GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Capítulo 7.

Administración del control de accesos. (2ª Parte)

José Pablo Hernández

¿Qué es la gestión de identidades?

Una identidad electrónica es un conjunto de datos sobre una persona que determina en qué momento y a qué sistemas puede acceder en una organización.

Un sistema de gestión de identidades es la infraestructura técnica y organizativa para la definición, gestión y administración de esas identidades electrónicas.

¿Qué es la gestión de identidades?

Una estrategia que permita llevar a buen término una gestión eficaz de identidades, adecuada a las necesidades de cada organización, conduce al logro de objetivos fundamentales:

- Ahorro de costes
- Garantía de calidad de los servicios
- Incremento de la seguridad
- Cumplimiento de las normativas

Gestión de identidades. Regulaciones.

Muchas instituciones nacionales e internacionales están demandando que las organizaciones que almacenan datos sobre las identidades cumplan con unas normas estrictas.

Ejemplo de estas normas es la directiva europea sobre protección de datos, el acta de protección de datos del Reino Unido, el acta canadiense de acceso a la información y las estadounidenses regulaciones HIPAA y COPPA.

Gestión de identidades. Regulaciones.

Muchas instituciones nacionales e internacionales están demandando que las organizaciones que almacenan datos sobre las identidades cumplan con unas normas estrictas.

Ejemplo de estas normas es la directiva europea sobre protección de datos, el acta de protección de datos del Reino Unido, el acta canadiense de acceso a la información y las estadounidenses regulaciones HIPAA y COPPA.

Este tipo de regulaciones son muy exigentes, y hacerlo mal no es una opción que pueda tener la empresa.

Gestión de identidades. Regulaciones.

En el caso español la aplicación de la directiva europea se ve reforzada con la legislación propia en materia de protección de datos de carácter personal (LOPD) y la denominada LSSI, que regula las transacciones electrónicas en Internet, entre otras materias.

La normativa nacional implica desde repercusiones económicas hasta penales, por lo que la seguridad de los datos sobre identidades se tercia más crucial si cabe, para cualquier actividad.

Gestión de identidades y accesos. IAM.

El término "gestión de identidades y acceso" (IAM), es un término que se aplica a distintas áreas relacionadas con la identidad de las personas en las organizaciones.

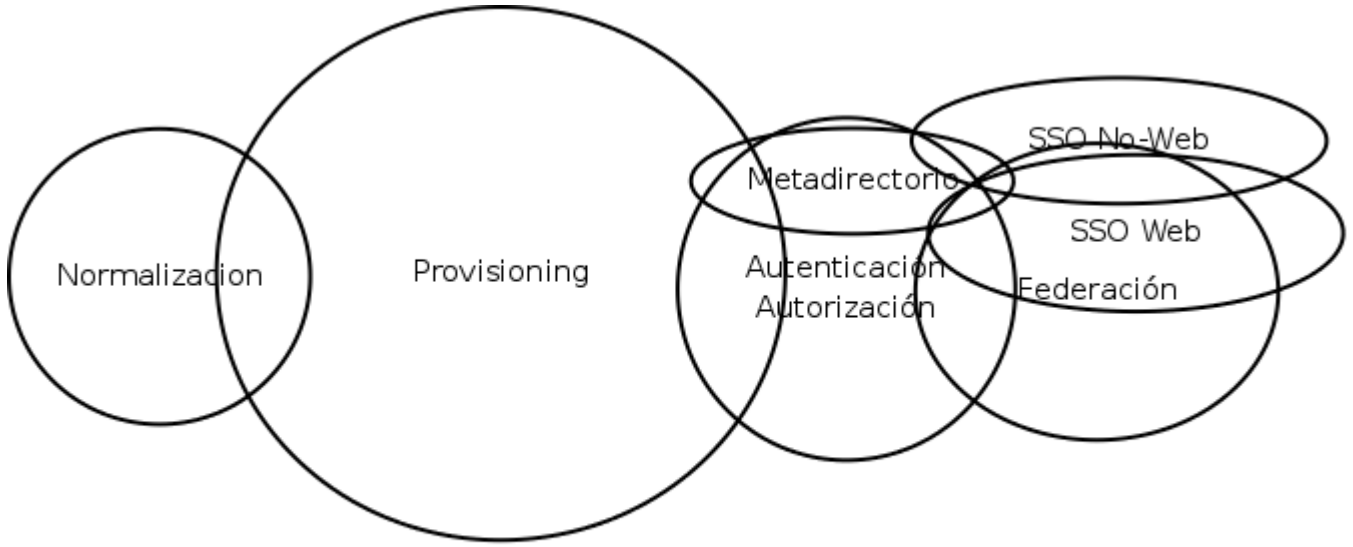
En orden a poder hablar con los distintos interlocutores, es necesario establecer un escenario común, por lo que resulta imprescindible establecer cada una de las áreas que de por si, o en conjuntos, suelen ser referidas como "gestión de identidades".

