Terminología en el Cuerpo de Conocimiento de IDPro

Heather Flanagan, editora - @ 2022 IDPro

Nota de la editora: Esta es una lista unificada de la terminología presente en cada artículo publicado en el Cuerpo de Conocimiento (BoK -*Body of Knowledge*-, por sus siglas en inglés). En ningún caso este documento pretende ser una lista de terminología definitiva ni consensuada globalmente. Ofrecemos esta lista unificada como un punto de partida para su discusión. En cuanto a los términos ya definidos en el BoK, invitamos a los autores de los artículos a revisar y utilizar las definiciones existentes antes de ofrecer nuevas.

Para comprender mejor por qué algunos de los términos utilizados en el espacio de Administración de Identidades y Accesos (IAM, por sus siglas en inglés) pueden llegar a ser ambiguos, les recomendamos leer el artículo “Palabras de Identidad” de Espen Bago.

Tenga en cuenta que puede enviarnos su devolución sobre los artículos que utilizan estos términos a través del repositorio GitHub de IDPro: https://github.com/IDPros/bok.

Término	Definición	Fuente
Abstracción	La práctica de identificar y aislar los aspectos repetidos de operaciones o lógicas de negocio, para que se encuentren en un solo lugar y puedan ser referenciadas en muchos lugares.	Introduction to Policy-Based Access Controls (v2)
Certificación de Acceso	La certificación es la revisión continua de quién tiene qué accesos (por ej., los procesos de negocio para verificar que los derechos de acceso son correctos).	Introduction to Identity - Part 1: Admin-time (v2), Techniques To Approach Least Privilege
Control de Acceso	Controlar quién tiene acceso a datos, sistemas, servicios, recursos,	Introduction to Access Control

	ubicaciones. “Quién” puede ser un usuario, un dispositivo o un servicio, entre otros.	
Control de Acceso	Los diversos métodos para limitar el acceso a datos, sistemas, servicios, recursos, ubicaciones de usuarios, dispositivos u otros.	IAM Reference Architecture
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 IT solo leer y denegar el acceso a todos los otros usuarios.	Authentication and Authorization
Sistema de Control de Acceso	Es una estructura que controla y ejecuta decisiones sobre el acceso dentro de la organización.	Introduction to Policy-Based Access Controls (v2)
Gobernanza de Acceso	La garantía de que todos los accesos han sido otorgados correctamente siguiendo todos los parámetros y criterios establecidos.	Introduction to Access Control
Gobernanza de Acceso	La Gobernanza de Acceso provee vigilancia y control sobre los derechos de acceso implementados en múltiples sistemas de autorización locales o compartidos. Estos derechos pueden ser controlados de varias formas, comenzando por la existencia o validez de la identidad digital. Existen otros tipos de mecanismos de control como las políticas, el mapeo de roles, los permisos y las	IAM Reference Architecture

	identidades. El concepto se abrevia IGA por las siglas en inglés para "Gobernanza y Administración de Identidades" y se utiliza mucho en el sector comercial. En términos generales, se corresponde a la sección "Certificación de Acceso" del componente de primera clase de los Sistemas de Gobernanza del modelo FICAM. IGA no está específicamente abordado en el modelo ISO/IEC.	
Gestión de acceso	La utilización de información de identidades para otorgar control de acceso a recursos protegidos como sistemas de computadoras, bases de datos o espacios físicos.	Introduction to IAM Architecture
Gestión de acceso	Son los procesos y las técnicas utilizados para controlar el acceso a recursos. Esta capacidad trabaja junto con la Administración de Identidades y los terceros confiables (*relying party*) para concretar su objetivo. En el modelo, la gestión de acceso es un conjunto de conceptos que reúne la función de Gobernanza de acceso y el componente de autorización compartido. Dicho esto, la gestión de acceso también impacta sobre la autorización local (a través de la función de gobernanza).	IAM Reference Architecture
Política de Acceso	Definición de las reglas que autorizan o deniegan el acceso a objetos seguros.	Introduction to Access Control
Solicitante de Acceso	La persona, proceso, sistema, dispositivo u otro que quiere acceder a un recurso protegido.	Introduction to Access Control

Proveedor de Acceso	El componente que otorga acceso a datos, sistemas o servicios después de que los requisitos de la Política de Acceso (definidos en el Punto de Administración de Políticas) han sido cumplidos por el Solicitante de Acceso.	Introduction to Access Control
Propietario de la Cuenta	Una entidad que "posee" o que reclama responsabilidad de una cuenta. En general, una cuenta es expedida a nombre de su(s) dueño(s) o representantes, en el caso de empresas.	Account Recovery (v2)
Recuperación de Cuenta	Es el proceso para devolver a un propietario el acceso a su cuenta cuando pierde, olvida o no puede generar las credenciales de la cuenta. Esto puede realizarse en persona, de forma remota o híbrida.	Account Recovery (v2)
Recuperación de Cuenta	El proceso para actualizar las credenciales de un usuario en el caso de que el usuario no pueda validar sus credenciales.	Managing Identity in Customer Service Operations
Usurpación de Cuenta	La usurpación de cuenta es una forma de robo de identidad y fraude, por la cual terceros maliciosos logran acceder exitosamente a las credenciales de la cuenta de un usuario.	Account Recovery (v2), Designing MFA for Humans, Techniques To Approach Least Privilege
Responsabilidad	La obligación de una persona de aceptar el resultado de una acción propia sea positiva o negativa. A menudo, esta persona es también algún tipo de propietario.	Introduction to Access Control
Acción	Una operación protegida disponible para un recurso, como "Ver", "Editar" o "Enviar".	Introduction to Policy-Based Access Controls (v2)

Autenticación Adaptativa	La Autenticación Adaptativa apunta a determinar y ejecutar el nivel de autenticación requerido en cualquier momento durante una sesión de usuario: cuando la sesión comienza, durante la sesión cuando los requisitos fuerzan a una reevaluación o cuando el *token* de la sesión expira. Los factores tomados en cuenta para alcanzar el nivel de autenticación requerido son determinados dinámicamente basados en la Política de Control de Acceso que gobierna los recursos que están siendo accedidos, así como una diversidad de condiciones del entorno y factores de riesgo presentes en ese momento para ese usuario.	Designing MFA for Humans
Agente (o "Agente de Atención al Cliente")	La persona responsable de comunicar y resolver problemas en nombre del cliente o usuario final.	Account Recovery (v2), Managing Identity in Customer Service Operations
Gestión Ágil de Proyectos	Es unmarco metodológico que utiliza un proceso continuo y repetitivo para entregar una pieza de funcionalidad, en general un componente de un producto o servicio. Scrum es un marco metodológico popular. (https://www.scrumalliance.org/about-scrum/overview)	Introduction to IAM Project Management
Alineamiento	El índice de sincronización de los procesos y entornos.	Strategic Alignment and Access Governance
Arquitectura	Marco metodológico para el diseño, despliegue y funcionamiento de una infraestructura de tecnología de la información. Provee una estructura	Introduction to IAM Architecture

	en la que una organización puede estandarizar la tecnología que utiliza y alinear su infraestructura TI con las políticas de transformación digital, planes de desarrollo TI y objetivos de negocio.	
Panorama de la Arquitectura	Describe los componentes de la arquitectura requeridos para respaldar la IAM en la empresa.	Introduction to IAM Architecture
Patrones de Arquitectura	Identifica los patrones esenciales que categorizan a la arquitectura de la infraestructura TI de una organización y determina las opciones de implementación de las soluciones IAM.	Introduction to IAM Architecture
Aserción	Un mensaje formal o *token* que transmite información sobre una entidad, normalmente incluye un nivel de seguridad sobre un evento de autenticación y algunas veces incluye información adicional sobre atributos. También se le llama *Token* de Seguridad.	IAM Reference Architecture
Nivel de Seguridad	Una categoría que describe la fortaleza del proceso de demostración de la identidad y/o el proceso de autenticación. Para más información, vea NIST SP.800-63-3.	IAM Reference Architecture
Criptografía Asimétrica	Cualquier algoritmo criptográfico que dependa de pares de claves de encriptación y descifrado. La entidad que genera las claves comparte una (ver Clave Pública) y conserva y protege la otra (ver Clave Privada). Se refiere a ellas como asimétricas porque una clave encripta y la otra descifra.	Practical Implications of Public Key Infrastructure for Identity Professionals
Proveedor de	Cuando la autoridad para los	IAM Reference Architecture

