TEMA 3: SEGURIDAD LÓGICA

SMR - SEGURIDAD INFORMÁTICA

CONTENIDO

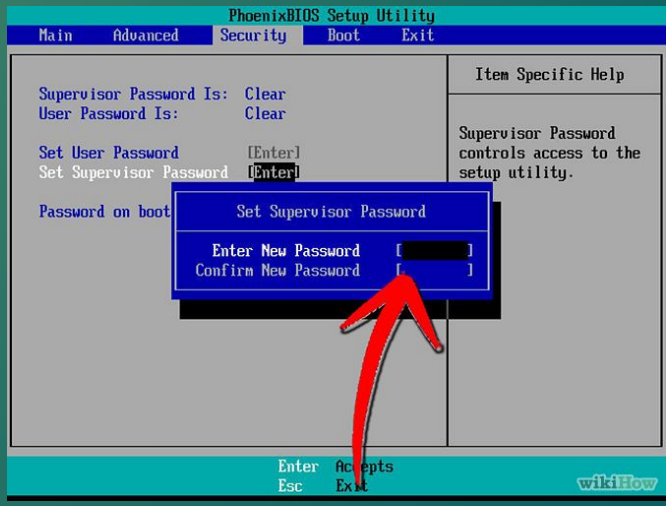
- **Introducción**
- Autenticación
  1. Contraseñas
  2. Listas de control de acceso (ACL)
- Amenazas para las contraseñas

¿POR QUÉ ES IMPORTANTE LA SEGURIDAD LÓGICA?

- ¿Qué es la seguridad lógica?
- ¿Por qué es importante la seguridad lógica?

SEGURIDAD LÓGICA

- **Seguridad lógica**: conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas, así como a garantizar el acceso a la información únicamente por las personas autorizadas.
- **Seguridad del equipo** (acceso al sistema)
  - Seguridad de acceso al equipo: BIOS, cifrado de particiones
  - Autenticación: local y global: contraseñas, formas de autenticar, ….
- **Seguridad en redes**
  - Cortafuegos: tipos, ubicación, tecnología, filtrado, arquitecturas,
  - Cortafuegos de alto nivel: proxy filtrado por aplicación y/o usuario.
  - Seguridad wifi y cableada.

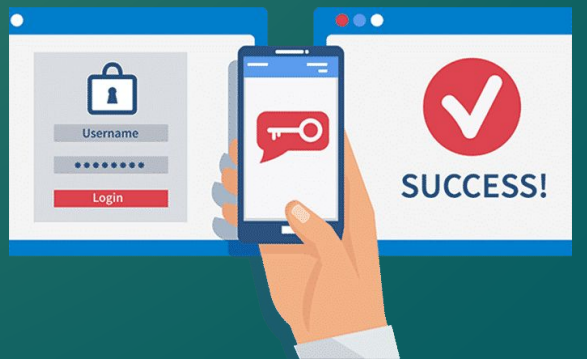


CONTENIDO

- Introducción
- **Autenticación**
  1. Contraseñas
  2. Listas de control de acceso (ACL)
- Amenazas para las contraseñas

AUTENTICACIÓN

- La **autenticación** es el proceso por el cual un sistema informático confirma que alguien, o algo, es quien dice ser. Es uno de los mecanismos establecidos en las políticas de seguridad informática.
- Tres grandes familias de esquemas de autenticación:
  - Algo que sabemos: contraseña o un código PIN.
  - Algo que poseemos: tarjeta de crédito, certificado digital, etc.
  - Algo que somos (autenticación biométrica): forma de la mano, huella dactilar, retina.



AUTENTICACIÓN

AUTENTICACIÓN

- **Autenticación fuerte**: se combinan al menos dos factores. Toda autenticación fuerte es, además, una autenticación multifactor (MFA), donde el usuario verifica su identidad tantas veces como factores se combinen.

- **Autenticación de dispositivos**: certificados digitales de ordenadores. Un certificado digital permite que una autoridad de certificación acredite la identidad de su propietario.

