término "Consumidores de Identidad" en el modelo Internet2.
Control de Acceso basado en Roles (RBAC, por sus siglas en inglés)	Es un patrón de sistema de control de acceso que utiliza un conjunto de definiciones manuales o estáticas de los permisos asignados a los "roles", y que puede asociarse a los usuarios con necesidades de acceso comunes, consistente y reiteradamente. El

	Control de Acceso basado en Roles es un sistema mediante el cual se otorgan roles a identidades y ellos son los que determinan qué acceso a los recursos deben tener esas identidades. Algunos roles básicos pueden ser “admin” o “usuario de solo lectura” – un admin estará habilitado para hacer cambios en el sistema y un usuario de solo lectura únicamente podrá ver los recursos.

¿Qué es la identificación?

La identificación es el acto de determinar qué identidad está en uso o con cuál se está interactuando, estableciendo de forma única a un usuario de un sistema o aplicación.
Antes de que una identidad pueda ser autenticada, se debe determinar qué identidad está siendo utilizada. Esto ocurre comúnmente a través del usuario que está proveyendo su nombre de usuario. El nombre de usuario se usa para identificar al usuario mientras que la contraseña se usa para autenticar al usuario.

Ciertos tipos de credenciales pueden proveer tanto identificación como autenticación simultáneamente, como las credenciales FIDO o una acción biométrica.

¿Qué es la autenticación?

Conceptualmente, la autenticación, a veces abreviada como AuthN, es el proceso de garantizar la propiedad de una cuenta al momento de ser usada para acceder a un recurso o para iniciar una sesión. Uno realiza decenas de autenticaciones por día sin darse cuenta. Cuando uno inicia sesión en su computadora con su nombre de usuario y contraseña, está autenticando. Cuando uno inicia sesión para revisar su email a través de un buscador o de una aplicación como Outlook, una vez más está autenticando para comprobar que es el propietario o responsable de esa cuenta de email. Cuando uno lleva a cabo una acción biométrica en su dispositivo móvil, como por ej. escanear su huella digital o rostro para desbloquear el dispositivo, una vez más está completando una autenticación. Cuando uno va a un cajero a extraer dinero, primero debe proveer la tarjeta y luego el PIN. Si la autenticación es correcta, el cajero puede confiar en que uno es el propietario de la cuenta. La autenticación puede tomar diferentes formas para diferentes recursos:

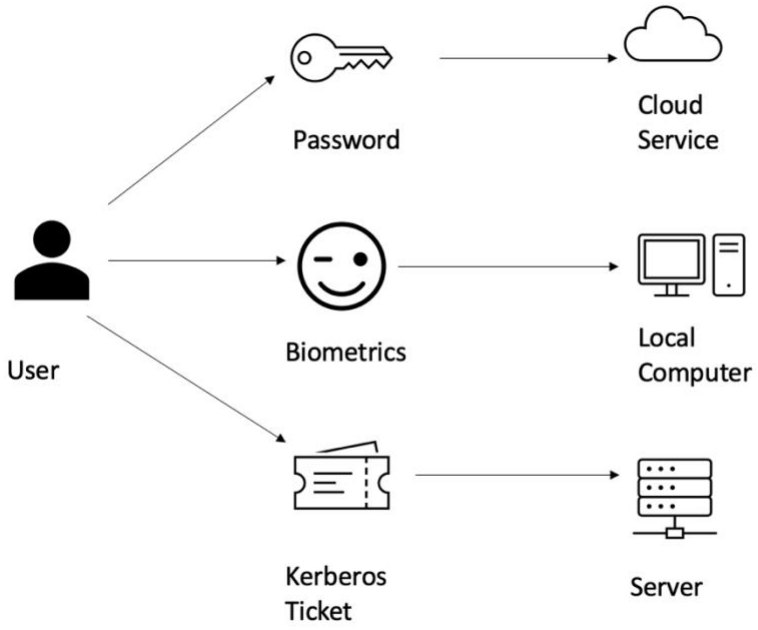

Figura 1: El usuario y sus diferentes factores de autenticación.

Existe una variedad de diferentes posibles factores de autenticación, como memorizar secretos, usar tokens de hardware y realizar acciones biométricas. Se los reconoce usualmente como "algo que sabes", "algo que tienes" y "algo que eres". El más común es el nombre de usuario y contraseña. También se han popularizado los métodos de autenticación de múltiples factores. Los más comunes son el mensaje de texto o la llamada telefónica, aunque estas ya no son las opciones más seguras disponibles. También existen métodos como aplicaciones o claves de hardware de autenticación con contraseña de un solo uso (OTP, por sus siglas en inglés), donde la contraseña puede ser usada una sola vez y normalmente es válida por un tiempo limitado. También existen diferentes aplicaciones autenticadoras donde una notificación *push* es enviada al dispositivo y es aprobada por el usuario final. Las claves de seguridad físicas de FIDO2 y las acciones biométricas como el escaneo de huellas digitales y el reconocimiento facial se han vuelto más comunes y las claves de acceso (*passkeys*) están reemplazando el tradicional ritual de contraseña de autenticación en su totalidad.[2] Las identidades no-humanas también deben autenticarse. Computadoras y servicios se autentican entre sí utilizando certificados, secretos compartidos (simplemente una contraseña para una aplicación), u otros protocolos desarrollados para este propósito. ¡La autenticación no es solo para las personas!

