# Administración del control de accesos adecuados de los sistemas de información

IFCT0109 – Seguridad informática

MF0490_3 (90 horas)

# Selección del sistema de registro en función de los requerimientos de la organización

- Introducción
- Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos
- Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos
- Requerimientos legales en referencia al control de accesos y asignación de privilegios
- Perfiles de acceso en relación con los roles funcionales del personal de la organización
- Herramientas de directorio activo y servidores LDAP en general
- Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)
- Herramientas de sistemas de punto único de autenticación:
- Single Sign On (SSO)
- Resumen

# Introducción

En el ámbito de los servicios en el sistema informático, la seguridad es un aspecto crucial que no debe ser subestimado. Un sistema informático vulnerable puede comprometer la integridad y confidencialidad de los datos que alberga, lo que puede derivar en serios problemas legales y generar daños significativos y costos elevados para las organizaciones.

Por esta razón, es esencial que las organizaciones implementen políticas de seguridad robustas que prevengan el uso indebido de los recursos y mitiguen cualquier tipo de incidente que pueda surgir debido a la falta de protección del sistema. Una medida de seguridad fundamental es el control de accesos. Al definir su política de seguridad, las organizaciones deben diseñar un sistema de control de accesos que garantice que cada usuario tenga acceso únicamente a los archivos necesarios para el desempeño de sus funciones y que las acciones que puedan realizar con dichos archivos sean estrictamente limitadas.

En este contexto, se describirán los principios fundamentales del control de accesos, junto con los requisitos legales pertinentes y, de manera práctica, las diversas herramientas y sistemas disponibles para gestionar los permisos y controles de acceso de los usuarios.

# Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos

## Requisitos de negocio para el control de accesos

Los principales requerimientos de acceso a los sistemas de información y recursos compartidos están recogidos en la normativa ISO/IEC 27002:2013. El apartado 9 de esta normativa se enfoca específicamente en el control de accesos, el cual se examinará a continuación.

Según la normativa ISO/IEC 27002:2013, la principal finalidad del control de accesos en una organización es regular el acceso a la información, tanto externo como interno. Este control es esencial para proteger la información, los medios de procesamiento y los procesos comerciales, basándose en los requerimientos comerciales y de seguridad. La normativa recomienda establecer una política de control de accesos adecuada y documentada, además de su revisión periódica.

Esta política debe definir las reglas de control de acceso y los derechos de cada usuario o grupo de usuarios. Los controles deben ser tanto lógicos como físicos y deben considerarse conjuntamente. Es crucial proporcionar a los usuarios y proveedores un enunciado claro de los requerimientos comerciales que deben cumplir los controles de acceso.

# Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos

## Requisitos de negocio para el control de accesos

**Al definir una política de control de accesos, se deben tener en cuenta los siguientes elementos:**

- Requerimientos de seguridad de las aplicaciones comerciales individuales.
- Identificación de toda la información relacionada con las aplicaciones comerciales y los riesgos que enfrenta la información.
- Políticas para la divulgación y autorización de la información.
- Consistencia entre el control de accesos y las políticas de clasificación de la información de los diferentes sistemas y redes.
- Legislación relevante y cualquier obligación contractual relacionada con la protección del acceso a los datos o servicios.
- Perfiles de acceso de usuario estándar para puestos de trabajo comunes en la organización.
- Gestión de los derechos de acceso en un ambiente distribuido y en red que reconoce todos los tipos de conexiones disponibles.
- Segregación de los roles del control de accesos.
- Requerimientos para la autorización formal de las solicitudes de acceso.
- Requerimientos para la revisión periódica de los controles de acceso.
- Revocación de los derechos de acceso.

# Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos

## Requisitos de negocio para el control de accesos

**Además, es necesario establecer una serie de parámetros al especificar los controles de acceso:**

- La diferenciación entre las reglas de cumplimiento obligatorio y las directrices de cumplimiento recomendado, pero opcional.
- Establecimiento de reglas basadas en la premisa: "Generalmente todo está prohibido a no ser que esté expresamente permitido" en lugar de "Generalmente todo está permitido salvo que esté expresamente prohibido".
- Cambios en los procesos de identificación de la información que se inician automáticamente mediante medios de tratamiento de la información o manualmente por un administrador.
- Cambios en los permisos de usuarios que se inician automáticamente por el sistema de información o manualmente por el administrador.
- Reglas que requieren la aprobación específica antes de promulgarse y aquellas que no la requieren.

# Análisis de los requerimientos de acceso de los distintos sistemas de información y recursos compartidos

## Requisitos de negocio para el control de accesos

**Otros puntos importantes sobre el control de accesos en ISO 27002:2013**

El apartado 9.1 de la normativa ISO/IEC 27002:2013 especifica concretamente los requerimientos sobre el control de accesos que deben considerar las organizaciones al establecer su política de seguridad. Además, hay otros puntos importantes a tener en cuenta al definir una política de control de accesos:

**Gestión de acceso del usuario**:

- Establecer procedimientos formales para el alta y baja de usuarios, asignación y revocación de derechos de acceso, y gestión de información de autenticación.
- Revisar periódicamente los derechos de acceso de los usuarios.
- Revocar los derechos de acceso de empleados o terceros desvinculados de su empleo, contrato o acuerdo.

**Responsabilidades del usuario**:

- Los usuarios deben proteger su información de autenticación y seguir las prácticas organizacionales.
- Mantener en secreto las claves de acceso y proteger los equipos desatendidos.
- Adoptar una política de escritorio y pantalla limpios para evitar que las claves de acceso estén expuestas.

**Control de acceso al sistema y a las aplicaciones**:

- Restringir el acceso a la información y funciones del sistema según la política de control de acceso.
- Asegurar que los procedimientos de conexión (log-on) sean seguros.
- Implementar sistemas de gestión de contraseñas interactivos que aseguren la calidad de las contraseñas.
- Restringir y controlar los programas de utilidad que puedan anular los sistemas y controles de aplicación.
- Restringir el acceso al código fuente de los programas.

Además del establecimiento de políticas de control de accesos, es fundamental proteger los recursos compartidos y aislar la información confidencial de la compartida en cada sistema de información.

# Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

## Introducción

Siguiendo con el estudio de la normativa ISO/IEC 27002:2013, esta recoge una serie de principios comúnmente aceptados para ejecutar el control de accesos y para gestionar adecuadamente los distintos tipos de accesos, tanto locales como remotos. En el apartado 9.2 de la ISO/IEC 27002:2013 se enumeran estos principios y buenas prácticas, diferenciando entre:

- Registro del usuario.
- Gestión de privilegios.
- Gestión de contraseñas de usuario.
- Revisión de los derechos de acceso de los usuarios.

El objetivo común de estos principios es asegurar el acceso de los usuarios autorizados, mientras se evita el acceso de los no autorizados a los sistemas de información de la organización, ya sean locales o remotos. Se recomienda establecer una serie de procedimientos formales para controlar la asignación de los derechos de acceso a los distintos sistemas de información.

# Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

## Registro del usuario

En cuanto al registro del usuario, las organizaciones deben establecer un procedimiento formal para el registro y la eliminación del registro de los usuarios, que permita otorgar y revocar el acceso a todos los sistemas de información de la organización. Este procedimiento formal debería incluir los siguientes principios:

- Utilizar identificadores (IDs) de usuario únicos. El uso de identificadores grupales debe limitarse solo por razones comerciales u operacionales, y deben ser aprobados y documentados bajo consenso.
- Comprobar que el usuario dispone de la autorización para el uso del sistema de información. Se recomienda también una aprobación separada de la gerencia para los derechos de acceso.
- Verificar que el nivel de acceso otorgado al usuario sea el adecuado para el propósito marcado y consistente con la política de seguridad definida en la organización.
- Facilitar a los usuarios un documento escrito en el que estén reflejados sus derechos de acceso.
- Requerir a los usuarios su firma en el documento donde se reflejan sus derechos de acceso, para acreditar que entienden los enunciados y sus derechos.
- Asegurar que los proveedores no faciliten el acceso hasta que no se hayan completado todos los procesos de autorización.
- Mantener un registro formal de todas las personas autorizadas para utilizar el sistema de información.
- Eliminar o bloquear de modo inmediato los derechos de acceso a los usuarios que han cambiado de puesto de trabajo o que han dejado de trabajar para la organización.
- Realizar comprobaciones periódicas para eliminar o bloquear identificadores de usuario y cuentas redundantes. Asegurar que no se emitan identificadores de usuario redundantes a otros usuarios.

# Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

## Gestión de privilegios

Como medida de control, es esencial restringir y controlar adecuadamente la asignación y el uso de los privilegios dentro de la organización. Para ello, se debe establecer un procedimiento de autorización formal que supervise la asignación de privilegios, proporcionando una mayor protección contra el acceso no autorizado.

Al definir este procedimiento formal, se deben considerar los siguientes elementos:

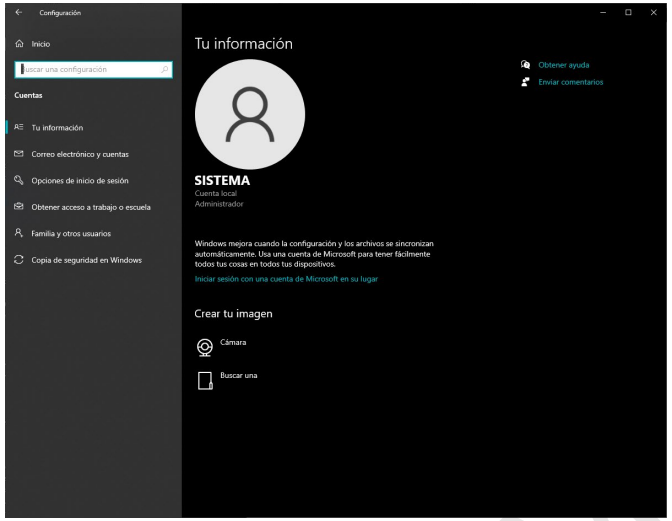
- **Privilegios de acceso específicos**: Asignar privilegios de acceso diferenciados para cada componente del sistema de información, por ejemplo, distintos privilegios para cada aplicación del sistema.
- **Principio de menor privilegio**: Los usuarios deben tener acceso únicamente a la información necesaria para desempeñar sus funciones, siguiendo el principio de "necesidad de saber".
- **Actualización continua**: Mantener el procedimiento de autorización y el registro de todos los privilegios asignados actualizado. Se recomienda no asignar privilegios hasta que el procedimiento de autorización esté completamente finalizado.
- **Minimización de privilegios**: Fomentar el desarrollo y uso de rutinas del sistema que minimicen la necesidad de asignar privilegios para tareas básicas y sistemáticas.
- **Desarrollo de aplicaciones seguras**: Promover la creación y uso de aplicaciones que reduzcan la necesidad de utilizar privilegios elevados.

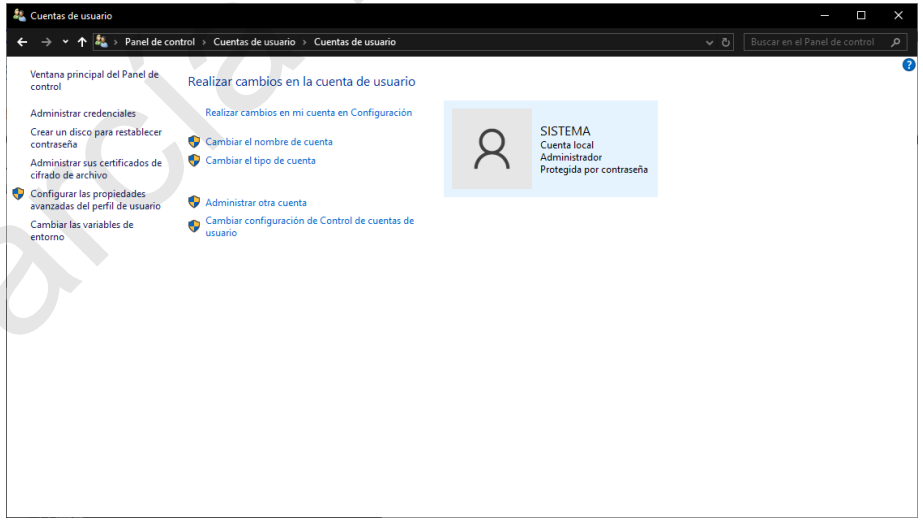
Por ejemplo, en el sistema operativo Windows, se utiliza la herramienta "Cuentas de usuario" para crear, eliminar y gestionar cuentas de usuario, así como para asignar privilegios a cada cuenta. Para acceder a esta herramienta, vaya a Inicio -> Panel de control -> Cuentas de usuario.

# Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

## Gestión de privilegios

Por ejemplo, en el sistema operativo Windows, se utiliza la herramienta "Cuentas de usuario" para crear, eliminar y gestionar cuentas de usuario, así como para asignar privilegios a cada cuenta. Para acceder a esta herramienta, vaya a Inicio -> Panel de control -> Cuentas de usuario.



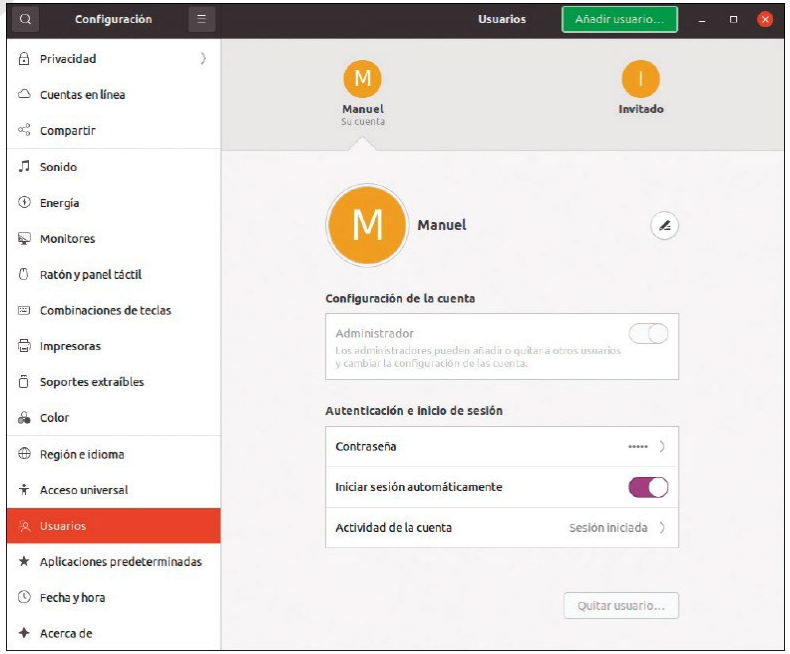

### Cuentas de usuario de Windows

En Windows, también puede asignar y modificar los privilegios de una cuenta como "Usuario estándar" (los usuarios con estos privilegios solo podrán acceder y modificar elementos que no afecten a otros usuarios ni a la seguridad del equipo) o "Administrador" (con privilegios de acceso completo al equipo). Para ello, haga clic en "Cambiar el tipo de cuenta" o asigne los privilegios directamente al momento de crear la cuenta.

# Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

## Gestión de privilegios

En el sistema operativo Linux, también existe una herramienta gráfica que permite la configuración de cuentas de usuario y grupos de cuentas con sus correspondientes privilegios. Para acceder a esta herramienta, inicie sesión como "root", pulse la combinación de teclas [Alt] + [F2] y ejecute el comando users-admin.



# Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

## Gestión de contraseñas de usuario

Para las organizaciones es fundamental establecer un procedimiento formal de gestión para la asignación de contraseñas a las cuentas de usuario. Este procedimiento debe incluir lo siguiente:

- **Confidencialidad y Documentación**: Requerir que los usuarios firmen un documento para mantener la confidencialidad de las contraseñas y conservar las claves grupales solo dentro de los miembros del grupo.
- **Contraseña Temporal**: Asignar a los usuarios una clave temporal segura que deben cambiar inmediatamente por una contraseña secreta propia.
- **Verificación de Identidad**: Establecer procedimientos que verifiquen la identidad de los usuarios antes de facilitarles una contraseña nueva, sustituta o temporal.
- **Entrega Segura**: Facilitar las contraseñas provisionales a los usuarios de un modo seguro, evitando la utilización de correo electrónico de terceros o no protegidos.
- **Seguridad de las Contraseñas**: Asegurar que las contraseñas provisionales sean únicas y difíciles de adivinar.
- **Reconocimiento de Recepción**: Requerir a los usuarios que reconozcan la recepción de una nueva contraseña.
- **Almacenamiento Seguro**: Evitar almacenar las contraseñas en lugares sin protección adecuada.
- **Cambio de Contraseñas Iniciales**: Modificar las contraseñas iniciales facilitadas por el proveedor después de la instalación del software adquirido.

Además de estos pasos, las contraseñas sirven como medio común para identificar y dar permiso a los usuarios antes de acceder a un sistema de información. No obstante, se recomienda la utilización de otras alternativas tecnológicas para identificar a los usuarios, como la utilización de firmas electrónicas o sistemas de verificación de huellas digitales, entre otras.

# Principios comúnmente aceptados para el control de accesos y de los distintos tipos de acceso locales y remotos

## Revisión de los derechos de acceso del usuario

Los directivos y gerentes de la organización deben encargarse de la revisión periódica de los distintos derechos de acceso de los usuarios mediante un procedimiento formal que debe incluir al menos los siguientes elementos:

- **Revisión Periódica**: Los derechos de acceso de los usuarios deben ser revisados periódicamente y después de cualquier cambio en la situación del usuario, como un ascenso en el puesto de trabajo o la terminación de la relación laboral.
- **Cambio de Puesto**: Los derechos de acceso deben revisarse y reasignarse cuando el usuario cambia de un puesto de trabajo a otro dentro de la misma organización, con una frecuencia máxima de cada seis meses.
- **Privilegios Especiales**: Las autorizaciones para privilegios especiales deben ser revisadas con mayor frecuencia que las autorizaciones estándar, con una frecuencia máxima de cada tres meses.
- **Registro de Cambios**: Mantener un registro de todos los cambios realizados en las cuentas privilegiadas para llevar un control de las mismas durante las revisiones periódicas.

En resumen, las organizaciones deben realizar revisiones periódicas de los derechos de acceso de los usuarios para asegurar un control completo y efectivo sobre el acceso a sus sistemas de información.

# Requerimientos legales en referencia al control de accesos y asignación de privilegios

## Introducción

Los requerimientos legales en referencia al control de accesos y a la asignación de privilegios que deben tenerse en cuenta se centran principalmente en la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD 3/2018) y en el Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (GDPR).

Ambas normativas establecen como principios fundamentales la garantía de las tres propiedades de la información:

- **Integridad de la información**: La información no debe sufrir cambios no deseados.
- **Confidencialidad de la información**: Solo los usuarios autorizados deben tener acceso a la información.
- **Disponibilidad de la información**: La información debe estar disponible siempre que las personas autorizadas lo requieran.

# Requerimientos legales en referencia al control de accesos y asignación de privilegios

## Medidas organizativas y técnicas

Los responsables o encargados del tratamiento de datos deben adoptar e implantar una serie de medidas para proteger los datos personales durante su tratamiento. Estas medidas se dividen en:

- **Medidas organizativas**: Procedimientos, normas, reglas y estándares de seguridad destinados a proteger los datos personales.
- **Medidas técnicas**: Acciones encaminadas a mantener la integridad, confidencialidad y disponibilidad de la información cuando contiene datos de carácter personal. Estas medidas se clasifican según el nivel de seguridad de los datos: básico, medio y alto.

## Reglamento de desarrollo de la LOPDGDD

El Real Decreto 1720/2007, que aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contienen datos de carácter personal, también menciona los niveles de seguridad y describe los datos para los cuales deben tomarse cada tipo de medida.

# Requerimientos legales en referencia al control de accesos y asignación de privilegios

## Medidas específicas de la LOPDGDD

La LOPDGDD promueve una serie de medidas de seguridad en relación con el control de accesos y la asignación de privilegios. Estas medidas pueden resumirse en:

- **Acceso autorizado**: Los usuarios deben tener acceso únicamente a los datos necesarios para el desempeño de sus funciones.
- **Mecanismos de control**: El responsable del tratamiento establecerá mecanismos para evitar que un usuario acceda a datos o recursos con derechos distintos de los autorizados.
- **Registro de acceso**: Se mantendrá una lista de usuarios con acceso autorizado al sistema de información, especificando el acceso permitido para cada uno.
- **Control de modificaciones**: Solo el personal autorizado podrá conceder, alterar o anular el acceso autorizado a los datos y recursos, según los criterios del responsable del tratamiento.
- **Identificación de usuarios**: Se implementará un mecanismo que permita la identificación inequívoca y personalizada de cada usuario que intente acceder al sistema de información y la verificación de su autorización.
- **Prevención de intentos de acceso no autorizados**: Se limitará la posibilidad de intentar reiteradamente acceder sin autorización al sistema de información.
- **Control de acceso físico**: Solo el personal autorizado podrá acceder a los locales donde se encuentren los sistemas de información con datos personales. Se registrarán, como mínimo, la identificación del usuario, la fecha y hora de acceso, el fichero accedido, el tipo de acceso y si fue autorizado o denegado.
- **Conservación de registros**: Los datos de acceso autorizados deben ser guardados para permitir la identificación del registro accedido.

# Requerimientos legales en referencia al control de accesos y asignación de privilegios

## Medidas específicas de la LOPDGDD

La LOPDGDD promueve una serie de medidas de seguridad en relación con el control de accesos y la asignación de privilegios. Estas medidas pueden resumirse en (II)

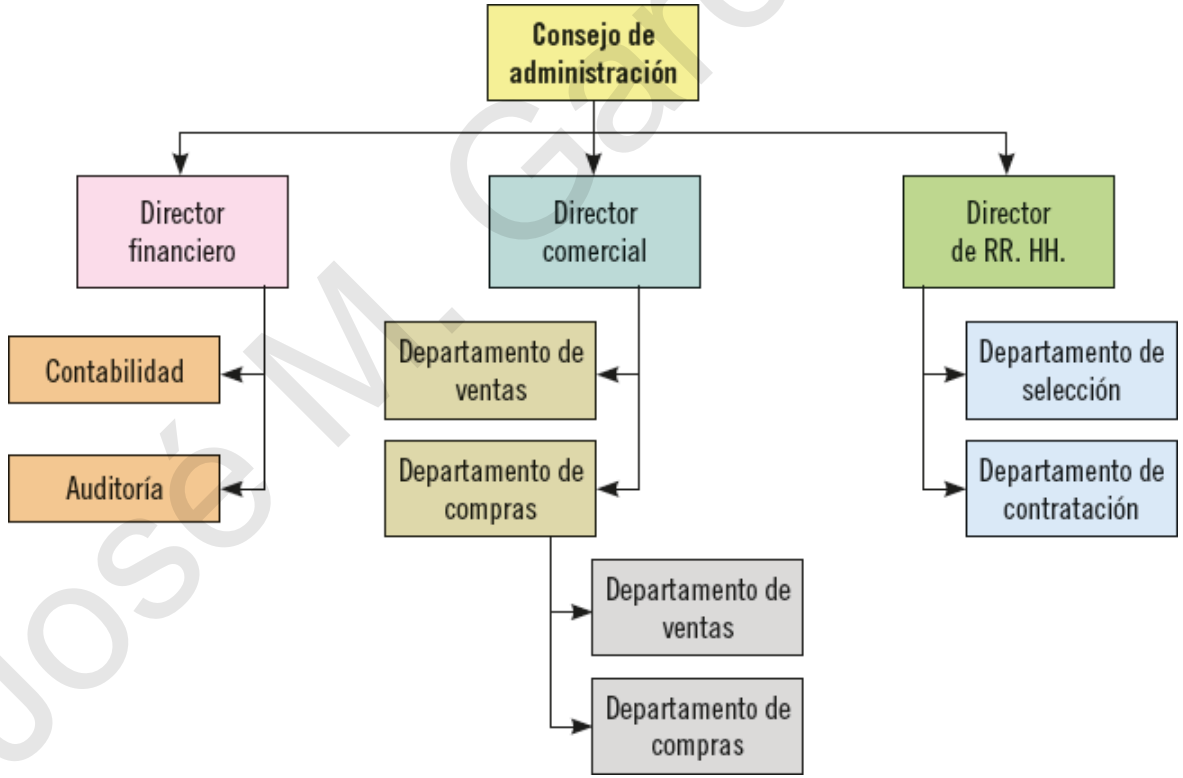
- **Control de registros**: Los mecanismos que registran los datos estarán bajo el control directo del responsable de seguridad y no podrán ser desactivados. El periodo mínimo de conservación de los datos registrados será de dos años.
- **Revisión periódica**: El responsable de seguridad revisará periódicamente la información registrada y elaborará un informe de las revisiones y problemas detectados, al menos, una vez al mes.