CONTENIDO

- Introducción
- Autenticación
  1. **Contraseñas**
  2. Listas de control de acceso (ACL)
- Amenazas para las contraseñas

AUTENTICACIÓN: GESTORES DE CONTRASEÑAS

- De nada sirve tener una contraseña segura si la almacenamos de forma insegura (en un papel, sin encriptar en un fichero). Para su **almacenamiento** debemos utilizar los **gestores de contraseñas**:
  - Keepass Password Safe, Gorilla Password, KeePassDroid, MiniKeePass
  - https://youtu.be/XEQAMvZoKNA (cómo usar un gestor de contraseñas)
- Para elegir uno de estos gestores tenemos que tener en cuenta:
  - **Reputación** de la aplicación y garantizar que es conocida, segura y tiene buenas referencias.
  - Si perdemos la **clave maestra** será imposible acceder a las claves almacenadas. Memorizar y no escribir.
  - Debemos realizar **copias de seguridad** del fichero de claves

AUTENTICACIÓN: GESTORES DE CONTRASEÑAS

- Los exploradores nos proporcionan gestores de contraseñas.
  - Firefox https://support.mozilla.org/es/kb/administrador-de-contrasenas-recordar-borrar-cambiar-importar-contrase%C3%B1as-firefox#w_managing-usernames-and-passwords
  - Chrome: https://passwords.google.com/
- Cada servicio debe tener una contraseña diferente, así minimizamos las consecuencias de que descubran nuestra contraseña.

POLÍTICA DE CONTRASEÑAS

Una política de contraseñas es un conjunto de normas y requisitos que una organización establece para garantizar que las contraseñas utilizadas por los usuarios sean seguras y difíciles de adivinar o vulnerar.

Su objetivo principal es proteger el acceso a sistemas, redes, aplicaciones y datos frente a accesos no autorizados.

POLÍTICA DE CONTRASEÑAS

Normas básicas:

- No deben ser o contener palabras usuales ni relacionadas con el entorno del usuario, como por ejemplo fecha de nacimiento.
- No deben ser palabras con significado.
- Evitar que el usuario utilice la misma contraseña en varios sitios.
- Cambiar las contraseñas proporcionadas por defecto.

POLÍTICA DE CONTRASEÑAS

Elementos habituales de una política de contraseñas:

- **Longitud mínima:** por ejemplo, al menos 8, 10 o 12 caracteres.
- **Complejidad:** debe incluir una combinación de letras mayúsculas y minúsculas, números y símbolos o caracteres especiales.
- **Caducidad o vigencia:** las contraseñas deben cambiarse cada cierto tiempo (por ejemplo, cada 90 días).
- **Historial de contraseñas:** impide reutilizar las últimas contraseñas usadas.
- **Bloqueo de cuenta:** tras varios intentos fallidos (por ejemplo, 3 o 5), la cuenta se bloquea temporalmente para evitar ataques de fuerza bruta.

POLÍTICA DE CONTRASEÑAS

Elementos habituales de una política de contraseñas:

- **Prohibición de contraseñas comunes o predecibles:** se rechazan contraseñas como “123456”, “password”, “qwerty”, etc.
- **Almacenamiento seguro:** las contraseñas deben guardarse cifradas o con algoritmos de hash, nunca en texto plano.
- **Autenticación adicional (opcional):** puede incluir autenticación multifactor (MFA), añadiendo una capa extra de seguridad.