Por ello es muy importante que al inicio de un estudio de "gestión de identidades" se identifiquen aquellas áreas que los interlocutores consideran su marco de referencia para la gestión de identidades".

Gestión de identidades y accesos. IAM.

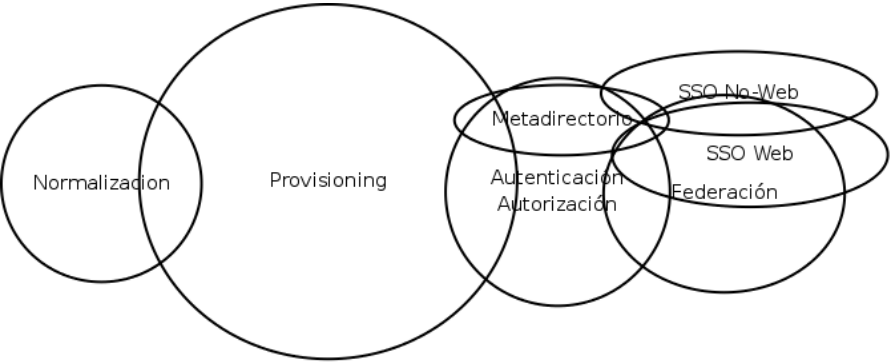
Un sistema de gestión de identidades puede estar focalizado a una, varias o todas las siguientes áreas de la gestión de identidad.

A continuación se muestra un diagrama de ámbito, en la que aparecen cada una de esas áreas y como se interrelacionan entre si:



GESTIÓN DE IDENTIDADES: ÁREAS

Gestión de identidades y accesos. IAM.



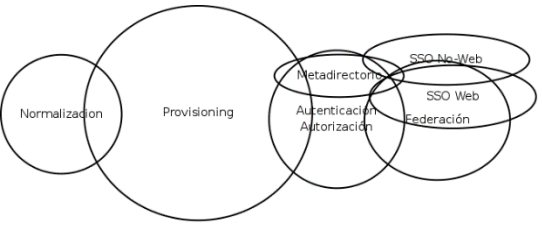
GESTIÓN DE IDENTIDADES: ÁREAS

Dichos procesos comienzan con un proceso de normalización de los repositorios de identidad de la organización que concluye con una carga de datos en el sistema de provisioning.

Este a continuación nutre de datos a los distintos repositorios con información normalizada (incluyendo en muchas ocasiones un nuevo repositorio de identidad global denominado meta-directorio), que a su vez son utilizados por los servicios para autenticar y autorizar a los usuarios.

Además en sistemas más complejos se suele trabajar en la inclusión mecanismos de SSO y federación utilizando los repositorios de identidad para la función de autenticación.

Gestión de identidades y accesos. IAM.



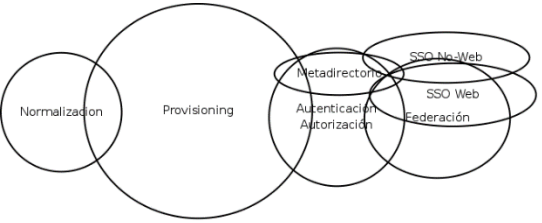
GESTIÓN DE IDENTIDADES: ÁREAS

Normalización. Los sistemas de "gestión de identidades" son una necesidad de aquellas organizaciones en las que debido a su crecimiento, el número de repositorios de identidad, usuarios y/o servicios ha alcanzado un tamaño lo suficientemente grande como para que sea complicado continuar cumpliendo con las reglas de negocio, enfocadas a la identidad, de la organización sin dedicar excesivas cantidades de recursos a ello.

