Líneas de trabajo grupo GT-Identidad

1.- Análisis de las fuentes de datos. Definición de validaciones y comprobaciones en las mismas.

a) Definición de los métodos de registro de la información (automático, presencial, autoregistro, otros)
b) Validaciones de la autenticidad de la información introducida en el registro.
c) Definición de los métodos de actualización de la información y ciclos de vida.
d) Definición de las comprobaciones realizadas antes de aceptar un dato para asegurar así que la información almacenada sea fiable.
e) Definición de comprobaciones y mecanismos de control a realizar para evitar usuarios duplicados.
f) Especificar con que aplicativos comparte información, detallando datos y frecuencia de actualización de los mismos.
g) Definición de las posibilidades de retroalimentación para poder corregir de esta forma errores detectados en el sistema que gestiona la identidad.

2.- Servicios ofrecidos a las aplicaciones.

a) Descripción de las propias aplicaciones: título, URL, breve descripción.
b) Definición de los datos de usuarios que consume.
c) Especificar si esta integrado en el SSO institucional o describir el Método de autenticación que utiliza.
d) Autorización: Detallar que usuarios lo utilizan, que perfiles existen y como se determinan, indicando cuándo y cómo se concede la autorización así como cuando y como se revoca.
e) Definición del procedimiento de integración de aplicaciones **en el SSO**.
f) Definición de posibles amenazas y nivel de riesgo de accesos no autorizados.

3.- Definición de tipos de usuarios de la institución y roles.

a) Definición de los tipos y subtipos de usuarios: PDI, PAS, ESTUDIANTES, Cuentas institucionales, Invitados, Otros (Socios de antiguos alumnos, personal de la fundación o de otros

institutos o servicios vinculados a la universidad, ...) Informe de número de usuarios por tipos/subtipos.
b) Definición de los ciclos de vida por colectivo.
c) Composición de una matriz de compatibilidades entre tipos de usuarios.
d) Definición de la procedencia de los tipos de usuarios.
e) Matriz de tipo de usuarios y Servicios ofrecidos
f) Solapamiento de tipos → prioridades
g) Definición de los procedimientos de deshabilitación, borrado de usuarios y roles caducados.

4.- Definición del flujo de la información y sincronización de datos entre repositorios.

a) Diseño de como fluye la información entre los distintos repositorios. Gráfico explicativo.
b) Descripción rigurosa de como se sincroniza la información (si va en un solo sentido, si los errores detectados en un punto se reportan y corrigen hacia atrás o no).
c) Definición de reglas de detección de usuarios duplicados.

5.- Directorio.

a) Información básica de un usuario: decidir la selección de atributos mínimos para gestionar la identidad de los usuarios que dependerá en gran medida de los puntos anteriores.
b) Seguridad en el directorio, Nivel de Hqdir.
c) Definición del proceso de emisión de credenciales. Como se generan y como se entregan al usuario por primera vez.
d) Definición de la gestión de recuperación de contraseñas en caso de olvido.
e) Definición de la política de contraseñas de la institución.
f) Definición del proceso de gestión de logins fallidos y bloqueo de usuarios.

6.- Servidores de atributos.

a) Documentación de webservices: acceso, datos que facilitan, a quién?, …
b) Definición del directorio virtual en caso de uso. Qué datos almacena, cómo lo hace, cómo se accede, …

6.- Normalización de la Información → Interoperabilidad.

a) Hacer uso de la normativa sobre normalización de almacenamiento de la información fundamental: DocID nombres y apellidos, fechas, Países, ciudades, pueblos, (Codificados todos ellos de modo estándar?) ampliable a Áreas, departamentos, facultades... carreras.. títulos... Existe ya algún catálogo elaborado por ENI de localidades, países, Unidades Orgánicas de las Universidades... etc que deberíamos empezar a manejar.

7.- Autenticación.

a) Si se dispone de SSO, esquema claro de cuantas aplicaciones están integradas.
b) Definición de los métodos de autenticación disponibles: user/passwd, eDNI, certificados, stork..
c) Definición de las posibles debilidades y vulnerabilidades.
d) Definición de las medidas de seguridad establecidas y en proceso de establecer.

8.- Autorización y Administración de Acceso: qué usuarios tienen acceso a qué recursos en cada momento, basado en políticas cambiantes.

a) Basadas en atributos.
b) Basadas en pertenencia a grupos.
c) Gestión de excepciones de manera independiente según requerimientos específicos.
d) Dónde se realiza la autorización?: centralizada en el SSO, o es cada administrador de cada servicio el responsable de manejar su política de autorizaciones, o se basa en roles(modelo RBAC- Rol-Based access control, una gestión basada en roles permite no asignar derechos a personas sino a funciones) Descentralizar complica la gestión integral, por ejemplo sería imposible o complicado crear un panel de servicios personalizado para un usuario autenticado.

9.- Auditorías.

a) Definición de las auditorías de datos.
b) Programación en el tiempo de las mismas.
c) Análisis de anomalías detectadas

d) Gestión de logs y estadísticas de uso

10.- Conformidad legal. Privacidad Seguridad e Interoperabilidad.

a) Gestión de la privacidad de los datos de los usuarios. LOPD, Derechos ARCO, se respetan?.
b) Medidas de seguridad implementadas en el acceso a los repositorios.
c) cumple el ENS?
d) Y el ENI?

11.- Interfaz de usuario final para visualizar y manejar datos de usuarios.

a) Mostrar datos al usuario final (sus propios datos). Permite detectar errores.
b) Posibilidad de modificar algunos datos puesto que el directorio también es fuente de datos.
c) Cambio de clave de usuario. Definir un lugar único desde donde se puede cambiar la clave.
d) Posibilidad de definir preguntas para facilitar recuperar claves olvidadas.

12.- Interfaz de administración de la Gestión de la Identidad.

a) Altas manuales
b) Bajas manuales
c) Modificaciones manuales
d) A/B/M por lotes
e) Informes
f) Auditorías de usuarios
g) Administraciones delegadas