POLÍTICA DE CONTRASEÑAS

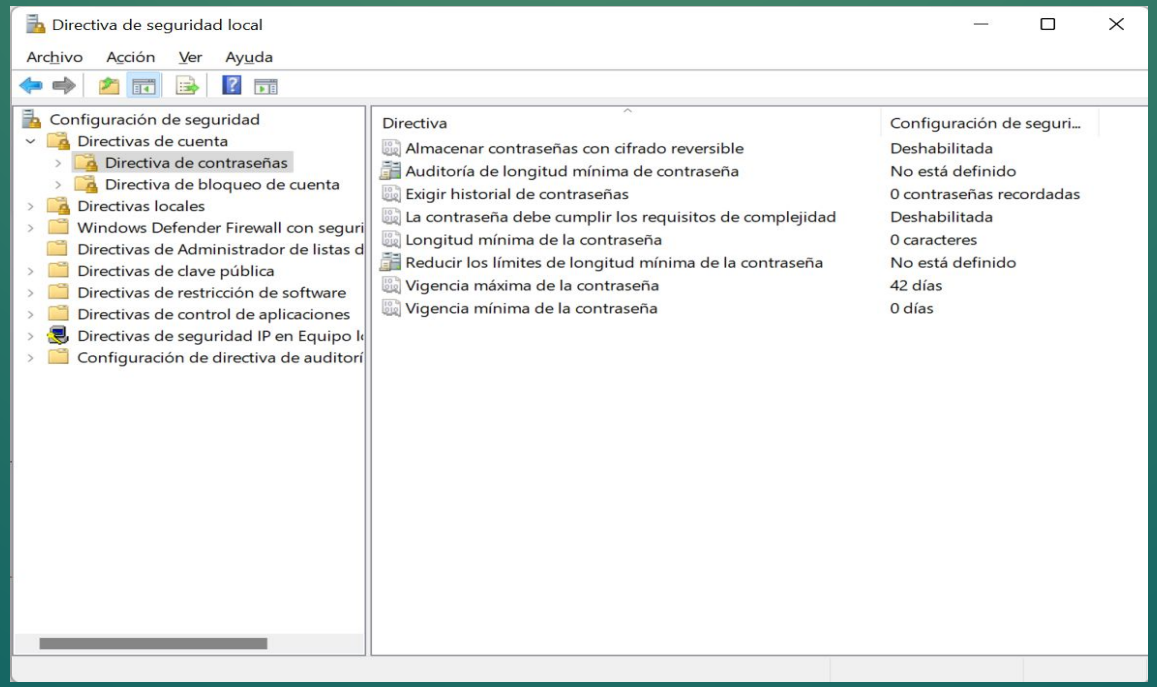
Política creación y duración de las contraseñas:

- ¿Cómo de extensas han de ser? Establecer un mínimo de caracteres.
- ¿Cómo de complejas? Establecer la obligatoriedad o no de caracteres como minúsculas, mayúsculas, números o signos de puntuación.
- ¿Cuánto tiempo ha de pasar para que la contraseña caduque? Establecer la duración de la contraseña. ¿Siempre es bueno cambiarla regularmente? ¿Dónde guardan los usuarios las contraseñas?
- ¿Cuántas contraseñas antiguas debe recordar el sistema?
- ¿Cuántas veces puede equivocarse un usuario? Establecer el número de intentos.

POLÍTICA DE CONTRASEÑAS

Ejemplo de la configuración de la política de contraseñas en Windows 10

Podemos acceder a ella desde las Herramientas administrativas > Directiva de seguridad local > Directiva de cuentas > Directivas de contraseña



GESTIÓN USUARIOS/CONTRASEÑAS EN LINUX

- El fichero /**etc/passwd** contiene la lista de los usuarios locales en el equipo. Si hay una x, la contraseña está cifrada en el fichero /etc/shadow
- El fichero /**etc/group** contiene la definición de los grupos de usuarios y los usuarios que pertenecen a cada uno de ellos.
- El fichero /etc/shadow contiene cada una de las contraseñas cifradas de cada usuario e información sobre su validez.
- La gestión de usuarios en sistemas Linux se apoya en la edición de estos ficheros. Para facilitar las tareas, existen los comandos **useradd, groupadd, usermod, groupmod, userdel, groupdel**, que permitirán crear, modificar y eliminar usuarios y grupos.
- Para adjudicar una contraseña se usa el comando **passwd**

POLÍTICA DE CONTRASEÑAS EN LINUX con passwd

Configurar una contraseña con passwd

Crea una cuenta de usuario llamado jefe_venta. Esta cuenta de usuario debe:

- Esperar a 10 días después de la inserción de una nueva contraseña para poder cambiarla
- Su contraseña será válida durante 60 días.
- Se le avisará 3 días antes de que deba cambiarla.
- Si no cambia la contraseña después de los 60 días, dispone de 7 días antes de que sea bloqueada.