Atributos	atributos se diferencia de la autoridad para las identidades, el término que se usa es “Proveedor de Atributos”. Es un subconjunto o un tipo de Autoridad de Información de la Identidad.	
Control de Acceso Basado en Atributos (“ABAC”) / Control de Acceso Basado en Notificaciones (“CBAC”)	Es un patrón de sistemas de control de acceso que involucra definiciones dinámicas de los permisos basados en información (como atributos o notificaciones), como por ejemplo códigos de trabajo, departamento o grupo de miembros.	Introduction to Policy-Based Access Controls (v2)
Atributos	Pares de claves/valores relevantes para la identidad digital (nombre de usuario, nombre, apellido, etc.)	An Overview of the Digital Identity Lifecycle (v2)
Repositorio de Auditoría	Es un componente que almacena registros de todo evento que pueda luego ser útil para determinar si las operaciones están acordes con la política, para apoyar investigaciones forenses y para permitir el análisis de patrones. Normalmente están altamente controlados para prevenir cualquier falsificación. Un repositorio de auditoría es el nombre ISO que se da a este concepto y forma parte del Administrador de Identidades (IDM, por sus siglas en inglés). En este modelo, el término está generalizado para referirse a cualquier servicio que apoye el registro de eventos desde cualquier parte del ecosistema.	IAM Reference Architecture
Autenticación	La autenticación es un proceso de demostración por el cual se	Introduction to Access Control (v3),

	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.	Authentication and Authorization
Autenticación (AuthN)	El acto de determinar que, a cierto nivel de seguridad, el sujeto/entidad es auténtico.	IAM Reference Architecture
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.	Identity and Access Management Workforce Planning
Aserción AuthN	Es un *token* de seguridad en el que el Proveedor de Identidades (IdP, por sus siglas en inglés) provee información de seguridad y autenticación de forma segura al tercero fiable (RP, por sus siglas en inglés).	IAM Reference Architecture
Fuente Acreditada	Es el sistema de registro (SOR, por sus siglas en inglés) para datos de identidad. Una organización puede tener más de una fuente acreditada de datos en su entorno.	User Provisioning in the Enterprise
Autorización	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	Introduction to Access Control, Authentication and Authorization

	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).	
Autorización (AuthZ)	La autorización es cómo se toma una decisión durante la ejecución para permitir el acceso a un recurso. Se divide en dos tipos: compartidas y locales. El marco metodológico FICAM incluye a la misma como un subcomponente del Sistema de Administración de Acceso. El concepto AuthZ no está incluido en los modelos ISO ni Internet2.	IAM Reference Architecture
Entorno de Gestión Automática de Certificados (ACME, por sus siglas en inglés)	Es un protocolo de comunicación para automatizar la gestión de certificados digitales de clave pública (PKI, por sus siglas en inglés). Proveedores destacados como *Let's Encrypt* hacen uso de ACME para respaldar la emisión de certificados TLS para servidores web.	Practical Implications of Public Key Infrastructure for Identity Professionals
Federación Bilateral	Una federación bilateral es aquella que consiste solamente en dos entidades: un Proveedor de Identidades (IdP, por sus siglas en inglés) y un Proveedor de Servicios (SP, por sus siglas en inglés). Este es el modelo más común para una federación de identidad empresarial.	Federation Simplified (v2)
Enlazar	Asociar un autenticador con una	Identity and Access

	identidad.	Management Workforce Planning
Bot	A veces llamado *bot* de Internet, es una abreviación de "robot" pero se refiere a un software rutinario que realiza tareas automatizadas en Internet. También puede ser un robot web que se refiere a una aplicación de red autónoma o simplemente "*bot*", que se refiere a una tarea automatizada, generalmente repetitiva, utilizada para un propósito específico.	Non-Human Account Management (v2)
Ceremonias	Son interacciones predecibles que los usuarios pueden ocasionalmente enfrentar en espacios vigilados.	Introduction to Identity – Part 2: Access Management
Lista de Certificados Raíz de Confianza (CTL, por sus siglas en inglés)	Un cliente mantiene una lista de Certificados Raíz de Confianza creada y gestionada por el software proveedor o por administradores locales. El cliente solo confía en los certificados emitidos bajo una de las autoridades de certificación (CA, por sus siglas en inglés) en la CTL, con lo cual la CTL sirve como "lista segura".	Practical Implications of Public Key Infrastructure for Identity Professionals
Sistema de Gestión de Certificados (CMS, por sus siglas en inglés)	Es un sistema que gestiona y reporta información sobre la emisión y revocación de certificados. Un CMS integra los productos de la autoridad de certificación (CA, por sus siglas en inglés) con sistemas de Gobernanza y Administración de Identidad (IGA, por sus siglas en inglés) así como con sistemas de Mesa de Ayuda.	Practical Implications of Public Key Infrastructure for Identity Professionals
Política de	Es un documento que define los	Practical Implications of

Certificados (CP, por sus siglas en inglés)	requisitos de alto nivel de las políticas para una infraestructura de clave pública (PKI, por sus siglas en inglés). RFC 3647 identifica un marco de políticas PKI y describe los contenidos y el resumen de la Política de Certificados (CP). Una empresa operando una autoridad de certificación (CA, por sus siglas en inglés) a menudo publica su política de certificados a partes externas para que las mismas puedan determinar si confían o no en los certificados emitidos por la CA.	Public Key Infrastructure for Identity Professionals
Declaración de Prácticas de Certificación (CPS, por sus siglas en inglés)	Una Política de Certificados (CP, por sus siglas en inglés) identifica los requisitos para gestionar una autoridad de certificación (CA, por sus siglas en inglés) y emitir certificados de infraestructura de clave pública (PKI, por sus siglas en inglés). Una CPS describe cómo el CA implementa dichos requisitos. El CPS utiliza la misma síntesis que la CP, definido en RFC 3647. A diferencia de con la CP, las empresas rara vez publican su CPS "en bruto", sin editar.	Practical Implications of Public Key Infrastructure for Identity Professionals
Lista de Revocación de Certificados (CRL, por sus siglas en inglés)	Una autoridad de certificación publicará una lista de los certificados revocados, llamada CRL, para que los clientes puedan verificar si un certificado aún es válido.	Practical Implications of Public Key Infrastructure for Identity Professionals
Solicitud de Firma de Certificado (CSR, por sus siglas en inglés)	Al solicitar un certificado, la entidad solicitante provee una copia de la clave pública, sus identificadores y otra información, en un objeto binario específicamente formateado	Practical Implications of Public Key Infrastructure for Identity Professionals

	llamado CSR.	
Canal	Es la ruta de comunicación entre tú y tu usuario final, o entre su agente y su cliente. Esta puede ser teléfono, chat, redes sociales u otras vías.	Managing Identity in Customer Service Operations
Triada CID	Son los conceptos fundamentales de clasificación de riesgos de la seguridad de la información de recursos desde las perspectivas de Confidencialidad, Integridad y Disponibilidad.	Non-Human Account Management (v2)
Control de Acceso basado en Notificaciones Proclamaciones (CBAC, por sus siglas en inglés)	Ver Control de Acceso basado en Atributos (ABAC, por sus siglas en inglés)	Introduction to Policy-Based Access Controls (v2)
Computadora Clásica	Es una computadora que utiliza código binario y álgebra de Boole para hacer sus cálculos de manera determinista. Usamos el término Computadora Clásica para diferenciarla de la Computadora Cuántica.	Practical Implications of Public Key Infrastructure for Identity Professionals
Gestión de derechos de infraestructura en la nube (CIEM, por sus siglas en inglés)	Una clasificación de las tecnologías enfocada en gestionar la otorgación, verificación y perfeccionamiento de los permisos para las tecnologías en la nube o híbridas. CIEM es a menudo visto como un componente de la Gobernanza y Administración de Identidades (IGA, por sus siglas en inglés).	Techniques To Approach Least Privilege
Modelo por Competencias	Una serie de tareas, conocimientos y aptitudes (TKS, por sus siglas en inglés) necesarias para el desarrollo eficaz de un trabajo. Un Modelo por	Identity and Access Management Workforce Planning

	competencias forma parte de un marco laboral.	
Consentimiento	Permiso para que algo ocurra o acuerdo de hacer algo.	Introduction to Privacy and Compliance for Consumers
Ley de Protección del Consumidor	Leyes y regulaciones que están diseñadas para proteger los derechos de los consumidores individuales y para impedir prácticas de negocio desleales, engañosas y fraudulentas.	Laws Governing Identity Systems
Contexto	Condiciones bajo las cuales se autoriza una acción en un recurso a un sujeto, como por ejemplo el tiempo de acceso, la ubicación de acceso o determinados requisitos de cumplimiento.	Introduction to Policy-Based Access Controls (v2)
Autenticación Continua	La autenticación continua es un mecanismo que utiliza diversos indicadores y medidas para determinar si, a lo largo de una sesión de usuario, ha habido algún cambio en el nivel de confianza de que se trata del mismo usuario que se autenticó al inicio de la sesión.y disparar una acción de autenticación si hay una caída en el nivel de dicha confianza.	Designing MFA for Humans
Derecho contractual	Leyes relativas a la creación y ejecución de acuerdos entre partes distintas.	Laws Governing Identity Systems
Credencial	Una credencial permite la autenticación de una entidad enlazando la identidad a un autenticador.	IAM Reference Architecture
Administración de Credenciales	Refiere a cómo emitir, administrar y revocar autenticadores enlazados a identidades. La administración de	Identity and Access Management Workforce Planning