| Medida | Temporalidad |
|---|---|
| Acceso autorizado solo a los datos necesarios. | |
| Establecimiento de mecanismos para evitar el acceso de usuarios con derechos distintos a los autorizados (responsable de tratamiento de datos). | |
| Relación de usuarios que contenga el acceso autorizado de cada uno de ellos. | |
| La concesión, alteración y/o anulación del acceso autorizado solo puede realizarla el personal autorizado en el documento de seguridad. | |
| El responsable de tratamiento de datos debe establecer un mecanismo para identificar a los usuarios que intentan acceder al sistema. | |
| Limitación de los intentos reiterados de accesos no autorizados. | |
| Control de acceso físico limitado al personal autorizado en el documento de seguridad. | |
| Almacenamiento de la identificación, fecha y hora del acceso, fichero accedido, tipo de acceso y acceso autorizado/denegado en cada acceso. | |
| En accesos autorizados, almacenamiento de la información que identifique al registro accedido. | |
| El responsable de seguridad debe controlar directamente los mecanismos de registro de los datos. | |
| Conservación de los datos | mínimo dos años. |
| Revisión de la información de control y elaboración de informes | una vez al mes por el responsable de seguridad. |

# Perfiles de acceso en relación con los roles funcionales del personal de la organización

Al definir los distintos perfiles de acceso, es fundamental tener en cuenta los roles funcionales del personal de la organización. Para establecer estos roles, primero se debe visualizar y entender el organigrama de la organización. Un organigrama es una representación gráfica de la estructura de una empresa u organización, en la que se muestran los distintos departamentos, sus competencias y las relaciones jerárquicas establecidas entre los puestos y departamentos.

El organigrama debe ser sencillo, conciso y sistemático. No es necesario incluir información detallada de las funciones de cada puesto de trabajo; basta con mostrar el nombre del puesto, el empleado que lo ocupa y sus relaciones jerárquicas para obtener una visión global de la estructura funcional de la empresa.



# Perfiles de acceso en relación con los roles funcionales del personal de la organización

Para definir los roles de acceso, una vez clara la estructura funcional de la organización, es necesario profundizar en las descripciones, funcionalidades y responsabilidades de cada puesto de trabajo. Esto permitirá conocer las características de cada uno y determinar el nivel de seguridad al que deben tener acceso los empleados de cada puesto.

Una vez concretados los permisos y privilegios de acceso de cada puesto de trabajo, es necesario identificar a cada empleado que ocupa esos puestos y otorgar permisos, identificadores y contraseñas personalizados, en función de su nivel de responsabilidad y del nivel de seguridad requerido para el desempeño de sus tareas.

Los accesos que se otorguen a cada empleado pueden clasificarse en:

- **Solo lectura**: El usuario solo puede leer y visualizar los ficheros, sin ejecutar ninguna aplicación.
- **Lista de contenidos**: El usuario puede abrir las carpetas para visualizar los archivos, pero no puede acceder a ellos.
- **Leer y ejecutar**: El usuario puede ejecutar aplicaciones que no influyan en los datos de la organización y visualizar los archivos, sin realizar modificaciones.
- **Leer y modificar**: El usuario puede visualizar y modificar archivos, ejecutar aplicaciones y modificar archivos a través de ellas, pero no crear nuevos archivos ni eliminar los existentes.
- **Control total**: El usuario puede realizar cualquier operación en los archivos, incluyendo su creación, modificación y eliminación.

**Nota**: El otorgamiento de accesos de control total debe limitarse al máximo para evitar exponer los archivos a un uso malintencionado.

# Perfiles de acceso en relación con los roles funcionales del personal de la organización

Es crucial que la asignación de permisos sea coherente con la jerarquía establecida en el organigrama de la organización. Los usuarios con menores responsabilidades deben tener menos privilegios o solo sobre archivos menos relevantes, mientras que los altos directivos deben tener privilegios para ejercer control total sobre los archivos de su competencia. Así, la estructura de los permisos otorgados a los usuarios debe reflejar la estructura real de la organización.

Además, los permisos asignados a cada puesto de trabajo deben limitarse a los archivos estrictamente necesarios para el desempeño efectivo de sus funciones, sin permitir la visualización o modificación de archivos que no son de su competencia.

Una correcta asignación de permisos acorde a los roles definidos dentro de la organización permite un control de seguridad óptimo sobre los accesos a los archivos. En concordancia con los requerimientos legales mencionados anteriormente, es recomendable y, en ocasiones, obligatorio documentar formalmente la asignación de permisos de acceso y privilegios, informando a cada empleado sobre sus permisos, derechos y obligaciones, así como las sanciones en caso de violar dichos permisos.

# Herramientas de directorio activo y servidores LDAP en general

## Introducción

El directorio activo es un servicio de directorio que gestiona todos los elementos de una red, desde equipos hasta grupos, usuarios, dominios, políticas de seguridad y cualquier otro objeto definido por el usuario.

**Importante**: Un servicio de directorio se refiere al directorio donde se almacena la información sobre los usuarios y los recursos, así como al conjunto de servicios que permite gestionar todos estos recursos.

**Funciones del directorio activo.** Las funciones del directorio activo se definen en torno a tres áreas principales:

- **Gestión de identidad**: Se encarga de identificar inequívocamente a cualquier persona
- **Seguridad**: Organiza y simplifica la localización y el acceso a los distintos recursos de la red
- **Gestión de la configuración**: Gesiona la configuración de los elementos de la red

# Herramientas de directorio activo y servidores LDAP en general

## Introducción

**Gestión de identidad**: El directorio activo se encarga de identificar inequívocamente a cualquier persona de una organización mediante:

- La elaboración y revisión de un repositorio central de usuarios, servidores y puestos.
- La reducción al mínimo necesario del número de repositorios y contraseñas.
- El establecimiento de políticas de seguridad, validación y autorización.

**Seguridad**: El directorio activo organiza y simplifica la localización y el acceso a los distintos recursos de la red de la organización. Además, aplica las políticas de seguridad establecidas mediante una herramienta de gestión unificada, a través de:

- La automatización del bloqueo de sistemas operativos.
- El refuerzo del uso de contraseñas y credenciales.
- La posibilidad de delegar tareas administrativas para lograr una administración homogénea.

**Gestión de la configuración**: El directorio activo gestiona la configuración de los elementos de la red para aumentar la productividad del usuario y reducir los costes de administración, soporte y aprendizaje. Para conseguir estos objetivos, se basa en funciones como:

- La gestión de usuarios y equipos de manera centralizada.
- La automatización de la aplicación de las políticas de seguridad.
- Una implementación eficiente de las configuraciones estándar para usuarios, grupos de usuarios y equipos.