[2] Para más información sobre FIDO2, ver Fido Alliance, "FIDO2: WebAuthn & CTAP – Moviendo el Mundo Más Allá de Las Contraseñas," sitio web, https://fidoalliance.org/fido2/ (accedido el 28 de setiembre de 2021); para más información sobre *passkeys*, ver FIDO Alliance, "Passkeys," sitio web, https://fidoalliance.org/passkeys/ (accedido el 10 de noviembre de 2022).

La autenticación suele ser el primer paso cuando una entidad quiere acceder a un recurso. Primero se debe determinar qué identidad está intentando acceder al recurso y si es una identidad legítima o no. Luego se puede proceder al siguiente paso: determinar qué acceso (si lo hay) se le debería otorgar o denegar a dicha identidad.

¿Qué es la autorización?

El siguiente paso crucial de la Administración de Identidades y Accesos es la autorización, a veces abreviada como Authz. Conceptualmente, es lo que se le permite hacer a una entidad. Una vez que la autenticación le permite al sistema o a los servicios saber quién eres, la autorización te otorgará derechos o permisos para poder proceder con diferentes acciones. La autenticación ayuda a verificar que tú eres el mismo sujeto cada vez que ingresas; la autorización determina si se te permite acceder o llevar a cabo cualquier acción. Estos derechos pueden ser tan simples como ver un archivo (un permiso otorgado) o denegar la posibilidad de verlo (un permiso denegado). Quizás hayas experimentado esto cuando alguien te envía un archivo o un enlace a un sitio y recibes un mensaje de error de “acceso denegado”. Es porque no tienes la autorización para acceder a ese recurso. Esto también lo has experimentado cuando sí puedes ver un archivo o acceder a un sitio, ¡Sólo que no hay un mensaje informándote de que sí puedes hacerlo! Es probable que te hayas cruzado con cientos o hasta miles de decisiones de autorización por día sin que te hayas dado cuenta (a no ser, por supuesto, que se te haya denegado un acceso).

Las decisiones de autorización pueden hacerse en base a varios factores. Un ejemplo común es que, si tienes un rol específico asignado a tu cuenta puede que tengas permisos en el sistema para agregar, modificar, eliminar o ver cosas. Esta arquitectura de autorización es comúnmente conocida como Control de Acceso Basado en Roles (RBAC, por sus siglas en inglés). Si por ejemplo posees el rol de administrador dentro de un sistema, puedes administrar todos los aspectos de ese sistema. Si tu rol dentro del sistema es el de lector, puede que estés habilitado a ver todo lo mismo que ve el administrador, pero sin la capacidad de hacer cambios.

Asimismo, existen los sistemas de Control de Acceso Basado en Atributos (ABAC, por sus siglas en inglés) donde a los usuarios se les puede otorgar derechos específicos dependiendo de los atributos de su cuenta. Si, por ejemplo, eres miembro del departamento de ventas, probablemente seas miembro de un grupo de ventas en tu directorio corporativo o quizás tengas un atributo de departamento asociado a “ventas”. Esta membresía de grupo o atributo te otorgará acceso a la carpeta de ventas compartida en la red o en un sitio para compartir archivos. Pero no podrás acceder a la carpeta de ingeniería compartida en la red o en el sitio de ingeniería. Solo aquellos que son miembros del departamento de ingeniería podrán hacerlo. Estas decisiones suelen ser tomadas por las Listas de Control de Acceso (ACLs, por sus siglas en inglés) determinadas por el administrador del sistema. El RBAC y el ABAC son temas complejos que ameritan sus propios artículos.[3]

Otro ejemplo donde la autorización está basada en la información sobre el usuario es su puesto de trabajo. Cuando un usuario común inicia sesión en su aplicación de recursos humanos, puede ver información sobre sí mismo. Cuántas horas trabajó, quién es su supervisor, su recibo de sueldo e información sobre sus beneficios. Esta persona está únicamente autorizada a ver su propia información. Su supervisor, por otro lado, tiene el mismo acceso a su propia información, pero también puede obtener información adicional sobre sus empleados, como cuántas horas trabajaron. Sin embargo, no puede acceder a información sobre el resto de los empleados de la organización. Según su cargo, solo se le autoriza ver información adicional sobre los que le reportan directamente. Por último, el superior de recursos humanos puede acceder a un amplio rango de información sobre la compañía. Puede ver la totalidad de horas trabajadas por todos en la compañía, la nómina completa y los beneficios utilizados. Al poseer el cargo de superior de recursos humanos, está autorizado a ver toda esta información.

