# Práctica 7: Control de accesos y sistemas de autenticación en redes corporativas

## Curso: IFCT0609 - Programación de Sistemas Informáticos

## Objetivo:

Comprender y aplicar los principios de control de acceso y autenticación en los sistemas de información, así como familiarizarse con herramientas de directorio activo y autenticación como LDAP, Active Directory u OpenLDAP.

## Enunciado:

Imagina que formas parte del equipo de seguridad informática de una empresa mediana. Tu tarea es establecer un sistema básico de control de accesos utilizando herramientas de directorio activo. Para ello, realiza las siguientes actividades:  
  
1. Define una política de control de accesos para tu organización:  
 a. Enumera los roles funcionales principales (por ejemplo, administrativo, comercial, técnico, dirección).

Roles: Desarrollo, RRHH, Formación

### ****Política de Control de Accesos****

#### ****1. Objetivo****

Garantizar que el acceso a los sistemas de información, datos y recursos tecnológicos esté restringido únicamente a usuarios autorizados, según los principios de necesidad y mínimo privilegio.

#### ****2. Alcance****

Aplica a los empleados, proveedores y terceros con acceso a los sistemas de información de la organización en los departamentos de Formación, RRHH y Desarrollo Multiplataforma.

#### ****3. Principios Generales****

* Definir roles y responsabilidades claras para la administración de accesos.
* Aplicar el principio de mínimo privilegio: cada usuario solo tendrá acceso a la información y recursos estrictamente necesarios para su función.
* Implementar autenticación robusta para el acceso a los sistemas, con doble factor en casos críticos.
* Registrar y monitorear los accesos para identificar posibles anomalías.

#### ****4. Normas Específicas por Departamento****

##### **Formación**

* Acceso limitado a materiales educativos y plataformas de aprendizaje.
* Autenticación de usuarios basada en credenciales internas.
* Los formadores tendrán acceso de edición a materiales, mientras que los alumnos solo podrán visualizar contenidos.

##### **RRHH**

* Control estricto sobre los datos de empleados, con acceso exclusivo al personal autorizado.
* Implementación de cifrado en bases de datos con información sensible.
* Aplicación de políticas de acceso basado en roles (RBAC) para garantizar que solo los responsables puedan modificar registros de empleados.

##### **Desarrollo Multiplataforma**

* Uso de repositorios de código con acceso restringido según niveles de desarrollo.
* Implementación de políticas de revisión de código para cambios críticos.
* Acceso a entornos de producción y pruebas solo para personal con autorización explícita.

#### ****5. Gestión de Identidades y Accesos****

* Revisar periódicamente los accesos de los empleados y revocar privilegios cuando sea necesario.
* Implementar un sistema centralizado de gestión de identidades con auditoría de accesos.
* Procedimientos claros para solicitud, modificación y eliminación de accesos.

#### ****6. Monitoreo y Auditoría****

* Registrar todos los accesos e intentos de acceso no autorizados.
* Realizar auditorías de seguridad periódicas para asegurar cumplimiento de la norma.
* Notificar cualquier incidente de acceso no autorizado a los responsables de seguridad.

#### ****7. Sanciones y Cumplimiento****

El incumplimiento de esta política podrá conllevar sanciones administrativas, incluyendo restricciones de acceso, medidas disciplinarias o acciones legales según la gravedad de la infracción.

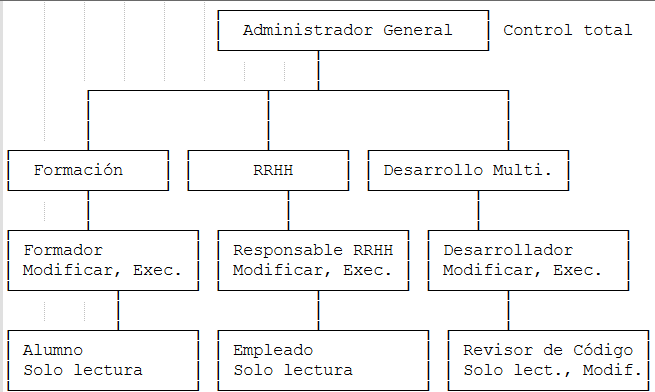
Esta política debe ser revisada y actualizada regularmente para alinearse con cambios normativos y tecnológicos.  
 b. Asigna los tipos de acceso a cada rol (solo lectura, control total, ejecutar, modificar, etc.).

| ****epartamento**** | ****Rol**** | ****Tipo de Acceso**** |
| --- | --- | --- |
| **Formación** | Alumno | Solo lectura |
|  | Formador | Modificar, Ejecutar |
|  | Administrador de plataforma | Control total |
| **RRHH** | Empleado | Solo lectura (datos personales) |
|  | Responsable de RRHH | Modificar, Ejecutar |
|  | Administrador de seguridad | Control total |
| **Desarrollo Multiplataforma** | Desarrollador | Modificar, Ejecutar (en entornos de desarrollo) |
|  | Revisor de código | Solo lectura, Modificar |
|  | Administrador de sistemas | Control total |

### ****Consideraciones adicionales:****

* **Principio de mínimo privilegio:** Cada usuario recibe únicamente los permisos necesarios para sus funciones.
* **Acceso basado en roles (RBAC):** Se asignan permisos según responsabilidades predefinidas.
* **Revisión periódica:** Los accesos deben revisarse regularmente para ajustar privilegios según cambios organizacionales.
* **Autenticación fuerte:** En casos críticos, se requiere doble factor de autenticación.