# Herramientas de directorio activo y servidores LDAP en general

## Introducción

El directorio activo está construido alrededor de una serie de protocolos de plataforma independiente que permiten trabajar con sistemas operativos Windows, Linux y Macintosh. Los principales protocolos son los siguientes:

- **LDAP (Lightweight Directory Access Protocol)**: Permite el acceso a un servicio de directorio ordenado y distribuido, cuya función principal es permitir la búsqueda de información en un entorno de red. A menudo, se considera una base de datos sobre la que se pueden realizar consultas para localizar los datos deseados.
- **DNS (Domain Name System)**: Es una base de datos jerárquica que almacena información sobre los nombres de dominio en las redes. Su uso más común está relacionado con la asignación de nombres de dominio a las direcciones IP.
- **DHCP (Dynamic Host Configuration Protocol)**: Es un protocolo que asigna de modo automático las direcciones IP.
- **Kerberos**: Es un protocolo de autenticación de usuarios que permite que dos equipos en una red de baja seguridad se puedan identificar mutuamente de un modo seguro.

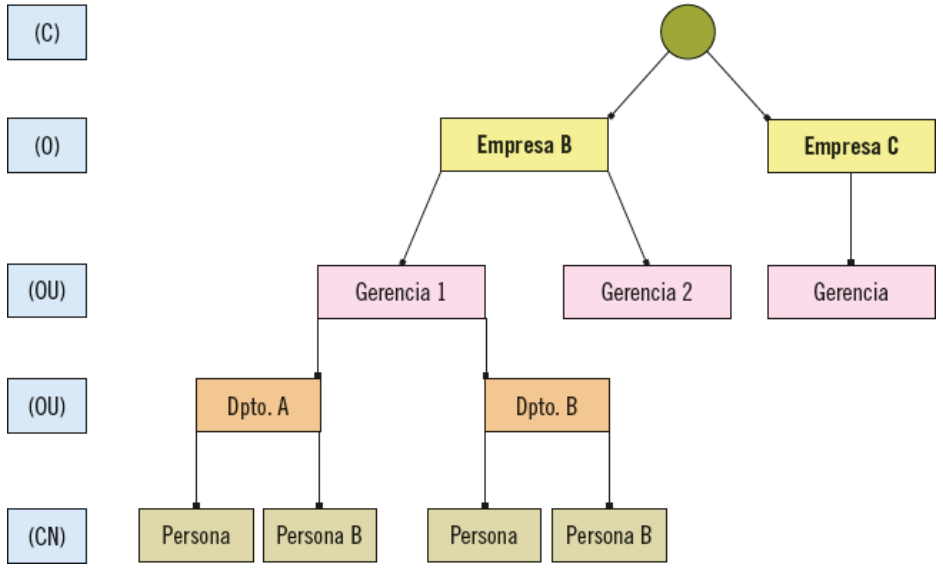
# Herramientas de directorio activo y servidores LDAP en general

## LDAP o Protocolo Ligero para Acceder al Servicio de Directorio

El Protocolo Ligero para Acceder al Servicio de Directorio, conocido como LDAP (Lightweight Directory Access Protocol), almacena la información de los usuarios que forman parte de una red y permite el acceso a los datos de un directorio ordenado y distribuido cuando se pretende localizar algún tipo de información.

En LDAP, la información se almacena en entradas. Una entrada es una colección de atributos con un único Nombre Global Distinguido o DN. Cada uno de los atributos de una entrada contiene un tipo y uno o varios valores. Los tipos suelen ser palabras nemotécnicas, por ejemplo, “mail” para referirse a correos electrónicos. Un atributo llamado “mail” podría contener valores como, por ejemplo: lgarcia@gmail.com.

Las entradas siguen una estructura jerárquica con forma de árbol invertido, con una serie de bifurcaciones, como se muestra en la siguiente imagen:



# Herramientas de directorio activo y servidores LDAP en general

## LDAP o Protocolo Ligero para Acceder al Servicio de Directorio

El mecanismo de LDAP busca e identifica las entradas requeridas mediante la utilización de pares clave/valor. Las claves más utilizadas por LDAP para localizar información son las siguientes:

- **uid**: identificación única obligatoria.
- **cn (common name)**: nombre común de la persona.
- **givenname**: nombre de pila de la persona.
- **sn (surname)**: apellido de la persona.
- **o (organization)**: organización donde trabaja la persona.
- **ou (organizational unit)**: unidad o departamento en el que trabaja la persona.
- **mail**: correo electrónico de la persona.

# Herramientas de directorio activo y servidores LDAP en general

## LDAP o Protocolo Ligero para Acceder al Servicio de Directorio

**Herramientas**

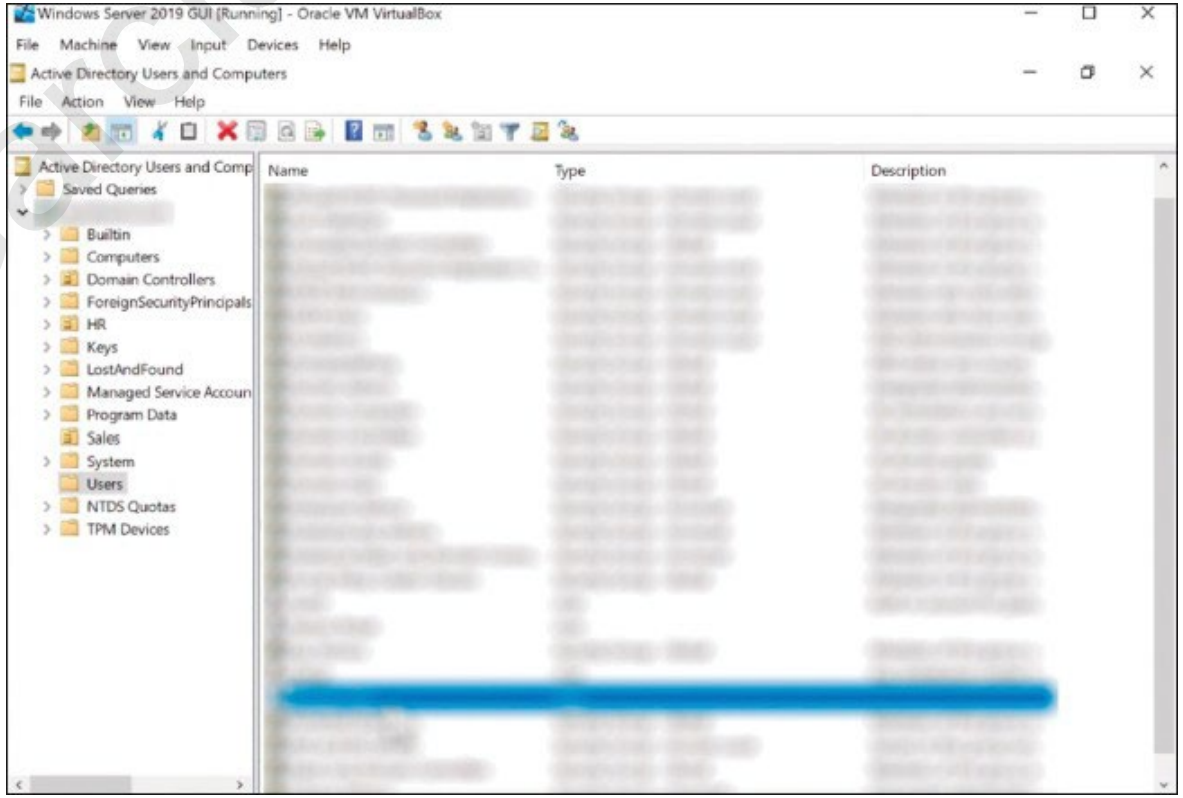
Actualmente, en el mercado hay numerosas herramientas de directorio activo y servidores LDAP. A continuación, se enumeran las herramientas más utilizadas.

**Active Directory (AD)** es la herramienta de directorio activo utilizada por Windows Server.

Almacena la información sobre los recursos de la red y permite el acceso de los usuarios y las aplicaciones a dichos recursos.

Es una herramienta muy útil si se pretende realizar una administración centralizada del acceso a los recursos de la red.