La autorización se aplica también a cuentas no-humanas. Una cuenta de servicio puede incluir roles en la mayoría de los directorios. Con este rol, ésta tendría los mismos permisos que cualquier cuenta humana. Las cuentas de servicio también pueden ser parte de grupos. Un ejemplo común es el servicio que opera los respaldos en los servidores en Windows. Dependiendo de su diseño, quizás deba formar parte de un grupo superior como operadores de respaldo para poder respaldar y restaurar archivos en el sistema.[3]

Hasta aquí, el concepto de autorización puede parecer simple. La autorización concede o deniega permisos a recursos tanto para cuentas humanas como no-humanas. Sin embargo, los detalles de la implementación pueden ser sumamente complejos. En el ejemplo anteriormente citado, el equipo de ventas y el equipo de ingeniería tienen acceso a recursos corporativos diferentes. Pero ¿Qué sucede cuando ambos necesitan colaborar en algo? El departamento de ingeniería está por lanzar un nuevo producto y el equipo de ventas necesita venderlo. ¿Agregamos el equipo de ventas al grupo de ingeniería? ¿Llevamos el grupo de ingeniería al de ventas? ¿O creamos un NUEVO grupo llamado ventas-ingeniería y agregamos a ambos grupos? Esta última parecería ser la solución correcta, pero ¿Qué hacemos cuando el grupo de operaciones también necesita trabajar con ingeniería para asegurarse de que la producción de su producto alcance sus estándares? Operaciones también necesita trabajar con ventas para cerciorarse que la cadena de suministro coincida con sus proyecciones de venta. ¿Creamos otro grupo nuevo para que los tres equipos trabajen juntos? Como puedes ver, esto comienza a descontrolarse. Es importante tener una autorización diseñada para este tipo de situaciones y que contemple cómo manejar casos excepcionales antes de implementar una solución de Administración de Identidades y Accesos (IAM).

---

[3] Para más información sobre la administración de cuentas no-humanas, ver Williamson, Graham y André Koot, “Administración de Cuentas No-Humanas,” Cuerpo de Conocimiento de IDPro, 30 de octubre de 2020, https://bok.idpro.org/article/id/52/.

Por último, debemos asegurarnos de seguir el concepto de mínimo privilegio. El mínimo privilegio es parte de una sólida estrategia que asegura que tanto usuarios como cuentas de servicio tengan la menor cantidad posible de permisos necesarios. Es fácil otorgar más permisos para hacer el proceso de autorización un poco más sencillo, pero luego pagaremos el precio por estas decisiones, a veces con resultados catastróficos. Es mucho más difícil quitarle los permisos a usuarios y cuentas no-humanas una vez que estos han sido otorgados. Tómate el tiempo y asegúrate que el mínimo privilegio esté incluido dentro de las decisiones de autorización. Tu "yo del futuro" te lo agradecerá.

El rol de los proveedores de identidad y la federación

Tanto la autenticación como la autorización pueden ocurrir dentro de un único sistema o aplicación o pueden ser externalizadas a través de una federación de identidad. Si tienes una aplicación que no reside en tu intranet corporativo (es decir, es un servicio alojado en la nube), tus usuarios deberán autenticarse de todos modos.[4]

El proveedor de identidad, frecuentemente abreviado IdP o IDP, gestiona la autenticación del usuario. La autenticación puede ser hecha mediante un buscador de red usando la autenticación basada en formularios, la autenticación integrada de Windows (IWA, por sus siglas en inglés), o a través de una aplicación usando una API. Esto es autenticación de usuarios como servicio. Hay IdPs alojados en instalaciones, así como servicios de nube que pueden ser usados como IdPs. Estos IdPs también efectúan autoriza ción hasta cierto punto. Supongamos que un usuario no logra autenticarse con el IdP porque no tiene una cuenta o porque no tiene el acceso asignado para una aplicación en particular. En ese caso, el IdP no le expedirá al usuario una aserción para acceder a la aplicación. Si el usuario se autentica de forma exitosa, entonces el IdP sí expide aserciones a la aplicación.