	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).	
Proveedor de Servicios de Credenciales	Siguiendo la guía incluida en NIST 800-63-3, agrupamos bajo el nombre “Proveedor de servicios de credenciales'' tanto la función de registro/inscripción como los servicios de credenciales.	IAM Reference Architecture
Servicios de Credenciales	Los Servicios de Credenciales expiden o registran a los autenticadores inscriptos, entregan la credencial para usar y consecuentemente administran dichas credenciales. Incluimos información de infraestructura de clave pública (PKI, por sus siglas en inglés) para arquitecturas de Administración de Identidades y Accesos (IAM, por sus siglas en inglés) que deben incluir componentes del sistema que requieran certificados y claves privadas. En líneas generales, esto se corresponde al componente FICAM llamado Sistemas de Administración de Credenciales.	IAM Reference Architecture
Credenciales	Cualquier atributo o secreto compartido que pueda ser utilizado para autenticar a un usuario.	Account Recovery (v2)
Módulo Criptográfico	Un componente de hardware o software que ejecuta operaciones criptográficas seguras dentro de un	Practical Implications of Public Key Infrastructure for Identity Professionals

	marco lógico. Los módulos criptográficos almacenan claves privadas y las utilizan para funciones criptográficas a pedido de un usuario o proceso.	
Programa de Validación de Módulos Criptográficos (CMVP, por sus siglas en inglés)	Es un programa que permite a los desarrolladores de módulos criptográficos testear sus módulos con los requisitos definidos en FIPS-140. El centro de recursos de seguridad informática que funciona bajo el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, por sus siglas en inglés), ofrece una lista de público acceso de los módulos validados.	Practical Implications of Public Key Infrastructure for Identity Professionals
Controlador de Datos	Según la definición del Artículo 4(7) del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés): “un controlador es la persona natural o legal, autoridad, agencia u otro órgano que, solo o juntamente con otros, determina los objetivos y significados del procesamiento de datos personales.” Este artículo utiliza el término “organización” como sinónimo de “controlador de datos” porque las organizaciones involucradas en la Administración de Identidades y Accesos (IAM, por sus siglas en inglés) son generalmente los controladores de datos.	An Introduction to the GDPR
Mapeo de Datos	Un sistema de registro de qué datos se recopilan, cómo se usan, dónde se almacenan y cómo viajan dentro y fuera de tu organización.	Impact of GDPR on Identity and Access Management

Procesador de Datos	Según la definición del Artículo 4(8) del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), es cuando una organización procesa datos personales únicamente a pedido de otros. Un procesador de datos no debe determinar el objetivo del procesamiento, por ejemplo, procesando datos para sus intereses personales ni más allá de las decisiones técnicas delimitadas. Los procesadores de datos están regulados por el Artículo 28: concretamente deben tener un contrato con el controlador de datos que cubra todos los ítems del Artículo 28(3). Los procesadores de datos están exentos de algunas, pero no de todas las responsabilidades y deberes de los controladores de datos.	An Introduction to the GDPR
Protección de Datos desde el Diseño	Protección de datos a través de tecnología de diseño. Ver el Artículo 25 del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) para más información	Impact of GDPR on Identity and Access Management
Oficial de Protección de Datos (DPO, por sus siglas en inglés)	Un individuo que debe ser designado por cualquier organización que procese cualesquiera datos definidos como sensibles por el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés). El DPO es responsable de “trabajar por el cumplimiento de todas las leyes relevantes de protección de datos, monitorear procedimientos específicos como la evaluación del	Impact of GDPR on Identity and Access Management

	impacto de la protección de datos, ampliar la conciencia de los empleados sobre la protección de datos y capacitarlos acorde, así como colaborar con las autoridades de supervisión." Ver los artículos 35, 37, 38 y 39 de GDPR para más información.	
Sujeto de Datos	Según la definición del Artículo 4(1) del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) - ver "Datos Personales"- es el término formal para referirse al humano vinculado a sus datos personales. Este artículo utiliza el término "individuo" como sinónimo de "sujeto de datos".	An Introduction to the GDPR
Identificador Descentralizado (DID, por sus siglas en inglés)	Es un identificador que es creado y anclado a un sistema descentralizado como una cadena de bloques (blockchain) o registro distribuido y puede representar a una entidad en el ecosistema -un emisor, un propietario, un verificador o incluso un *hub* de identidad.	A Peek into the Future of Decentralized Identity
Infraestructura de Autenticación Delegada	Es un marco de control de acceso que separa la autenticación de la autorización, permitiendo que la contraseña se mantenga local y protegida.	Introduction to Identity – Part 2: Access Management
Tarjetas Digitales	Son las credenciales verificables que los usuarios recopilan con el tiempo y que están almacenadas como parte del agente o del *hub* de identidad del usuario. En cierta forma, es más sencillo referirse a ellas como tarjetas digitales que	A Peek into the Future of Decentralized Identity

	como credenciales verificables.	
Identidad Digital	Es la combinación de un identificador único con los atributos relevantes que identifican unívocamente a una entidad.	An Overview of the Digital Identity Lifecycle (v2)
Billetera Digital	Es una metáfora digital que representa a una billetera física y que es en general representada por la combinación del agente de usuario y de las subyacentes capacidades del dispositivo informático, como el almacenamiento y enclave seguros en un teléfono móvil. La billetera digital contiene tarjetas digitales.	A Peek into the Future of Decentralized Identity
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.	Authentication and Authorization
Control de Acceso Discrecional	Es un modelo de sistema de control de acceso que involucra definiciones manuales fijas sobre los permisos asignados directamente a los usuarios.	Introduction to Policy-Based Access Controls (v2)
Infraestructura descentralizada de clave pública (dPKI, por sus siglas en	Es una infraestructura descentralizada de clave pública que generalmente se implementa mediante una cadena de bloques	A Peek into the Future of Decentralized Identity

inglés)	(blockchain) o un registro distribuido -un lugar donde los identificadores descentralizados (DIDs, por sus siglas en inglés) pueden registrarse y ser buscados junto a las claves públicas asociadas al DID y sus metadatos. En términos generales, una dPKI puede ser descrita como un registro de datos verificables ya que la dPKI es solo una de las muchas formas de implementación de un registro de datos verificables que existen. Si bien este artículo se refiere a la infraestructura descentralizada de clave pública, el lector debe saber que un registro de datos verificables no debe ser necesariamente descentralizado.	
Servicios Electrónicos de Identificación, autenticación y Confianza (eIDAS, por sus siglas en inglés)	Legislación europea que otorga estatus legal a las firmas electrónicas. Para cumplir con los requisitos de firma electrónica calificada, esta legislación también documenta cómo proveer firmas digitales con certificados X.509 que sean legalmente vinculantes.	Practical Implications of Public Key Infrastructure for Identity Professionals
Criptografía de Curva Elíptica (ECC, por sus siglas en inglés)	Un sistema criptográfico asimétrico basado en calcular puntos da lo largo de curvas elípticas.	Practical Implications of Public Key Infrastructure for Identity Professionals
Cifrado	Es el procesamiento de datos utilizando un algoritmo criptográfico para asegurar la confidencialidad.	Practical Implications of Public Key Infrastructure for Identity Professionals
Cumplimiento	Son los mecanismos que aseguran que un individuo no pueda ejecutar una acción o acceder a un sistema cuando los mismos estén	IAM Reference Architecture