Es un servicio de directorio que almacena un repositorio estructurado sobre todo tipo de objetos: equipos, impresoras, usuarios, servidores, etc.



# Herramientas de directorio activo y servidores LDAP en general

## LDAP o Protocolo Ligero para Acceder al Servicio de Directorio

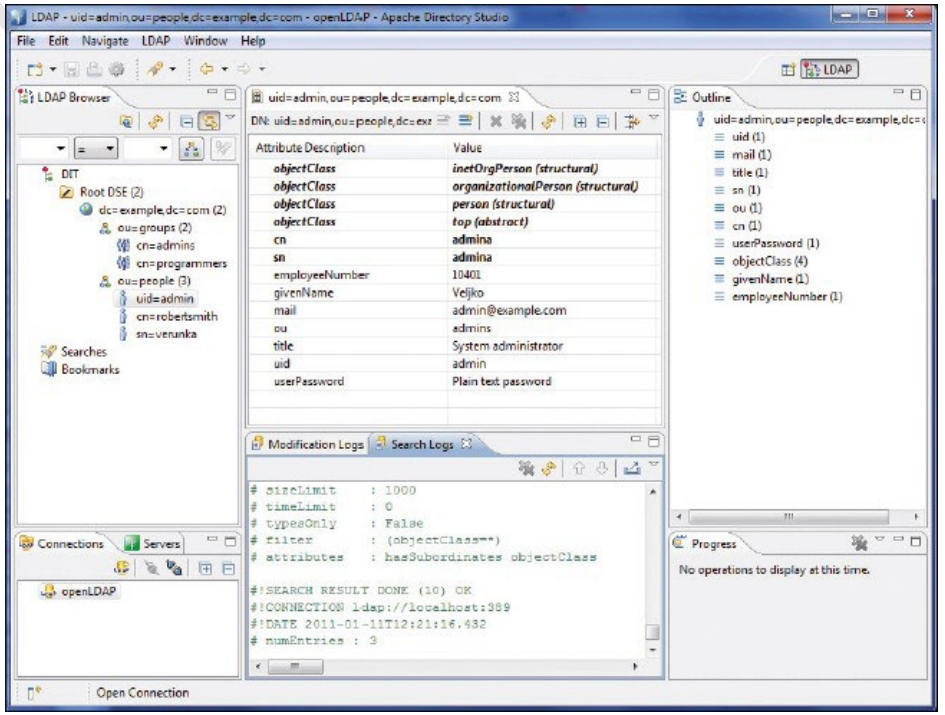
**Herramientas**

**OpenLDAP** es una implementación libre del protocolo LDAP con licencia propia.

Es un protocolo independiente de la plataforma y se puede utilizar tanto en Linux como en Macintosh y Microsoft Windows, entre otros sistemas operativos.

Esta distribución contiene, a su vez, varios programas:

- **Slapd**: servidor LDAP que permite utilizar múltiples bases de datos.
- **Slurpd**: programa que se encarga de distribuir los cambios producidos en el servidor maestro a los demás servidores.
- **Librerías**: librerías LDAP que se pueden generar de forma estática y/o dinámica.



# Herramientas de directorio activo y servidores LDAP en general

## LDAP o Protocolo Ligero para Acceder al Servicio de Directorio

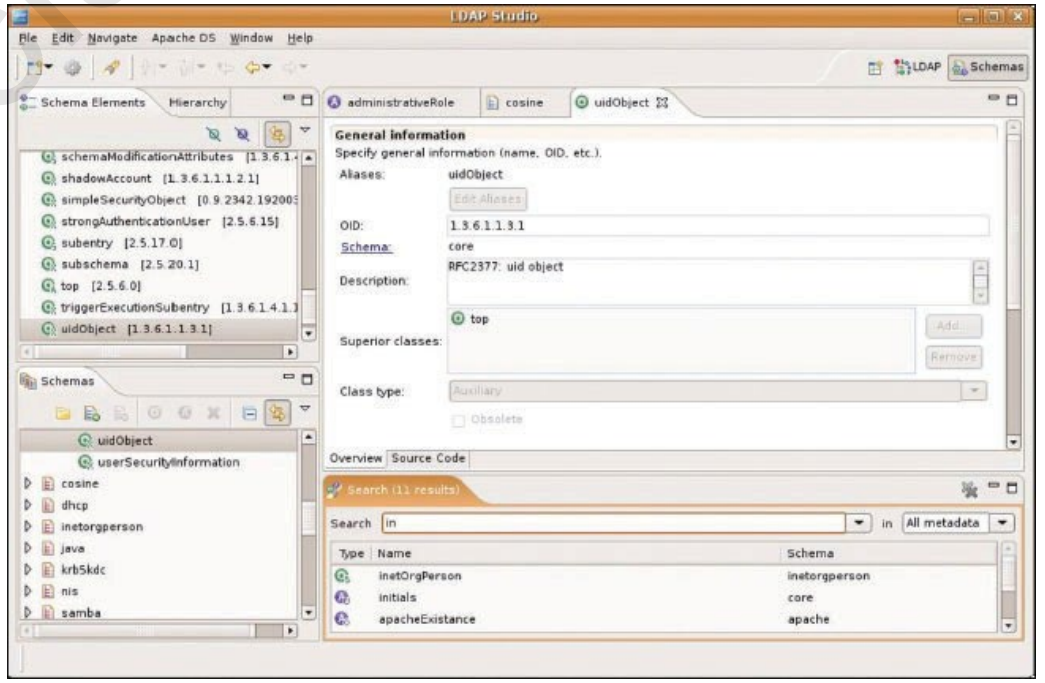
**Herramientas**

**Apache Directory Server/Apache Directory Studio** es un servidor de directorio LDAP desarrollado en lenguaje Java bajo la licencia de Apache Software.

El navegador LDAP de este servidor es el llamado Apache Directory Studio. Además del protocolo LDAP, Apache DS también soporta más protocolos como Kerberos, DNS y NTP, entre otros.

Facilita un directorio de usuarios y sus respectivos grupos a los que pertenecen y tiene funciones propias de las bases de datos relacionales, lo que lo diferencia de otras herramientas.

Es una de las herramientas más útiles para administrar servidores LDAP.



# Herramientas de directorio activo y servidores LDAP en general

## LDAP o Protocolo Ligero para Acceder al Servicio de Directorio

**Herramientas**

Además de las herramientas mencionadas anteriormente, existen varias otras herramientas útiles para la gestión de directorios activos y servidores LDAP. Aquí se destacan algunas adicionales:

- **Herramientas de verificación de LDAP de Active Directory**: Microsoft Active Directory ofrece diversas herramientas para gestionar el entorno LDAP del sitio, permitiendo una administración eficiente y segura del directorio.
- **Herramientas de administración remota del servidor (RSAT)**: Estas herramientas proporcionan una gama completa de opciones para la administración de servidores, incluyendo la gestión de directorios activos y la configuración de políticas de seguridad en entornos Windows.
- **SofTerra LDAP Browser**: Una herramienta que permite explorar y gestionar directorios LDAP de manera intuitiva. Es útil para visualizar la estructura del directorio, realizar búsquedas y modificar entradas.
- **JXplorer**: Un navegador LDAP de código abierto que proporciona una interfaz gráfica de usuario para explorar y modificar los datos en directorios LDAP. Es compatible con varios sistemas operativos y facilita la administración de datos en entornos LDAP.

Estas herramientas complementan a Active Directory, OpenLDAP y Apache Directory Server, ofreciendo opciones adicionales para la administración de directorios y la seguridad de los datos en la red.

# Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)

## Introducción

La identidad es la representación de un individuo o entidad dentro de un sistema de información. Es lo que permite distinguir a un usuario de los demás. Un perfil de identidad incluye aspectos como:

- Identificación única.
- Información personal del usuario.
- Credenciales de autenticación.
- Permisos de acceso y roles asignados al usuario.