El área de la normalización de la información implica el estudio de los sistemas de identidad existentes, la puesta en marcha de criterios para unificar la utilización de los mismos, y el preparar los datos para que estos puedan ser cargados en un sistema de "provisioning" futuro.

Es importante destacar la diferencia entre el área de normalización y el de provisioning, mientras los procesos de normalización van a enfocados a organizar la información de identidad de una organización, previo a su integración en un sistema de gestión de identidad, los procesos implementados en el área de provisioning, van enfocados a implementar las reglas de negocio de la organización enfocadas a la identidad.

Gestión de identidades y accesos. IAM.



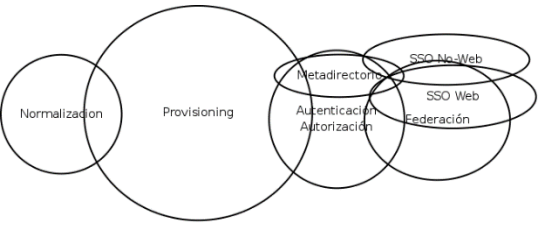
GESTIÓN DE IDENTIDADES: ÁREAS

Provisioning. El área de provisioning está enfocado a implementar las reglas de negocio en los procesos de provisión de usuarios, de las organizaciones.

Como se ha destacado en el apartado anterior, el objeto de este área son las propias reglas de negocio, no el reordenar la información, que previamente a implantar un sistema de gestión de identidades, se encontraba "desordenada".

En dicha área se tratan procedimientos, como la creación/borrado/modificación de usuarios en la organización, la propagación de los datos de identidad a los distintos repositorios en función del tipo de usuario, la captura de datos de identidad desde distintos repositorios, tareas en el tiempo (como políticas de cambio de contraseñas, expiraciones), e interfaces gráficos de gestión de los datos.

Gestión de identidades y accesos. IAM.



GESTIÓN DE IDENTIDADES: ÁREAS

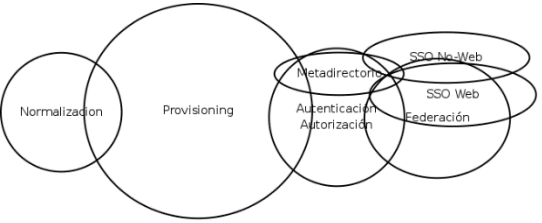
Metadirectorio. En las organizaciones generalmente se disponen de diversos repositorios de identidad.

De modo que el listado completo de usuarios y los datos completos de identidad de los usuarios de la organización se encuentran repartidos, encontrándose parte de ellos en cada uno de los repositorios.

Además durante la implantación de los sistemas de gestión de identidades, suelen aparecer nuevos campos de identidad en la organización que hasta ese momento no existían, y que se utilizan generalmente para categorizar los datos de identidad de los usuarios.

El servicio de meta-directorio, viene a plasmar en un directorio de identidad un volcado de todos los usuarios de la organización, con un conjunto grande de datos que actualmente se encuentran divididos en diversos repositorios, y algunos de esos nuevos datos utilizados para gestionar la identidad, de modo que puedan ser utilizados por futuros servicios en la organización.

Gestión de identidades y accesos. IAM.



GESTIÓN DE IDENTIDADES: ÁREAS

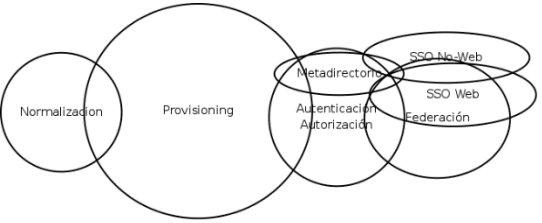
Autenticación/Autorización. El área de autenticación/autorización, es el apartado que se encarga de autenticar/autorizar a los diversos usuarios en los diferentes servicios de la organización.

En realidad dependiendo de la organización no suele implicar cambios adicionales en los sistemas/servicios de la organización, sino que viene dado como producto del área de provisioning.