2. Crea un organigrama representando visualmente la estructura jerárquica y los accesos asignados.



3. Investiga e instala una herramienta de directorio activo o servicio LDAP (por ejemplo, OpenLDAP o Active Directory):

Instalacion de Active directory en windows server 2019   
 a. Describe el proceso de instalación y configuración básica.

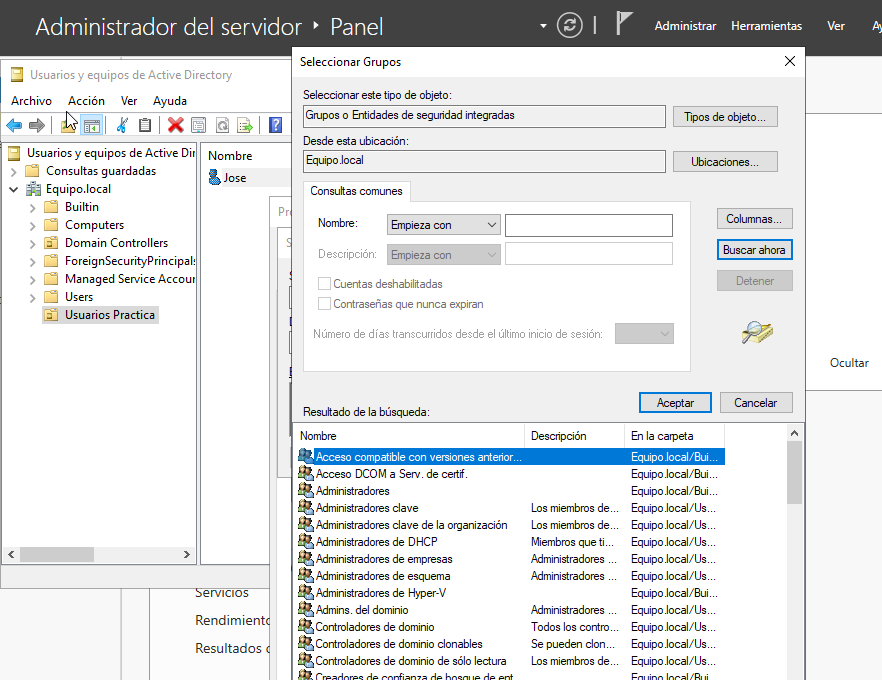
La instalacion referente al tutorial:

¹https://www.zentinels.net/instalar-active-directory-en-windows-server-2022-y-2019/

como indica el tutorial, una vez instalado se promueve el servidor a controlador de dominios, si no existe un bosque, se agrega uno, se recomienda que sea con extension .local.

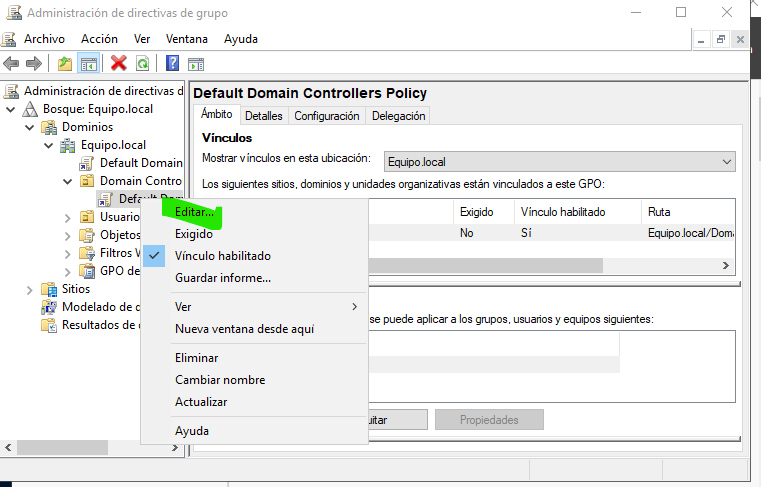
b. Explica qué atributos clave se utilizan para identificar a los usuarios.

Los atributos clave son nombre, contraseña, y rol, este rol ,lo define el grupo al que pertenezca

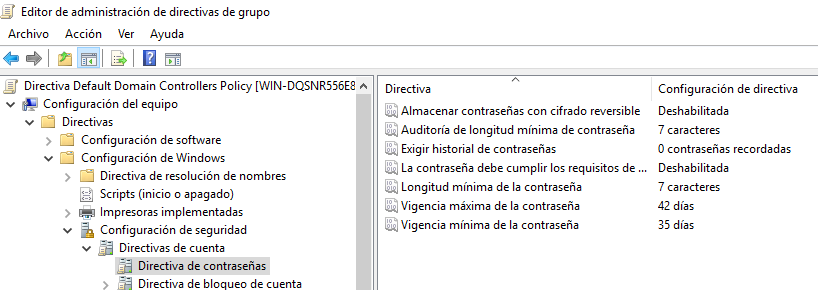


4. Establece un sistema de autenticación para los usuarios:  
 a. Explica cómo se gestionan las contraseñas.

Se ha creado al usuario Jose, y la politica de contraseñas se configura en el user por defecto, Administrador, en el administrador de directivas de grupo, en Default Domain Controllers Policy



y ahí en la opcion que indica la imagen se establecen las caracteristicas de la contraseña



la idea es establecer un sistema de autenticacion por RDP, con las licencias CAL de usuario para los servidores

Notas:

¹ licencia propiedad de Zentinels soporte informático y tecnologías