	prohibidos por políticas.	
Inscripción	La inscripción o registro concierne los aspectos de demostración y ciclo de vida del sujeto. La entidad que lleva a cabo la inscripción es a veces conocida como Autoridad de Registro pero nosotros, conforme a NIST SP.800-63-3, utilizaremos el término Proveedor de Servicios de Credenciales.	IAM Reference Architecture
Arquitectura Empresarial	Una arquitectura que cubre todos los componentes del entorno de la Tecnología de la Información (TI).	Introduction to IAM Architecture
Derechos	Artefacto que permite el acceso a un recurso por parte de una entidad principal. Se conoce también como privilegio, derecho de acceso, permiso o autorización. Un derecho puede ser implementado de muchas formas.	IAM Reference Architecture
Catálogo de recursos para la Administración de Derechos	Es una base de datos de los derechos y los metadatos asociados. El catálogo incluye un índice de datos de derechos tomados de sistemas de negocios, aplicaciones y plataformas, así como descripciones técnicas y de negocio de los derechos y sus usos.	User Provisioning in the Enterprise
Administración de Derechos	Catalogación y gestión de todos los accesos que una cuenta puede tener. Este es el proceso de negocio para suministrar accesos.	Introduction to Identity - Part 1: Admin-time (v2)
Identificador Externo	Son los recursos mediante los cuales una persona que controla una identidad digital se refiere a esa identidad cuando está interactuando con un sistema.	Identifiers and Usernames

Número de la Credencial Inteligente para una Agencia Federal (FASC-N)	Un identificador único asociado a una tarjeta inteligente. FASC-N se utiliza en el estándar PIV (Verificación de Identidad Personal) del Gobierno Federal de Estados Unidos para apoyar el Acceso Físico.	Practical Implications of Public Key Infrastructure for Identity Professionals
Estándar Federal de Procesamiento de Información ("FIPS") 140	Un estándar del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) que define los requisitos de seguridad para los módulos criptográficos.	Practical Implications of Public Key Infrastructure for Identity Professionals
Control de Acceso Federado	Es una arquitectura de control de acceso que contempla la separación de la autoridad usuario/sujeto de la autoridad recurso/objeto.	Introduction to Policy-Based Access Controls (v2)
Identidad Federada	Son los medios para enlazar la identidad electrónica y atributos de una persona, almacenados en múltiples y diferentes sistemas de administración.	Introduction to Identity – Part 2: Access Management
Identidad Fracturada	Un caso donde un usuario final tiene múltiples y dispares identidades digitales.	Managing Identity in Customer Service Operations
Ley Antifraude	Leyes que protegen contra la representación falsa e intencional de información hecha por una persona hacia otra que confía en ella, con conocimiento de su falsedad y con el propósito de inducir a la otra persona a actuar de forma que resulte en daños y perjuicios para sí misma.	Laws Governing Identity Systems
Diagrama de Gantt	Es un formato popular de organización que muestra en un mismo gráfico la tarea a realizar y el periodo de tiempo para hacerla.	Introduction to Project Management for IAM Projects
Reglamento General	Oficialmente, el Reglamento	An Introduction to the GDPR

de Protección de Datos (GDPR, por sus siglas en inglés)	2016/679 de la Unión Europea vigente desde el 25 de mayo de 2018. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679	
Gobernanza	Garantizar que los propietarios responsables tienen el control, de forma demostrable.	Strategic Alignment and Access Governance
Grupos	Un conjunto de identidades con permisos definidos. En este contexto específico, un grupo alberga muchos individuos, pero la identidad de grupo es opaca y ningún tipo de información sobre qué acción realizó un miembro individual del grupo está disponible.	Practical Implications of Public Key Infrastructure for Identity Professionals
Módulo de Seguridad de Hardware (HSM, por sus siglas en inglés)	Es un dispositivo de hardware que genera y protege claves criptográficas.	Practical Implications of Public Key Infrastructure for Identity Professionals
Titular	Es la entidad que posee credenciales verificables. Los Titulares son generalmente usuarios, pero también pueden ser organizaciones o dispositivos.	A Peek into the Future of Decentralized Identity
Identificación	Establecer inequívocamente al usuario de un sistema o de una aplicación.	Introduction to Access Control
Identificador	La forma en la que un sistema se refiere a una identidad digital. Los certificados de infraestructura de clave pública (PKI, por sus siglas en inglés) apoyan tanto a los identificadores internos como a los externos. Para tener un panorama general sobre los identificadores vea el articulo de Ian Glazer:	Practical Implications of Public Key Infrastructure for Identity Professionals

	"Identifiers and Usernames,"	
Identidad	Son los atributos que definen a un usuario humano y que pueden variar en los diferentes dominios. Por ejemplo: la identidad digital de un usuario tendrá una definición diferente en su entorno laboral que en el banco del usuario. Un dispositivo identificador es a veces referido como su identidad.	Non-Human Account Management (v2)
Analítica de Identidad e Inteligencia (IdA, por sus siglas en inglés)	La analítica de identidad e inteligencia significa observar los datos de derechos, concretamente la asignación de estos, y tratar de averiguar qué tipo de riesgos se enfrenta. IdA ofrece un enfoque de riesgo para administrar sistemas de identidades y accesos, con el objetivo de centralizar la gobernanza, visibilidad y reporte para el riesgo basado en el acceso.	Introduction to Identity - Part 1: Admin-time (v2)
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.	Authentication and Authorization
Administración de Identidades y Accesos (IAM, por sus siglas en inglés)	La disciplina que permite a los individuos correctos acceder a los recursos correctos, en los momentos correctos y por las razones correctas.	Identity and Access Management Workforce Planning
Planificación del trabajo para la Administración de Identidades y Accesos	Actividades realizadas para garantizar que el equipo de administración de identidades y accesos de una empresa está compuesto de las aptitudes indicadas para ejecutar los objetivos técnicos y de negocio.	Identity and Access Management Workforce Planning

Administración de Identidades, Credenciales y Accesos (ICAM, por sus siglas en inglés)	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 de acceso y para valerse de las credenciales a fin de proveer un acceso autorizado a los recursos de una organización.	Identity and Access Management Workforce Planning
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 identidad ocurre cuando un Proveedor de Identidades (IdP) y un Proveedor de Servicio (SP) 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 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	Federation Simplified (v2)

	refiere al estatus y afiliación de un usuario. La Federación 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]No obstante y dado que es lo más común hoy en día, este artículo se centra en los casos de uso de empresa en los que los acuerdos bilaterales federados, es decir donde los acuerdos son uno-a-uno entre IdP y SP, son la forma de federación de identidad utilizada.	
Administración y Gobernanza de Identidades (IGA, por sus siglas en inglés)	Es una disciplina que se enfoca en la gestión del ciclo de vida de la identidad y el control de acceso desde una perspectiva administrativa.	Introduction to Identity - Part 1: Admin-time (v2)
Administración y Gobernanza de Identidades (IGA, por sus siglas en inglés)	Incluye la recopilación y uso de información de identidad, así como procesos de gobernanza que aseguran que la persona correcta tiene el acceso correcto a los sistemas correctos en el momento correcto.	Introduction to IAM Architecture
Administración y Gobernanza de Identidades (IGA, por sus siglas en inglés)	Una solución para automatizar la administración de usuarios y las autorizaciones en los sistemas objetivo, construida sobre los procesos de clientes y de recursos humanos de la organización.	Strategic Alignment and Access Governance
Hub de Identidad o Repositorio	Es el lugar en el que los usuarios pueden almacenar la información relativa a su identidad encriptada. Un *hub* de identidad puede estar en cualquier lado -en la frontera, en la	A Peek into the Future of Decentralized Identity

	nube o en tu propio servidor. Su propósito es almacenar datos personales. Algunas implementaciones pueden permitir que otras entidades accedan al *hub* de identidad de un usuario si el usuario específicamente concede dicho acceso. Se puede pensar los *hubs* de identidad como un almacén de datos personales de un individuo.	
Autoridad de Información de Identidades (IIA, por sus siglas en inglés)	Representa una o más fuentes de datos usados 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.	IAM Reference Architecture
Administración del Ciclo de vida de Identidades	Es un proceso que detecta cambios en los sistemas de registro acreditados y que actualiza los registros de identidades basado en políticas.	User Provisioning in the Enterprise
Administración de Identidades (IDM, por sus siglas en inglés)	Es un conjunto de políticas, procedimientos, tecnología y otros recursos usados para mantener la información de identidades. La IDM contiene información sobre entidades principales/sujetos,	IAM Reference Architecture