Eso sí, algunas veces es necesaria la modificación en la configuración de los servicios para realizar un ajuste completo con las reglas de negocio de la organización.

En otros casos, en este área se trabaja en la implementación de APIs, que generalmente funcionan utilizando como backend de identidad el servicio de meta-directorio, que permiten autenticar/autorizar a los usuarios.

Gestión de identidades y accesos. IAM.

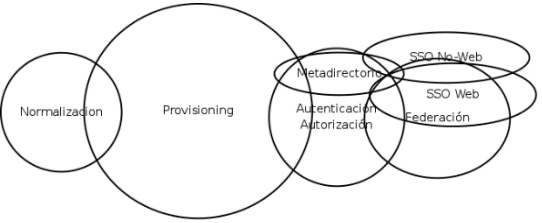


GESTIÓN DE IDENTIDADES: ÁREAS

SSO. El "Single Sign On", es el siguiente área a tratar tras la autenticación/autorización, trata de que dichos procesos se realicen de modo que una vez que un usuario se ha autenticado en uno de los servicios, no sea necesario volver a autenticar a dicho usuario en otros servicios de la organización, ya que el primer servicio envía una credencial al usuario, que el usuario utiliza para demostrar en el resto de los servicios cual es su identidad.

Los servicios de SSO, se dividen en dos tipos, por una parte los servicios Web/Desarrollo, y por otra parte los servicios basados en servicios de sistemas, como pueden ser un servidor de correo, un servidor ftp, el acceso a un terminal Windows/Linux ...

Gestión de identidades y accesos. IAM.



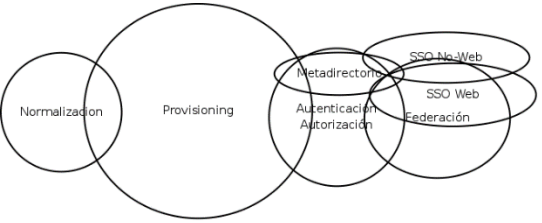
GESTIÓN DE IDENTIDADES: ÁREAS

Gestión de contraseñas. La sincronización de contraseñas evita los inconvenientes que sufren los usuarios que deben acceder a diferentes sistemas con múltiples cuentas y contraseñas.

De esta manera, los usuarios deben de cambiar su contraseña únicamente en uno de los sistemas.

Un sistema de autoreseteo de la contraseña evita, además, la gran cantidad de llamadas que se reciben en el help-desk de forma habitual, así como los tiempos de espera del usuario afectado.

Gestión de identidades y accesos. IAM.



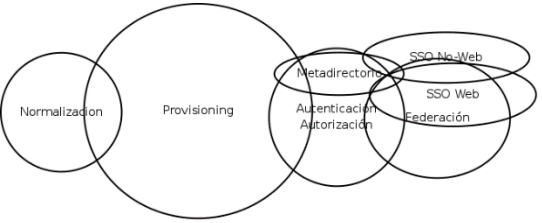
GESTIÓN DE IDENTIDADES: ÁREAS

SSO Web/Desarrollos. En los servicios tipo web/desarrollo el acceso al SSO se realiza mediante el uso de APIs, o de ampliaciones de funcionalidad en los servidores Web/Aplicaciones.

Generalmente los nuevos desarrollos se realizan incluyendo llamadas a un API de un servicio de autenticación/autorización, o utilizan una cookie que permite identificar y autorizar a un usuario.

Existen múltiples soluciones que proporcionan dicha funcionalidad, comenzando por soluciones propietarias como Sun Access Manager, y soluciones libres como Shibboleth, OpenSSO (también de Sun) o PAPI (solución desarrollada en España por Rediris).

Gestión de identidades y accesos. IAM.



GESTIÓN DE IDENTIDADES: ÁREAS

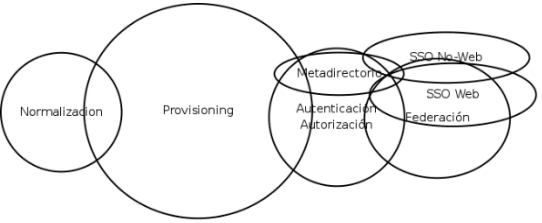
SSO Sistemas. Otro tipo de servicios son aquellos basados en servidores de sistemas, como puede ser el acceso a un servicio de correo, el acceso a un terminal de trabajo, o a un servidor de ficheros.