Solución: `passwd -n 10 -x 60 -w 3 -i 7 jefe_ventas`

AUTENTICACIÓN: LOGIN EN EL SISTEMA

- Proceso de autentificarse para ingresar en un sistema.
- Una vez aceptado el login, se asocian permisos y privilegios al usuario.
- Cada usuario debe tener un usuario y contraseña diferente, sus acciones quedan registradas.
- Los administradores deben tener dos usuarios, solo se usa el administrador para funciones de administración.
- En Ubuntu el administrador debe poner sudo para realizar operaciones con el perfil de administrador.
- Si la cuenta de usuario se ve comprometida, el atacante tendrá los permisos del usuario comprometido.

```
usuario@equipo:~$ sudo apt get update
[sudo] password for usuario:
```

AUTENTICACIÓN: VERIFICACIÓN EN DOS PASOS

- **Verificación en dos pasos o de doble factor (two factor authentication)**: requerir del usuario algo que **conoce** (nombre de usuario y contraseña) y algo que **posee** (tarjeta, teléfono móvil, escaneo biométrico) . Dicha prueba puede ser un código generado sobre la marcha y que el usuario debe introducir en la pantalla de *login* o un enlace sobre el que el usuario debe pulsar.
- Los pagos por Internet, o el acceso a los sistemas bancarios suelen ser ejemplos de este tipo de autenticación. También se puede activar en servicios como los de Google.

AUTENTICACIÓN CENTRALIZADA

- Las redes de ordenadores (LAN) plantearon, desde sus inicios, el problema de la administración de usuarios.
- Inicialmente los administradores debían **replicar la base de datos de usuarios** en todos los equipos por dos motivos:
  - Un usuario podría querer o necesitar iniciar sesión en cualquiera de los equipos.
  - El almacenamiento compartido debía conocer todos los usuarios para poder asignar correctamente permisos de acceso a los datos .
- Esto suponía grandes problemas de mantenimiento: altas y bajas de usuarios, cambios de contraseña, etc… Por ese motivo, se crearon métodos de **gestión centralizada de los usuarios** de modo que:
  - El administrador solo mantenía una única base de datos de usuarios y grupos.
  - Todos los equipos confrontaban las credenciales del usuario que iniciaba sesión con esa base de datos centralizada.