	incluyendo credenciales. Puede también incluir otros datos como metadatos para habilitar la interoperabilidad con otros componentes. La IDM se muestra con una línea punteada para indicar que es una agrupación conceptual de componentes y no un sistema en sí mismo.	
Demostración de Identidad	Es la acumulación de evidencia para sustentar "de quién se trata". La demostración de identidad es la última parte, pero no por eso menos importante, de esta parte de la administración. Es el proceso de recopilar y verificar la información sobre una persona con el objetivo de proveer una cuenta o la credencial correspondiente. Normalmente esto se realiza antes de que una cuenta sea creada, que una credencial sea emitida o que un privilegio especial sea otorgado.	Introduction to Identity - Part 1: Admin-time (v2)
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,	Federation Simplified (v2), Authentication and Authorization

	como es el caso de los navegadores de Internet.”	
Proveedor de Identidad (IdP, por sus siglas en inglés)	Un Proveedor de Identidades o IdP es un término común. Lo consideramos un subconjunto de servicios dentro de la Administración de Identidades. Consiste en las interfaces de servicios: AuthN/Aserción, Agentes de Aprovisionamiento de Servicios, Administración de Sesiones, Servicios de Detección y Administración de Metadatos.	IAM Reference Architecture
Registro de Identidad	Es un almacén de datos que contiene las entidades inscritas o registradas y sus correspondientes atributos, incluyendo sus credenciales. Vea la sección IDM para mas detalles. Los términos Directorio, Repositorio de Identidad y Almacén de Atributos se utilizan frecuentemente como sinónimos.	IAM Reference Architecture
Repositorio de Identidades	Un repositorio de identidades es un directorio o base de datos que puede ser referenciado por sistemas y servicios externos (como servicios de autenticación o autorización).	User Provisioning in the Enterprise
Leyes de Robo de Identidad	Leyes que rigen los crímenes en los que un perpetrador accede a información personal sensible perteneciente a la víctima (como fecha de nacimiento, contraseñas, direcciones de correo electrónico, números de seguridad social, registros financieros, etc.) y luego la utiliza para hacerse pasar por la víctima para beneficio personal, como por ejemplo cometer fraude,	Laws Governing Identity Systems

	sacar préstamos en nombre de la víctima o acceder a las cuentas de la víctima.	
Impersonar un usuario (‘impersonar’ no existe en español, pero ‘suplantación de identidad’ me parece que lleva incorrectamente a un caso de robo de identidad)	Es una situación en la que un usuario puede realizar acciones como si fuera otro usuario.	Managing Identity in Customer Service Operations
Infraestructura como Código	Es un proceso de administración y aprovisionamiento de los centros de datos informáticos (*Data Centers*) mediante ficheros legibles por máquina en lugar de configuraciones físicas de hardware o de herramientas interactivas de configuración.	Techniques To Approach Least Privilege
Intercambio de Claves de Internet (IKE, por sus siglas en inglés)	Es una norma subordinada a IPsec que especifica cómo utilizar los certificados X.509 para establecer claves simétricas para un túnel IPsec.	Practical Implications of Public Key Infrastructure for Identity Professionals
Seguridad de Protocolo de Internet (IPsec)	Es una norma para la comunicación entre dos máquinas que provee confidencialidad e integridad del Protocolo de Internet.	Practical Implications of Public Key Infrastructure for Identity Professionals
Intraorganizacional (Inicio de Sesión Único)	Es una identidad digital central, como una cuenta en un directorio, vinculada por sistemas internos como acreditada para la autenticación.	An Overview of the Digital Identity Lifecycle (v2)
Interorganizacional (Federación)	Es una organización que confía en la identidad digital de otra	An Overview of the Digital Identity Lifecycle (v2)

	organización y en sus procesos de administración del ciclo de vida.	
Identificador interno	La forma en que el sistema de administración de identidades se refiere a una identidad digital.	Identifiers and Usernames
Emisor	La entidad que emite credenciales verificables sobre sujetos a propietarios o titulares. En general, los emisores son entidades gubernamentales o corporaciones, sin embargo, un emisor puede también ser una persona o un dispositivo.	A Peek into the Future of Decentralized Identity
Incorporaciones/Traslados/Bajas	Es el ciclo de vida de incorporación/traslado/baja de la identidad de un empleado y tiene en cuenta los tres estados del ciclo de vida de un empleado: la incorporación a la organización, el traslado dentro de la organización (cambio de área o departamento) y la partida o baja de la organización.	Introduction to Identity - Part 1: Admin-time (v2)
Creación de la Identidad Digital mediante un recorrido *(Journey-based Creation*)	Es un proceso que guía a un cliente a través de una serie de interacciones antes de establecer una identidad digital. Por ejemplo, registrar la información básica mínima requerida para que un cliente pueda crear su identidad digital.	An Overview of the Digital Identity Lifecycle (v2)
Acceso JIT (por sus siglas en inglés) o Acceso Justo a Tiempo	Es una técnica mediante la cual una credencial o un permiso son otorgados temporalmente a una entidad principal por el lapso necesario para desarrollar una actividad determinada. El acceso es revocado una vez que la actividad es completada, limitando su uso.	Techniques To Approach Least Privilege

Clave	En un sistema criptográfico, una clave es un dato utilizado en un algoritmo criptográfico para encriptar o descifrar datos.	Practical Implications of Public Key Infrastructure for Identity Professionals
Autenticación basada en el conocimiento (KBA, por sus siglas en inglés)	Es un método de autenticación que usa información conocida por el usuario final y por el servicio de autenticación, pero que no es necesariamente secreta.	Account Recovery (v2), Managing Identity in Customer Service Operations
Principio de Mínimo Privilegio	Principio por el cual un recurso, como un usuario, puede acceder únicamente a los recursos (como aplicaciones, datos, etc.) que son necesarios para el cumplimiento de su función.	Introduction to Identity – Part 2: Access Management
Principio de Mínimo Privilegio	Es el principio fundamental sobre el cual debe diseñarse una arquitectura de seguridad de modo de que se otorgue el acceso y las autorizaciones mínimas necesarias a los recursos del sistema para que una entidad pueda realizar su función. (*NIST Information Technology Laboratory*).	Techniques To Approach Least Privilege
Autorización Local	Una autorización local es otorgada por el RP (*Relying Party* o tercero fiable).	IAM Reference Architecture
Administración de Metadatos	Son los procesos y técnicas que permiten recopilar, utilizar y eventualmente eliminar los datos de control usados por la IDM para reconocer y confiar en el *Relying Party* (o tercero fiable). El término se corresponde con "Datos del *Relying Party*" utilizado en el modelo Internet2.	IAM Reference Architecture
Bombardeo por	El bombardeo por autenticación	Multi-factor Authentication

Autenticación Multifactor	*multifactor* es una técnica de ciberataque en la que un atacante bombardea a un usuario con notificaciones *push* vía celular o teléfono móvil. Esto lleva al usuario a aprobar la solicitud por cansancio lo que puede a su vez derivar en una apropiación de cuenta.	
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—).	Account Recovery (v2), Introduction to Access Control
Federación Multilateral	Es una federación que consiste en múltiples entidades que han acordado un marco de confianza específico. Existen muchas formas de federación multilateral incluyendo modelos de distribución *hub-and-spoke* y *mesh*. Las federaciones multilaterales son el modelo de federación de identidad más usado en el ámbito académico.	Federation Simplified (v2)
Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés)	Es una agencia gubernamental estadounidense que define y publica varios estándares. Uno de los departamentos del NIST, el Centro de Recursos de Seguridad Informática (CSRC, por sus siglas en inglés), publica las series de Estándares Federales de Procesamiento de la Información (FIPS, por sus siglas en inglés). Si bien estos estándares son obligatorios únicamente para las	Practical Implications of Public Key Infrastructure for Identity Professionals