Para la integración de dichos servicios generalmente se utiliza "Kerberos" u otros servicios que están basados finalmente en el uso de esa misma tecnología como “Spnego”.

Dichas soluciones permite la implementación de SSO mediante el uso de credenciales, aunque no están muy extendidas, y suelen tener costes realmente altos de implantación al ser específicas de cada escenario.

Además existe una amplia variedad de software propietario en esta sección.

Gestión de identidades y accesos. IAM.



GESTIÓN DE IDENTIDADES: ÁREAS

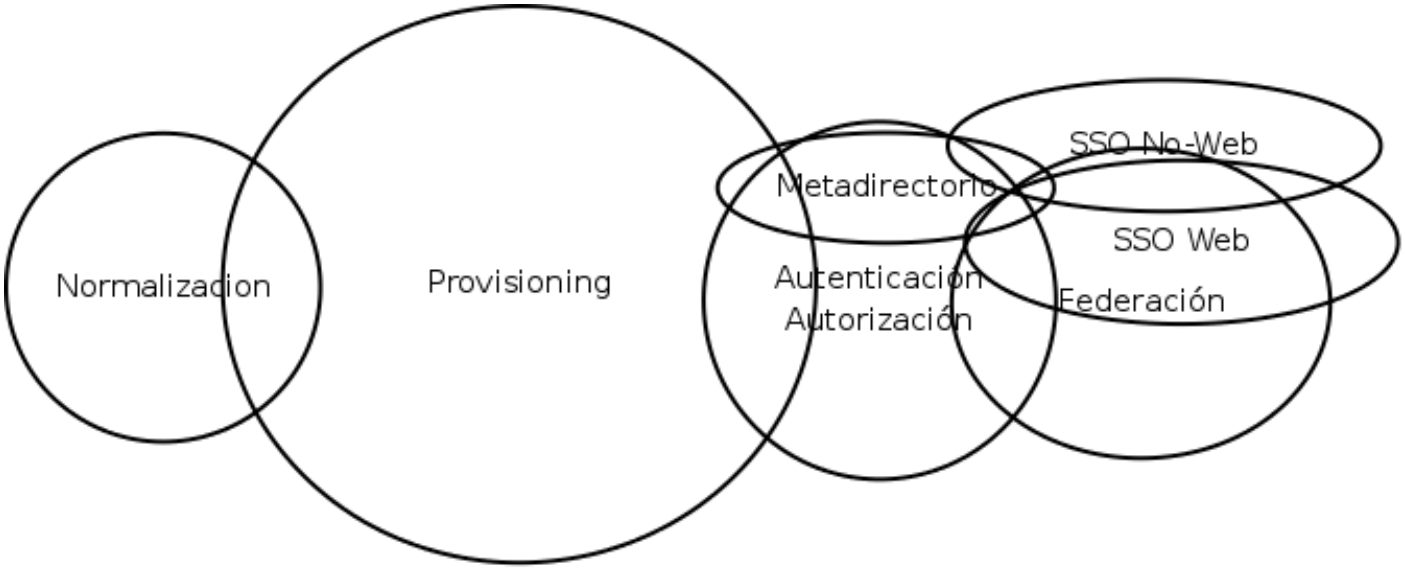
Federación. Un paso más allá de la autenticación/autorización y el SSO está la federación.

La federación es el área que trabaja los mecanismos para el intercambio de identidades entre diferentes organizaciones.

Para el intercambio de dicha información los diferente productos que hay en el mercado se basan en los protocolos Liberty Alliance Project y S.A.M.L.

Gestión de identidades y accesos. IAM.