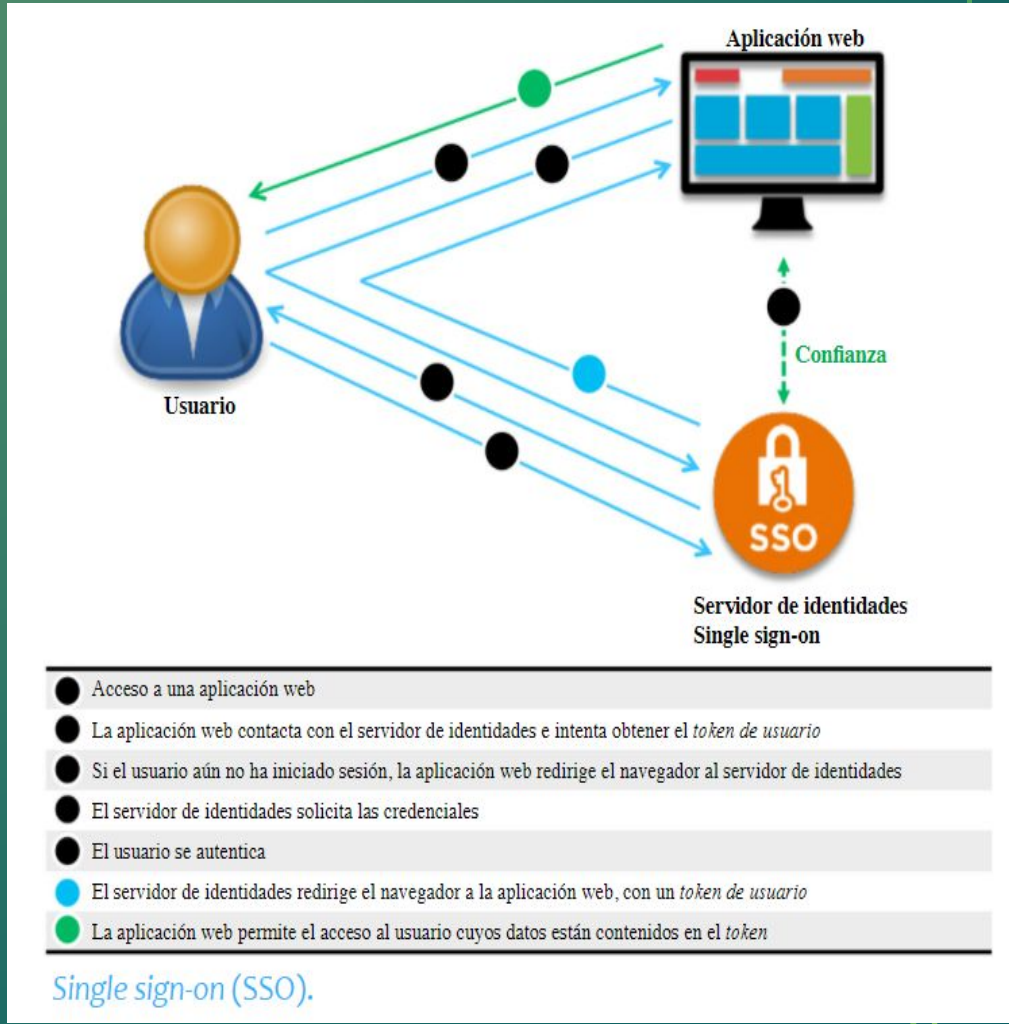
AUTENTICACIÓN CENTRALIZADA

Ejemplos prácticos de autenticación centralizada:

- Windows: Active directory
- Linux: PAM (*Pluggable Authentication Modules*)
- LDAP
- Kerberos
- RADIUS

AUTENTICACIÓN: SINGLE SIGN-ON (SSO)

- El concepto de **Single Sign-On (SSO)** hace referencia a un método gracias al cual, un usuario introduce sus credenciales una única vez, pero accede a diversas aplicaciones que, usualmente, requieren un inicio de sesión independiente.
- Un ejemplo se da en las aplicaciones online de Google: una vez iniciada sesión en una de ellas , Gmail por ejemplo, es posible abrir otras aplicaciones sin tener que volver a introducir la pass. Del mismo modo, al cerrar sesión en cualquiera de ellas coma el resto quedan automáticamente inaccesibles.
- Este método de autentificación requiere de la existencia de un servidor de entidad central, accesibles por todas las aplicaciones relacionadas y en el que todas ellas confían con el cual almacena las cuenta de los usuarios (habitualmente se trata de un servidor LDAP).



Single sign-on (SSO).

AUTENTICACIÓN: LISTAS DE CONTROL DE ACCESO

- Una vez que un usuario ha sido autenticado, el sistema debe darle acceso solo a los recursos a los que ha sido autorizado.
- Para facilitar el trabajo se crean grupos de usuarios, los permisos y privilegio se conceden al grupo y no a cada usuario.
- A cada grupo o usuario se le asocia una lista de control de acceso.
  - **Lectura**: Entrar carpeta/ejecutar fichero, Listar carpeta /leer fichero, Leer atributos, Leer permisos.
  - **Escritura**: Crear ficheros en carpeta / escribir datos, crear carpetas / anexar datos, escribir atributos, Eliminar subcarpetas y ficheros, Eliminar carpeta / fichero.
  - **Ejecución**
  - Otros: tomar posesión, conceder permisos, control total