	agencias gubernamentales estadounidenses, muchos países los reconocen como los estándares mundiales de facto.	
Cuenta de Persona No Humana	Cualquier cuenta que no sea utilizada por una persona, como cuentas usadas para dispositivos, servicios y servidores.	Non-Human Account Management (v2)
Entidades No Humanas (NPE, por sus siglas en inglés)	Es una combinación única de hardware y firmware (por ej.: un dispositivo) que utiliza las capacidades de otros programas, dispositivos o servicios para llevar a cabo una función. Las entidades no humanas pueden actuar independientemente o en el nombre de un individuo autenticado o de otra NPE.	Practical Implications of Public Key Infrastructure for Identity Professionals
OAuth 2.0	OAuth 2.0 es un protocolo de código abierto que permite a los Propietarios de Recursos, como aplicaciones, compartir datos con sus clientes facilitando la comunicación con un Servidor de Autorización (AS, por sus siglas en inglés). Los datos toman la forma de credenciales otorgadas a las aplicaciones para obtener información/datos de otras aplicaciones. El Servidor de Autorización es en general el Proveedor de Identidades (IdP, por sus siglas en inglés). El Servidor de Autorización puede otorgar autorizaciones directa o indirectamente. Por ejemplo, el AS puede proveer atributos o datos del perfil del Propietario de Recursos u otorgar acceso a datos que puedan ser usados con propósitos de	Federation Simplified (v2)

	autorización, como permisos de un IDM o IGA.	
Protocolo de Estado de Certificado En Línea (OCSP, por sus siglas en inglés)	Es un protocolo que permite a un cliente consultar el estatus de un certificado individual ante la Autoridad de Certificación o Autoridad de Validación en vez de descargar una Lista de Revocación de Certificados (o CRL).	
OpenID Connect (OIDC)	OpenID Connect es una capa de identidad simple sobre el protocolo OAuth 2.0. Habilita a los clientes a verificar la identidad del Usuario Final basándose en la autenticación llevada a cabo por un Servidor de Autorización y permite obtener un perfil de información básico sobre el usuario final de manera interoperable y siguiendo la transferencia de estado representacional (REST, por sus siglas en inglés).	Federation Simplified (v2)
Detección y Validación de Rutas (PDVal)	Es el proceso para determinar si un certificado está validado y acreditado por el validador.	Practical Implications of Public Key Infrastructure for Identity Professionals
Permiso	Es una declaración de autorización para uno o más sujetos para que realicen una o más acciones sobre uno o más objetos.	Introduction to Policy-Based Access Controls (v2)
Datos Personales	De acuerdo con la definición del Artículo 4(1) del Reglamento General de Protección de datos (GDPR, por sus siglas en inglés): “Los datos personales son cualquier información relativa a una persona natural identificada o identificable (sujeto de datos); una persona	An Introduction to the GDPR

	natural identificable es una persona que puede ser identificada directa o indirectamente; concretamente referenciando un identificador como el nombre, número de identificación, datos de ubicación, un identificador en línea o uno o más factores específicos a la identidad de la persona natural como componentes físicos, fisiológicos, genéticos, mentales, económicos, culturales o sociales". Nota: el término "persona natural" (humano) es usado para diferenciarse de compañías u otras entidades corporativas que son "personas legales".	
Datos Personales	Los Datos Personales son cualquier información asociada a una persona natural identificada o identificable.	Account Recovery (v2), Impact of GDPR on Identity and Access Management
Número de Identificación Personal (PIN, por sus siglas en inglés)	Es un número secreto comúnmente usado para desbloquear un contenedor de clave privada en un software o hardware.	Practical Implications of Public Key Infrastructure for Identity Professionals
Verificación de Identidad Personal (PIV, por sus siglas en inglés)	Es un programa del gobierno estadounidense basado en una Infraestructura de Clave Pública que está diseñado para habilitar una autenticación fuerte para todos los empleados gubernamentales y contratistas públicos.	Practical Implications of Public Key Infrastructure for Identity Professionals
Punto de Administración de Políticas (PAP, por sus siglas en inglés)	Es la ubicación donde los diferentes tipos de propietarios definen las políticas de acceso.	Introduction to Access Control
Punto de Decisión de Políticas (PDP, por sus siglas en	Es el motor de políticas que valida las solicitudes de acceso y los atributos provistos ante la Política	Introduction to Access Control

inglés)	de Acceso (tal y como definido en el Punto de Administración de Políticas).	
Punto de Aplicación de Políticas (PEP, por sus siglas en inglés)	Es la autoridad que habilitará únicamente a un Solicitante de Acceso a conectarse al Proveedor de Acceso si el Punto de Decisión de Políticas lo permite.	Introduction to Access Control
Motor de Política	Es un componente de seguridad que valida si un actor tiene permitido acceder a un recurso protegido, siguiendo los requisitos de una política de acceso.	Introduction to Access Control
Punto de Información de Políticas	Es la autoridad que consulta a los proveedores confiables (externos) de los atributos que serán usados en la Decisión de Acceso. Un ejemplo de esto es el servicio myacclaim.com que administra las Insignias Abiertas (*open badges*) de certificación como CISSP y MSCP.	Introduction to Access Control
Control de Acceso basado en Políticas (PBAC, por sus siglas en inglés)	Es un patrón de sistema de control de acceso que tiene en cuenta las definiciones dinámicas sobre los permisos de acceso, basándose en los atributos del usuario (como en ABAC) y en las variables del contexto para permitir o denegar el acceso.	Introduction to Policy-Based Access Controls (v2)
Principio de Mínimo Privilegio	Es la mejor práctica de seguridad de la información para garantizar que dentro de un sistema de control de acceso, los usuarios no tengan acceso a recursos más que el estrictamente necesario para la realización de sus actividades.	Introduction to Policy-Based Access Controls (v2)
Privacidad	Es un concepto abstracto que no tiene una única definición general.	Introduction to Privacy and Compliance for Consumers

Ley de Privacidad	Es el conjunto de leyes que regula la recopilación, uso, almacenamiento y transferencia de datos personales asociados a individuos identificados o identificables.	Laws Governing Identity Systems
Clave Privada	Es una clave que sólo una única entidad individual controla de forma privada y exclusiva. Se asocia con una clave pública que la entidad puede compartir para la encriptación de datos o verificación de firma.	Practical Implications of Public Key Infrastructure for Identity Professionals
Administración de Accesos con Privilegios	Es un mecanismo para administrar el acceso temporal a cuentas con permisos de riesgo alto. A menudo, PAM (por su siglas en inglés) implica la entrega y devolución de una credencial generada para un solo uso.	Techniques To Approach Least Privilege
Administración de Cuentas con Privilegios (PAM, por sus siglas en inglés)	Realizar un control especial de los accesos de alto nivel de riesgo. La Administración de Cuentas con Privilegios (PAM, por sus siglas en inglés) es un mecanismo para tener bajo control esas cuentas especiales.	Introduction to Identity - Part 1: Admin-time (v2)
Procesamiento	De acuerdo con la definición del Artículo 4(2) del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés): “el ‘procesamiento‘ significa cualquier operación o conjunto de operaciones que se realicen sobre datos personales o conjuntos de datos personales, ya sea o no por medios automáticos. Las mismas pueden ser la recopilación, el registro, la organización, la estructuración, el almacenamiento,	An Introduction to the GDPR

	la adaptación o alteración, la recuperación, la consulta, el uso, la divulgación por transmisión, la diseminación o puesta a disposición, el alineamiento o la combinación, la restricción, el borrado o la destrucción." Nótese que incluso esta larga lista de actividades no es exhaustiva: otras actividades pueden caer dentro del concepto de "procesamiento". Reglas adicionales, presentes en el Artículo 22, aplican para las "tomas de decisión automáticas individuales, incluyendo el trazado de un perfil". En general estas reglas fortalecen los derechos de información y los derechos de objeción descritos más adelante, y pueden limitar el uso de la automatización en decisiones de alto impacto.	
Proyecto	Una actividad de tiempo limitado para lograr uno o varios resultados determinados.	Introduction to Project Management for IAM Projects
Estatuto del Proyecto	La autorización documentada para que el gerente o gestor de proyecto proceda con un proyecto; en general incluye una descripción breve del objetivo del proyecto.	Introduction to Project Management for IAM Projects
Plan de Proyecto	Es un documento que describe a un proyecto, generalmente incluye un resumen general, un calendario, un plan de recursos, un plan de comunicación y un plan de calidad.	Introduction to Project Management for IAM Projects
Clave Pública	Es una clave puesta a disposición públicamente por una entidad. Está asociada a una clave privada que la	Practical Implications of Public Key Infrastructure for Identity Professionals