La gestión de identidades y autorizaciones (IAM) es un conjunto de sistemas y procesos encargados de gestionar y controlar la identidad de las personas que acceden a los recursos del sistema de información y todo lo que puede hacer cada usuario con estos recursos, cumpliendo en todo momento con las políticas definidas por la organización.

### Funcionalidades de la gestión de identidades

- **Creación y mantenimiento de perfiles**: Simplifica la gestión de los usuarios.
- **Control de acceso**: Facilita o deniega el acceso a los recursos, tanto lógicos como físicos, a los usuarios adecuados.
- **Visibilidad de servicios**: Añade visibilidad a los servicios de la organización, ampliando de un modo seguro los servicios que esta ofrece a los usuarios.

# Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)

**Acciones posibles con herramientas IAM**

- **Provisión o desprovisión de cuentas**: Alta de cuentas nuevas y baja de cuentas que ya no deben acceder al sistema.
- **Automatización del flujo de trabajo**: Permiten automatizar tareas para la integración de procesos de autenticación y autorización.
- **Administración remota**: Gestionar las identidades desde equipos externos con conexión a Internet.
- **Sincronización de contraseñas**: Permite que los usuarios tengan la misma contraseña para cada sistema y aplicación.
- **Reemplazo automático de contraseñas**: Reemplazo automático de contraseñas tras varios intentos de acceso no autorizados para impedir accesos indebidos.

**Ventajas principales**

- **Mejora de la seguridad**: Incrementa la seguridad de la organización.
- **Consolidación de políticas de seguridad**: Refuerza las políticas de seguridad definidas.
- **Reducción de costes**: Disminuye los costes de administración.

**Problemáticas solucionadas por las herramientas IAM**

- **Acceso de múltiples usuarios**: Gestiona el acceso de un número creciente de usuarios internos y externos.
- **Oportunidades de negocio**: Ofrece control y seguridad en las operaciones de negocio.
- **Diversidad de aplicaciones y sistemas**: Integra sistemas con diferentes formas de autenticación y autorización.
- **Múltiples autorizaciones**: Gestiona autorizaciones basadas en distintos mecanismos.
- **Requerimientos legales**: Cumple con altos controles de seguridad exigidos por la LOPDGDD.
- **Competencia en el mercado**: Facilita la reducción de costes para enfrentar la competencia

# Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)

No obstante, a pesar de las numerosas ventajas de estas herramientas, también hay que tener en cuenta una serie de desventajas:

- **Riesgos de seguridad**: La funcionalidad de sincronización de contraseñas puede incrementar los riesgos de seguridad. Si se descubre una contraseña, se puede acceder a todas las aplicaciones a las que el usuario tiene acceso.
- **Fallas en autenticación y autorización**: En las herramientas de gestión de identidades y autorizaciones, el acceso a las aplicaciones se realiza mediante la autenticación de los usuarios. Si hay algún fallo en los procesos de autenticación y autorización, esto afectaría a todas las aplicaciones integradas en estas herramientas.
- **Reestructuración de procesos**: La implementación de estas herramientas suele requerir una reestructuración de los procesos y de la operativa de las organizaciones, lo que supone tiempo, gasto y recursos. Además, se necesita una elevada inversión de dinero, tiempo y recursos, lo que no resulta viable para proyectos a corto plazo.
- **Conocimiento profundo requerido**: Es necesario tener un conocimiento profundo de las aplicaciones que se pretenden integrar en la solución IAM para que las configuraciones de autenticación y autorización se realicen correctamente.

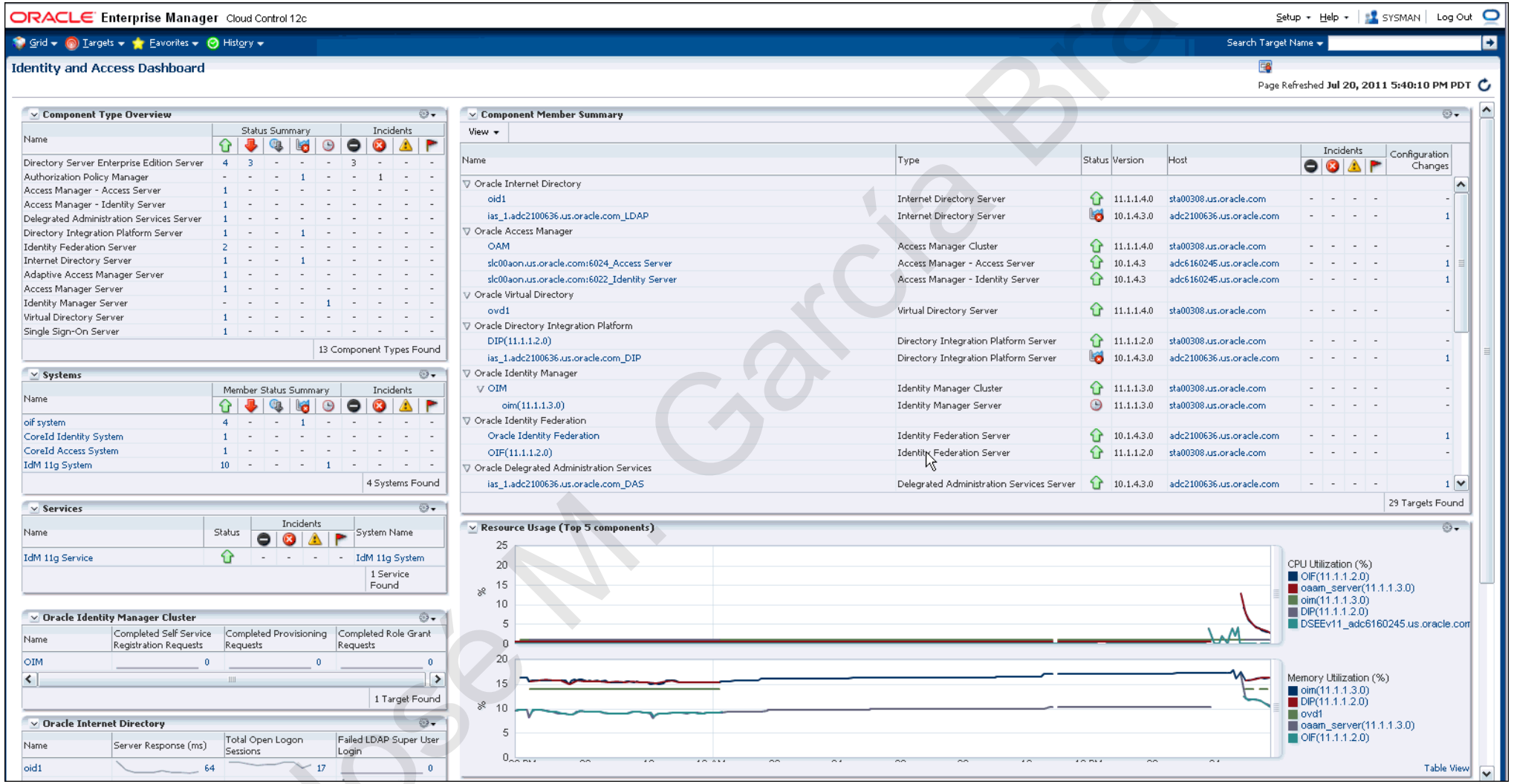
# Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)

**Herramientas**

**Oracle Identity Manager** es una herramienta desarrollada por Oracle que ofrece una solución integrada para la gestión de identidades y accesos. Esta herramienta incluye las siguientes funcionalidades:

- **Repositorio estándar LDAP**: Facilita la gestión de la información de identidad mediante un repositorio estándar LDAP.
- **Integración con otros directorios**: Permite la integración con diferentes directorios, facilitando una gestión centralizada.
- **Aprovisionamiento automático**: Permite el aprovisionamiento automático de los usuarios en el entorno Oracle, mejorando la eficiencia de la administración de identidades.
- **Herramientas de administración**: Facilita herramientas que permiten a la propia organización gestionar las identidades de manera autónoma.
- **Single sign-on (SSO)**: Ofrece herramientas de inicio de sesión único para aplicaciones web, mejorando la experiencia del usuario y simplificando el acceso a múltiples sistemas.

# Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)



# Herramientas de sistemas de gestión de identidades y autorizaciones (IAM)

**Otras herramientas**

**ManageEngine ADManager Plus:** Esta herramienta proporciona una solución completa para la administración de Active Directory, incluyendo la gestión de usuarios, informes detallados y automatización de tareas administrativas

**AWS Identity and Access Management (IAM):** Utilizado para gestionar el acceso a los recursos de Amazon Web Services, esta herramienta permite definir y aplicar políticas detalladas de acceso, mejorando la seguridad y gestión en la nube

**Azure Active Directory (Azure AD)**, ahora conocido como **Microsoft Entra ID**, es una solución de administración de identidades y accesos basada en la nube que protege los datos y gestiona los accesos a aplicaciones empresariales. Esta herramienta ofrece varias funcionalidades clave:

- **Gestión de Identidades y Accesos**: Permite autenticar a los usuarios y regular el acceso a sistemas, redes y datos.
- **Seguridad Mejorada**: Salvaguarda la información sensible mediante políticas de acceso y autenticación robustas.
- **Single Sign-On (SSO)**: Facilita el acceso de los usuarios a múltiples aplicaciones con una sola autenticación.
- **Multi-Factor Authentication (MFA)**: Añade una capa adicional de seguridad mediante la autenticación multifactor.
- **Integración con Otras Herramientas**: Se integra fácilmente con otras soluciones de Microsoft y aplicaciones de terceros, proporcionando una gestión centralizada y simplificada de identidades.

# Herramientas de sistemas de punto único de autenticación: Single Sign On (SSO)

Las herramientas de sistemas de punto único de autenticación o Single Sign On (SSO) facilitan que los usuarios de los sistemas de información realicen solo una vez el procedimiento de identificación y autenticación para acceder a los distintos servicios que facilitan dichos sistemas. Es decir, los procedimientos SSO habilitan al usuario para acceder a todos los servicios del sistema con una sola autenticación.

**Se distinguen cinco tipos de herramientas SSO:**

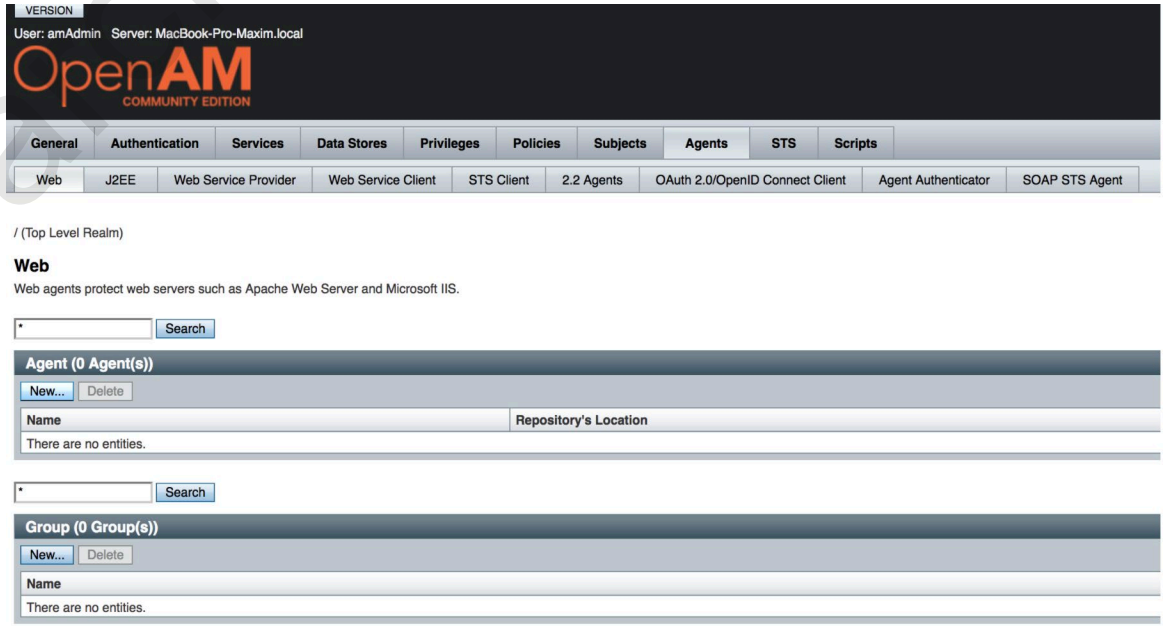
- **Enterprise Single Sign-On (E-SSO) o Legacy Single Sign-On**: Estas herramientas utilizan una autenticación primaria para completar automáticamente las aplicaciones secundarias con el mismo usuario y contraseña.
- **Web Single Sign-On (Web-SSO) o Web Access Management (Web-AM)**: Funciona solo en aplicaciones y recursos web y utiliza cookies para reconocer a aquellos usuarios que han accedido exitosamente y su estado de autenticación.
- **Kerberos**: Protocolo que externaliza la autenticación de los usuarios a través del servidor Kerberos.
- **OpenID**: Herramienta que compila la identidad en una dirección URL, la cual puede ser verificada posteriormente por cualquier aplicación o servidor para conocer la identidad y los privilegios del usuario que pretende acceder.
- **Identidad federada**: Herramienta mediante la cual se evitan autenticaciones redundantes para identificar a los usuarios en aplicaciones web.

# Herramientas de sistemas de punto único de autenticación: Single Sign On (SSO)

Una herramienta SSO útil y de código abierto es la antigua OpenSSO, ahora llamada OpenAM. Esta está distribuida por la empresa Sun Microsystems y dispone de funcionalidades que permiten la simplificación de la identificación de los usuarios en infraestructuras de red segura.

**Capacidades principales de OpenAM**

- Servicios de autenticación de usuarios.
- Permite establecer políticas de autorización.
- Adapta el proceso de autenticación al riesgo de la red y/o aplicación: cuanto más riesgo haya, más pasos habrá que seguir hasta concluir con la autenticación.
- Facilita servicios de identidad federada.
- Provee múltiples mecanismos distintos SSO.
- Alta disponibilidad, con una tasa muy baja de fallos en los inicios de sesión.
- Permite que los administradores puedan realizar modificaciones en la aplicación con conocimientos de programación.



# Resumen

Al definir la política de acceso de los sistemas de información de una organización, es fundamental realizar un análisis inicial de los requerimientos de acceso. Estos requerimientos se encuentran principalmente en la normativa ISO/IEC 27002:2013, concretamente en el apartado 9.

Además de la normativa ISO, es crucial referirse a la Ley de Protección de Datos Personales y garantía de derechos digitales (Ley 3/2018), que adapta a la normativa española las recomendaciones del Reglamento Europeo (UE) 2016/679. Este reglamento tiene como objetivo unificar criterios de actuación en todos los países miembros en relación a la protección de las personas físicas respecto al tratamiento de datos personales y a la libre circulación de estos datos.

Una vez definida la política de seguridad de la empresa y revisadas las medidas de seguridad que deben adoptarse conforme a los requerimientos legales, es posible definir los distintos perfiles de acceso de la organización según el puesto de trabajo. No todos los empleados deben tener acceso al mismo tipo de información; es vital observar el organigrama de la organización y las responsabilidades de cada puesto para asignar acceso y privilegios exclusivamente a la información necesaria para cada empleado.

Existen varias herramientas de control de accesos:

- **Herramientas de directorio activo**: Gestionan todos los elementos que forman parte de una red.
- **Herramientas de gestión de identidades y autorizaciones (IAM)**: Gestionan la identidad de las personas que acceden a los recursos del sistema de información y controlan lo que cada usuario puede hacer con estos recursos.
- **Herramientas de sistemas de punto único de autenticación o Single Sign On (SSO)**: Facilitan que los usuarios solo tengan que identificarse una vez para acceder a los distintos servicios del sistema de información.

Con estas herramientas, las organizaciones pueden implementar una política de control de accesos activa y eficiente, incrementando así el nivel de seguridad de la organización.