Introducción.

Desde los inicios de la informática ha existido siempre la necesidad de proteger recursos de manos inadecuadas.

Hablamos de autenticación cuando nos referimos a la acción de validar a un usuario para permitirle acceder a dichos recursos.

En el caso que tratamos en ese proyecto, partimos de la siguiente situación. Tenemos un centro de cálculo que provee de diversos servicios a un grupo de usuarios, los cuales deben ser autenticados para poder acceder al servicio solicitado en cuestión.

Aunque existen distintas formas de realizar la autenticación, se utilizará una de las más simples; la autenticación mediante clave secreta.

En la situación inicial tenemos una serie de servicios, como son el acceso a internet y a bases de datos, correo y otros, en los que se utilizan la clave secreta. Para este uso necesitamos almacenar un par usuario – clave, que permitiría a los usuarios registrados, aquellos que poseean dicho par, acceder a estos servicios. Cuando se pretende dar acceso a estos usuarios se debe registrar a cada usuario en cada servicio, y elegir una clave, que perfectamente puede ser distinta en cada uno de ellos.

Conforme crecen el número de servicios y de usuarios, la administración de este sistema se vuelve cada vez más complicada. Incluso al usuario no le resulta nada sencillo tener que manejar diferentes claves en lugar de una sola.

En este proyecto pretendemos centralizar la información necesaria para llevar a cabo la autenticación: nombre de usuario, clave y otros campos que permitirán cierta gestión sobre estos datos. De este modo, integrada la autenticación, los servicios recurrirán a un repositorio central para comprobar la validez de las

claves. El repositorio será gestionado por un servidor, que será contra el que se autentiquen los servicios, en lugar de usar ficheros del sistema operativo o bases de datos propias.

Nuestro repositorio centralizado será un directorio OpenLDAP, que por sus características será el más adecuado para esta finalidad. Además como ya hemos mencionado antes, podremos almacenar otro tipo de información del usuario, que nos permitirá disponer de ciertos perfiles, y efectuar así algún tipo de personalización en los servicios.

Uno de los puntos importantes que se tendrán en cuenta es la cuestión de la seguridad. En un entorno intrínsecamente inseguro, una red local ethernet, la información sensible puede ser capturada y por tanto, puede ser usada malintencionadamente.

Esta información "sensible" se compone de nombres de usuarios, contraseñas, datos personales, correos electrónicos, etc, que debe ser protegida. Vamos a considerar, al menos, cifrar los nombres de usuario y contraseñas. Este será el mínimo de seguridad exigido.