	entidad controla de forma exclusiva y privada.	
Certificado de Clave Pública	Es un certificado que contiene una clave pública, uno o más identificadores del propietario de la clave privada, un identificador de la Autoridad de Certificación y metadatos adicionales para apoyar a los requisitos de seguridad.	Practical Implications of Public Key Infrastructure for Identity Professionals
Infraestructura de Clave Pública	Es un conjunto de herramientas, estándares y políticas relacionadas, diseñado para la administración de la confianza basada en pares de claves públicas y privadas, y de los certificados.	Practical Implications of Public Key Infrastructure for Identity Professionals
Recurso Protegido	Es un sistema, proceso, servicio, objeto de información o incluso una ubicación física que está sujeta al control de acceso en función de cómo esté delimitada por el propietario del recurso y por otras partes interesadas como pueden serlo los propietarios de procesos de negocio o los gestores de riesgos.	Introduction to Access Control
Conciliación	Es el proceso de identificar y procesar los cambios en los usuarios y en los accesos del usuario hechos directamente en los sistemas objetivo.	User Provisioning in the Enterprise
Autoridades de Registro (RA, por sus siglas en inglés)	Es un individuo, sistema o función de negocio que provee el registro y la comprobación de identidad para las entidades a las que se otorgan certificados y que también administra la emisión y la renovación de certificados. Las responsabilidades más importantes	Practical Implications of Public Key Infrastructure for Identity Professionals

	de una RA incluyen la demostración de identidad y la asociación de la clave privada a la identidad.	
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.	IAM Reference Architecture
Recurso u Objeto	Es un valor protegido por los controles de acceso, como una aplicación, un sistema o puerta.	Introduction to Identity - Part 1: Admin-time (v2)
Revocar	La Revocación es el anuncio de que un determinado certificado individual ya no es confiable para el cliente.	Practical Implications of Public Key Infrastructure for Identity Professionals
Directiva de Servicios de Pago (PSD2)	La Directiva de Servicios de Pago (PSD2) (Directiva de Servicios de Pago revisada, Directiva (UE) 2015/2366) es una directiva de la Unión Europea (UE) administrada por la Dirección General de Mercado Interno de la Comisión	Designing MFA for Humans

	Europea, que regula los pagos de servicios y los proveedores de pagos de servicios a lo largo de la Unión Europea y del Espacio Económico Europeo (EEE). Contiene muchos requisitos específicamente relacionados con la Autenticación Reforzada de Clientes.	
Contexto de Riesgos (RCTX)	El Contexto de Riesgos es la información adicional que pueda ser aportada para ayudar a mejorar la seguridad general del ecosistema. Los eventos internos o externos y datos se pueden usar para habilitar, limitar o terminar el acceso. Este término es similar a la sección de Monitores y Sensores de los Sistemas de Gobernanza FICAM así como a varias de las entradas del Punto de Decisión de Políticas en la Publicación Especial 800-207 de NIST, un documento sobre Confianza Cero (*Zero Trust*).	IAM Reference Architecture
Administración de Roles	Es una manera de agrupar las reglas de acceso para hacerlas más manejables.	Introduction to Identity - Part 1: Admin-time (v2)
Control de Acceso basado en Roles (RBAC, por sus siglas en inglés)	Es el objetivo que tienen los roles durante el tiempo de ejecución; es una manera de controlar quién tiene acceso a qué en función de los roles de los usuarios dentro de la organización.	Introduction to Identity - Part 1: Admin-time (v2)
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	Introduction to Policy-Based Access Controls (v2), Authentication and Authorization

	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.	
Rol	Es un conjunto de permisos. Un rol debe estar asociado a un usuario individual que adquiere las autorizaciones asociadas al rol.	Practical Implications of Public Key Infrastructure for Identity Professionals
RSA	Es un sistema criptográfico asimétrico basado en grandes números primos. El acrónimo RSA proviene de las iniciales de sus tres inventores principales: Ron Rivest, Adi Shamir y Len Adleman.	Practical Implications of Public Key Infrastructure for Identity Professionals
S/MIME	Es un estándar para crear y enviar mensajes firmados digitalmente o encriptados usando criptografía asimétrica.	Practical Implications of Public Key Infrastructure for Identity Professionals
Calendario	Es un documento que define las actividades y los recursos necesarios para realizar las entregas y los resultados planificados.	Introduction to Project Management for IAM Projects
Secure Socket Layer (SSL) / Capa de puertos seguros	Un estándar obsoleto para encriptar datos en tránsito; el TLS lo reemplazó.	Practical Implications of Public Key Infrastructure for Identity Professionals
Lenguaje de Marcado para Confirmaciones de Seguridad (SAML)	SAML es un protocolo de comunicación basado en XML entre los Proveedores de Servicios (SP, por sus siglas en inglés) y los	Federation Simplified (v2)

	Proveedores de Identidades (IdP, por sus siglas en inglés). En general, la empresa aloja el IdP mientras que las aplicaciones (incluyendo servicios en la nube) son los SP.	
Segmento	Es una agrupación de sujetos que puede ser útil para autorizaciones, como empleados de tiempo completo, estudiantes de grado, administradores de TI o clínicos.	Introduction to Policy-Based Access Controls (v2)
Identidad Auto-Soberana	Es un movimiento digital fundado en el principio de que todo individuo debe poseer y controlar su identidad sin la intervención de autoridades administrativas.	A Peek into the Future of Decentralized Identity
Cuenta de Servidor	Es una cuenta que tiene permisos de acceso privilegiado a las operaciones de un servidor. Normalmente es usada con fines de configuración del servidor.	Non-Human Account Management (v2)
Protocolo de Validación de Certificados basado en Servidor (SCVP, por sus siglas en inglés)	Es un protocolo que habilita a un cliente a explorar un servidor con el fin de determinar si un certificado es válido y confiable. El servidor no debe estar necesariamente asociado con la Autoridad de Certificación (CA) emisora. SCBP hace dos cosas: (1) determina la ruta entre la entidad final y el certificado de raíz con lo cual el cliente no necesita confiar en ninguna CA intermediaria. (2) realiza validaciones de ruta delegadas, en acuerdo con las políticas.	Practical Implications of Public Key Infrastructure for Identity Professionals
Cuenta de Servicio	Es una cuenta utilizada por una aplicación informática para acceder a otras aplicaciones o servicios con un objetivo específico.	Non-Human Account Management (v2)

Proveedor de Servicios (SP, por sus siglas en inglés)	Según la definición de la organización OASIS que es la responsable de las especificaciones SAML, es un “rol otorgado por una entidad del sistema donde la entidad del sistema provee servicios a entidades principales u otras entidades del sistema”. En general es una aplicación que ofrece servicios a usuarios que requieren autenticación y autorización.	Federation Simplified (v2)
Sesión	El período de tiempo que se inicia luego de un evento de autenticación, cuando un tercero confiable (RP, por sus siglas en inglés) otorga acceso a recursos para el sujeto o entidad principal. La duración de la sesión y los mecanismos para su ejecución varían según la implementación.	IAM Reference Architecture
Administración de Sesiones	Una función de administración provista por un Proveedor de Identidades (IdP, por sus siglas en inglés) para controlar las sesiones de terceros confiables (RP, por sus siglas en inglés) suscritos.	IAM Reference Architecture
Autorización Compartida	La autorización compartida es provista por servicios por fuera del tercero confiable (RP, por sus siglas en inglés). En este glosario, lo tomamos como parte del conjunto de recursos de la administración de accesos.	IAM Reference Architecture
Firma	Es el procesamiento de datos utilizando un algoritmo criptográfico para proveer garantía de integridad.	Practical Implications of Public Key Infrastructure for Identity Professionals
Inicio de Sesión	Un Inicio de Sesión Único es un	Federation Simplified (v2)