Las aserciones, también referidas como proclamaciones, son fracciones de información enviadas a la aplicación (proveedor de recursos) que en este caso identifica al usuario y cualquier otra información adicional sobre el mismo. Estas fracciones de información son también conocidas como atributos. El atributo del primer nombre puede ser provisto como una aserción y contener palabras como "John" o "Jane". La información requerida y enviada varía según la aplicación, pero datos tales como cargo, supervisor, identificación del empleado, etc. pueden ser incluidos en la aserción.

[4] Para más información sobre las federaciones de identidad y fuentes de verdad, ver Lunney, Patrick, "Federación en la Empresa", Cuerpo de Conocimiento de IDPro, 19 de abril de 2021, https://bok.idpro.org/article/id/62/, y Dingle, Pam, "Introducción a la Identidad- Parte 2: Administración de Acceso," Cuerpo de Conocimiento de IDPro, 17 de junio de 2020, https://bok.idpro.org/article/id/45/.

Antes de que un usuario pueda autenticar y enviar información a modo de aserción para acceder a la aplicación, es necesario establecer una confianza de federación[5]. Los detalles de la configuración varían según los protocolos de la federación, pero el IdP y la aplicación intercambiarán información como la clave pública del IdP y los *endpoints* de la aplicación para lograr la autenticación. Esta información suele encontrarse en los metadatos de confianza. Los estándares como FastFed definen cómo deben ser formateados estos metadatos para establecer la confianza entre la aplicación y el IdP.[6]

La federación y los IdPs nos permiten controlar la autenticación y autorización para aplicaciones incluso por fuera de la red corporativa de trabajo. Estas herramientas son importantes, especialmente dentro de ambientes modernos donde las aplicaciones de nube y otros servicios continúan proliferando. Las organizaciones deben poder autenticar a los usuarios, validar que son quienes dicen ser, autorizarlos y otorgarles el acceso apropiado basándose en quiénes son, en cualquier lugar incluyendo la nube o en instalaciones propias.

Conclusión

Este documento repasa dos conceptos centrales de IAM: la autenticación y la autorización. Estos conceptos son usados en todas las organizaciones para validar identidades y otorgarles el acceso apropiado una vez que han sido determinadas como legítimas. Validar la legitimidad de una identidad es crucial para evitar ataques a los sistemas de las organizaciones. También se recomienda otorgar la mínima cantidad de permisos necesarios; minimizando el daño en caso de que un usuario malicioso acceda u obtenga un nivel más alto del necesario dentro de un sistema, reduciendo así posibles daños. Hoy en día, la federación a través de los Proveedores de Identidad (IdPs) es una forma común de autenticar y autorizar, ya que los servicios y las aplicaciones suelen encontrarse cada vez más por fuera de las redes corporativas. Las técnicas de autenticación y autorización logran proteger estos recursos e identidades más allá de su ubicación.

Biografía de los Autores

Michael Epping es jefe de programas en el equipo de ingeniería de Azure AD en Microsoft. Es parte del equipo de experiencias de cliente y su rol es acelerar la incorporación de servicios de nube en los clientes de la empresa. Michael ayuda a clientes a utilizar productos de Microsoft tales como Azure AD, Intune y Office 365.

Mark Morowczynski (@markmorow) es el jefe principal de programas en el equipo de éxito del cliente en la división de identidad de Microsoft. Pasa la mayor parte de su tiempo

---

[5] Para más información sobre las arquitecturas de IAM, ver Dobbs, G. B., (2021) "Referencia de Arquitectura de IAM", *Cuerpo de Conocimiento de IDPro* 1(6). doi: https://doi.org/10.55621/idpro.76

[6] Fundación OpenID, *Fast Federation (FastFed) Working Group*, sitio web, https://openid.net/wg/fastfed/ (accedido el 31 de agosto de 2021).

trabajando con los clientes en el despliegue del Directorio Activo Azure. Anteriormente fue ingeniero de campo primer nivel apoyando el Directorio Activo, Los Servicios de Federación del Directorio Activo y el Desempeño de Clientes de Windows. También fue uno de los fundadores del blog AskPFEPlat. Ha dado presentaciones en varios eventos de la industria como el *Black Hat 2019*, *Defcon Blue Team Village*, *GrayHat*, varios *BSides*, *Microsoft Ignite*, *Microsoft Inspire*, Cumbres de Microsoft MVP, La Conferencia de los Expertos (TEC, por sus siglas en inglés), La Cumbre de Identidad de Nube, Cumbre de Seguridad de SANs y *TechMentor*. Se lo puede encontrar en Twitter como @markmorow discutiendo sobre béisbol y a veces creando gifs graciosos.

Registro de cambios

Fecha	Cambio
2021-09-30	V1 publicada
2022-12-15	V2 publicada; sección de terminología expandida (ABAC, Identificación, Autoridad de Información de Identidad, Servidor de Confianza); referencia incluida a los *passkeys*; información sobre PKI eliminada