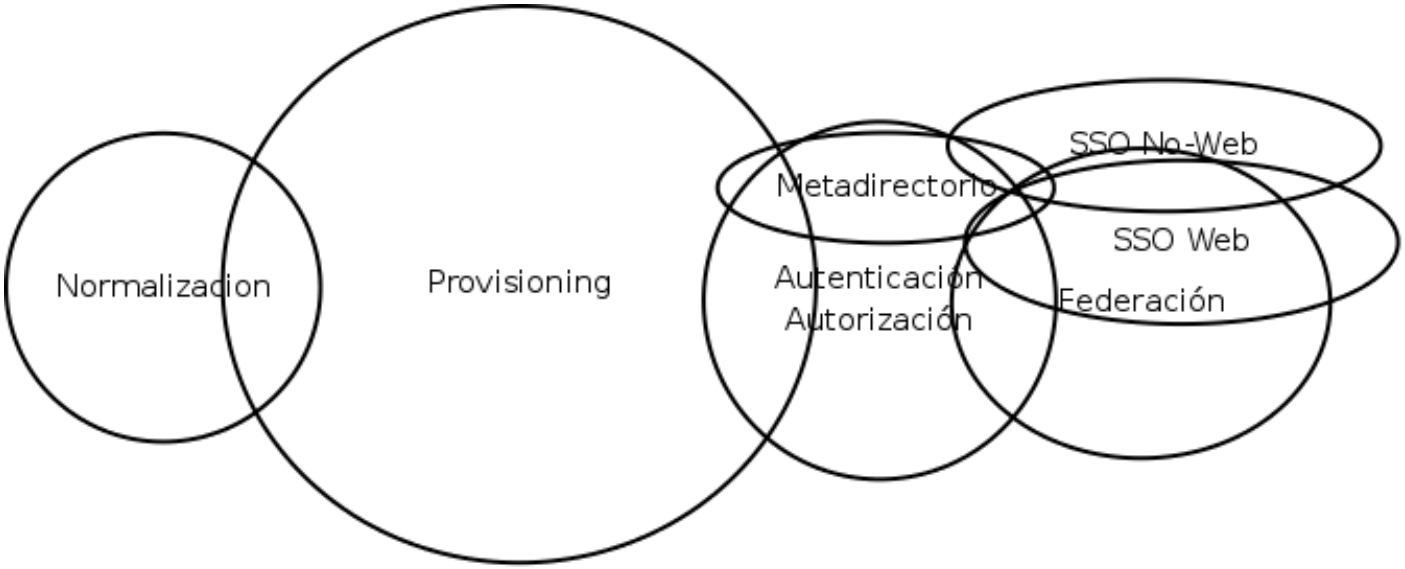
Mientras en el ámbito de la gestión de identidad se suele hacer referencia a todas estas áreas, sólo en contadas ocasiones se suelen encontrar sistemas de gestión de identidad implantados que cubren la totalidad de las mismas.



GESTIÓN DE IDENTIDADES: ÁREAS

Gestión de identidades y accesos. IAM.

Mientras en el ámbito de la gestión de identidad se suele hacer referencia a todas estas áreas, sólo en contadas ocasiones se suelen encontrar sistemas de gestión de identidad implantados que cubren la totalidad de las mismas.



GESTIÓN DE IDENTIDADES: ÁREAS

Gestión de identidades y accesos. Herramientas.

Las funcionalidades anteriores se pueden lograr mediante programas a medida o mediante soluciones de gestión de identidades.

En el mercado hay varios fabricantes que han lanzado diferentes soluciones, algunas de estas son :

- Oracle Identity Management
- Sun Identity Manager
- Microsoft Identity Lifecycle Management
- Novell Identity Manager

Gestión de identidades y accesos. Herramientas.

Aún que cada una de estas soluciones tiene sus particularidades, el funcionamiento básico de estas soluciones está compuesta por un repositorio central en el que se crean y mantienen los objetos y un motor que escucha cualquier cambio que se realice en él , altas , bajas, modificaciones, etc.

Cuando se genera un evento en este repositorio central este es replicado a los sistemas conectados mediante el envío de documentos XML , así como a la inversa , cuando se produce un evento en uno de los sistemas conectados este es replicado hacia el repositorio central y, desde este, hacia todos los sistemas conectados

Gestión de identidades y accesos. Herramientas.

La replicación de cuentas , aún que es una de las partes mas importantes de estas soluciones sólo forma una mínima parte de lo que engloban estas soluciones, entre otras cosas permiten tener interfaces web para que los propios usuarios puedan mantener sus cuentas, requerir la aprobación de uno o varios usuarios para que un objeto de replique (workflows), tener roles etc.

Gestión de identidades y accesos.