Único (SSO, por sus siglas en inglés)	servicio que habilita a un Proveedor de Servicios (SP, por sus siglas en inglés) a verificar identidades de usuarios finales, facilitando la comunicación con los Proveedores de Identidades (IdP, por sus siglas en inglés). SSO hace de puente para deslindar los SP y los IdP. Esto se puede hacer a través de varios protocolos como la integración basada en agente, integración directa LDAP, SAML u OpenID Connect, por mencionar algunos.	
Ingeniería Social	La Ingeniería Social es un método de manipulación de las personas para que divulguen información confidencial, como contraseñas e información bancaria, u otorguen acceso a sus computadoras para instalar secretamente software malicioso.	Account Recovery (v2), Designing MFA for Humans
Fuentes de Verdad	El lugar donde residen los datos fidedignos de los individuos.	Introduction to Identity - Part 1: Admin-time (v2)
Categorías Especiales de Datos (SCD, por sus siglas en inglés)	Son categorías de datos que son considerados especialmente sensibles, es decir que están sujetos a regulaciones adicionales. De acuerdo con la definición del Artículo 9(1) del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) se trata de “datos personales que revelen información racial o étnica, opiniones políticas, creencias políticas o filosóficas, afiliación sindical, información genética o médica, datos biométricos que identifiquen a la persona natural, información sobre la orientación o vida sexual de la persona.” Los	An Introduction to the GDPR

	"datos personales relacionados con condenas y delitos penales" referidos en el Artículo 10 también requieren un trato similar así que en general son considerados como una categoría más de SCD.	
Autenticación Incremental	Es un método para incrementar el nivel de seguridad (o confianza) que un sistema tiene sobre la autenticación de un usuario, generando uno o más retos de autenticación, normalmente utilizando factores diferentes de los que se usaron para establecer la sesión autenticada inicial. Normalmente, la necesidad de incrementar el nivel de seguridad es disparado por el riesgo asociado con los recursos sensibles que el usuario está intentando acceder.	Designing MFA for Humans
Nombre Alternativo de Sujeto	Son uno o más identificadores de un sujeto de certificado que los emisores pueden usar al transportar identificadores específicos de aplicaciones como una dirección de correo electrónico o Nombre Principal de usuario (UPN, por sus siglas en inglés).	Practical Implications of Public Key Infrastructure for Identity Professionals
Nombre Distinguido del Sujeto (*Subject DN*)	Es un identificador único para el sujeto, delimitado por el alcance de la Autoridad de Certificación. Los emisores diseñan el Nombre Distinguido de Sujeto como un nombre de acceso LDAP.	Practical Implications of Public Key Infrastructure for Identity Professionals
Cuenta de Sistema	Es un término genérico para una cuenta con privilegios que tiene permisos amplios que le permiten realizar cambios en la configuración del sistema.	Non-Human Account Management (v2)

Tarea	Es el nivel más básico de actividad definido; en general, muchas tareas conforman las etapas de las distintas fases del proyecto.	Introduction to Project Management for IAM Projects
Modelado de Amenazas	El Modelado de Amenazas es una técnica de análisis utilizada para ayudar a identificar amenazas, ataques, vulnerabilidades y contraataques que puedan impactar en la aplicación o en el proceso.	Account Recovery (v2), Designing MFA for Humans
Tort (Responsabilidad Civil Extracontractual)	Es el cuerpo de jurisprudencia de situaciones en las que el comportamiento de una persona causa daños, perjuicios, sufrimiento o pérdida injusta a otra persona, otorgando a la persona damnificada el derecho de iniciar una demanda civil con el fin de ser compensada por la persona que causó el daño. Algunos ejemplos de esto son: agresión, fraude, difamación, negligencia y responsabilidad objetiva.	Laws Governing Identity Systems
Seguridad de la Capa de Transporte (TLS, por sus sigals en inglés)	Es un protocolo criptográfico diseñado para proveer confidencialidad e integridad en las comunicaciones entre dos puntos finales (*endpoints*).	Practical Implications of Public Key Infrastructure for Identity Professionals
Federación de confianza	Es un marco de confianza entre múltiples entidades para usar información de identidad y de administración de accesos de manera controlada.	Introduction to Identity – Part 2: Access Management
Marco de Confianza	Es un componente que representa el aparato legal, técnico y organizacional que habilita la confianza entre la IDM	IAM Reference Architecture

	(Administración de Identidades) y los RP (terceros confiables).	
Raíz de confianza	Es una estructura técnica que otorga a los IdP (Proveedores de Identidad) y los terceros confiables (RP, por sus siglas en inglés), la habilidad de reconocerse mutuamente a un nivel alto de seguridad. Es similar al concepto de Ancla de Seguridad (*Trust Anchor* / NIST SP.800-63-3) salvo que nosotros también incluimos en la definición a cualquier estructura que confíe en un tercero en el marco de un mutuo acuerdo. La Raíz de Confianza deriva de la ejecución de un Marco de Confianza.	IAM Reference Architecture
Autenticación de dos Factores (2FA)	Se trata de un tipo específico de autenticación de múltiples factores (vea: IDPro's Consolidated Terminology) en el que dos factores deben ser verificados para validar la identidad de un usuario.	Designing MFA for Humans
Resolutor Universal	Es un resolutor de problemas de identificadores que funciona con cualquier identificador descentralizado (DID, por sus siglas en inglés) a través de los controladores del DID. El objetivo de un resolutor universal es entregar un documento DID con los metadatos DID ante determinado valor DID. Esta función es muy útil ya que los DID pueden ser anclados en una variedad de implementaciones disímiles de infraestructuras descentralizadas de clave pública (dPKI).	A Peek into the Future of Decentralized Identity

Usuario o Sujeto	Una persona o entidad que puede recibir acceso dentro de determinado sistema de control de acceso.	Introduction to Policy-Based Access Controls (v2)
Agente de Usuario	Un agente de usuario es cualquier software que recupere, provea y facilite la interacción entre usuarios finales y el contenido web.	Cloud Service Authenticates Via Delegation – SAML
Aprovisionamiento de Usuarios	Los recursos mediante los cuales se crean, mantienen y desactivan/eliminan las cuentas de usuarios en un sistema de acuerdo con las políticas definidas.	User Provisioning in the Enterprise
Administración de Aprovisionamiento y Ciclo de Vida de Usuarios	Gestión para que los registros de usuarios estén donde se los necesite, pero únicamente cuando sean necesarios.	Introduction to Identity - Part 1: Admin-time (v2)
Nombre de Usuario	El término común usado para un identificador externo.	Identifiers and Usernames
Nombre de Usuario	Es un identificador único del servicio de autenticación que se usa en conjunto con un secreto compartido para autenticar a un usuario.	Account Recovery (v2), Managing Identity in Customer Service Operations
Validador	Es una entidad que verifica un certificado y confirma que la otra parte controla las claves privadas en una operación.	Practical Implications of Public Key Infrastructure for Identity Professionals
Credenciales Verificables	Son atestaciones o confirmaciones que hace un emisor sobre un sujeto. Las credenciales verificables están firmadas digitalmente por el emisor.	A Peek into the Future of Decentralized Identity
Presentaciones Verificables	Conjunto de credenciales verificables, atestaciones autogeneradas o cualquier artefacto	A Peek into the Future of Decentralized Identity

	que se presenta ante los verificadores para ser verificado. Las presentaciones verificables están firmadas digitalmente por el propietario y pueden contener toda la información que un verificador solicita en un solo paquete. Es también donde los propietarios delimitan las condiciones de uso específicas en las que una presentación debe usarse.	
Verificador	Es la entidad que verifica las credenciales verificables para poder proveer servicios a un propietario.	A Peek into the Future of Decentralized Identity
Marco de la Fuerza Laboral	Es un resumen de las categorías de trabajo, roles y modelos de competencia necesarios para ejecutar la planificación de la fuerza laboral.	Identity and Access Management Workforce Planning
Planificación de la Fuerza Laboral	Son las actividades que aseguran que una organización tiene las aptitudes necesarias para llevar a cabo los objetivos técnicos y de negocio.	Identity and Access Management Workforce Planning
X.509	Es un estándar ISO de la serie X.500 que define las reglas básicas para cifrar certificados de clave pública.	Practical Implications of Public Key Infrastructure for Identity Professionals
Eliminación Completa de Privilegios (*Zero Standing Privilege* - ZSP)	Es un estado en el que un Acceso Justo a Tiempo (JIT, por sus siglas en inglés) se utiliza en todos los permisos y en el que ningún permiso duradero es asignado a una entidad principal.	Techniques To Approach Least Privilege
Confianza Cero	De acuerdo con el Borrador de la Publicación Especial NIST 800-207, "La Confianza Cero implica que no hay ninguna confianza garantizada	Introduction to Identity – Part 2: Access Management

	en un recurso o cuenta de usuario basándose únicamente en su ubicación física o de red (por ej. redes locales versus Internet).”	