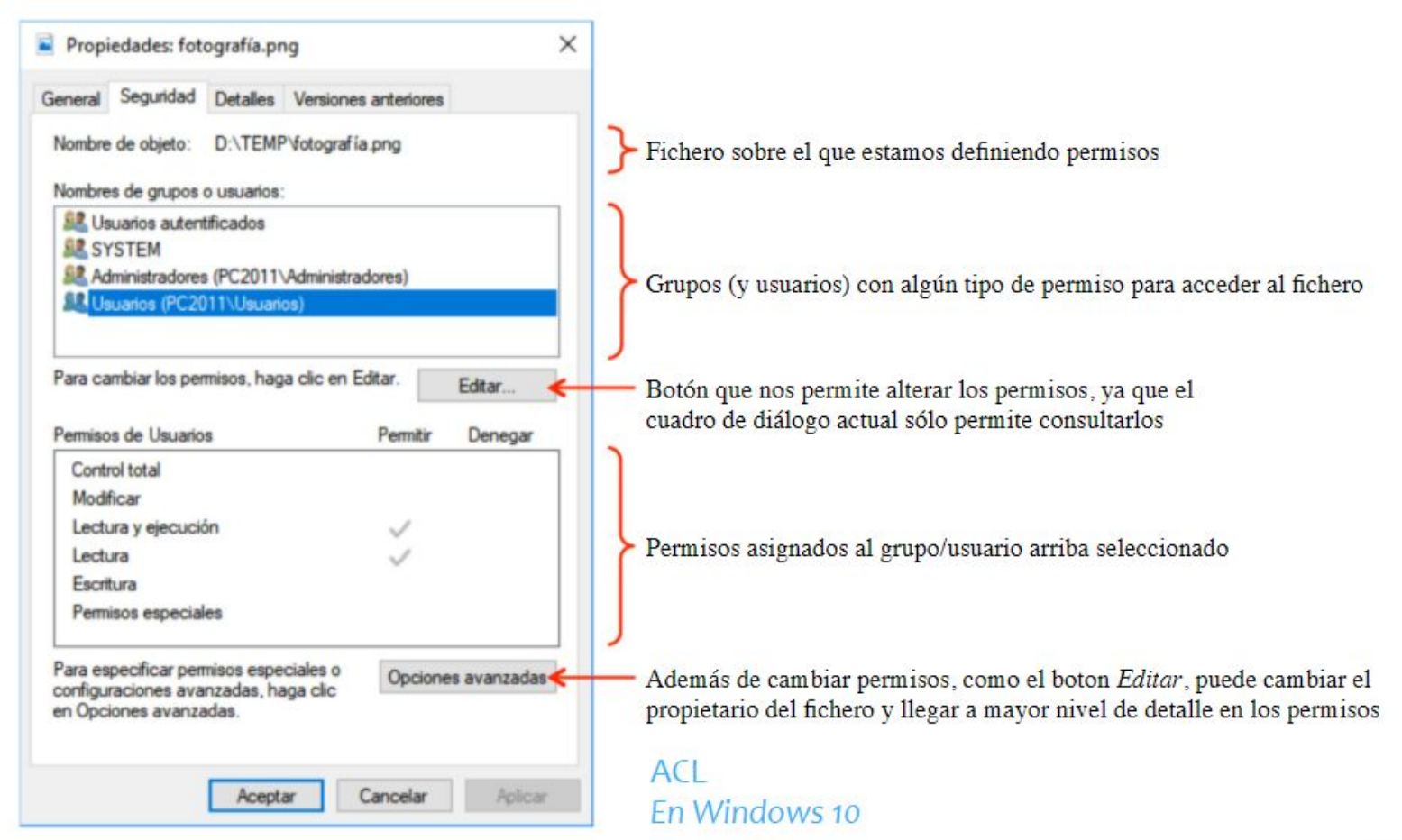
AUTENTICACIÓN: SISTEMAS BIOMÉTRICOS

- Los humanos tenemos ciertas características físicas que nos distinguen inequívocamente a uno de otros, y que pueden ser utilizadas para autentificarnos en sistemas de informáticos.
- Estos sistemas pueden clasificarse en fisiológicos y conductuales
  - Físicos: huella dactilares, el iris y la retina, las facciones del rostro, el olor corporal o la geometría de las orejas.
  - Conductuales: forma en la que realiza una firma manuscrita (analizando su velocidad, aceleración, presión del lápiz, orden de los trazos, etc..), o por la forma de vocalizar una frase (tono, timbre, frecuencia, acento, ritmo,..)
- La principal ventaja de los sistemas biométricos es que no es necesario recordar una contraseña ni portar ninguna tarjeta magnética.

CONTENIDO

- Introducción
- Autenticación
  1. Contraseñas
  2. **Listas de control de acceso (ACL)**
- Amenazas para las contraseñas

AUTENTICACIÓN: LISTAS DE CONTROL DE ACCESO



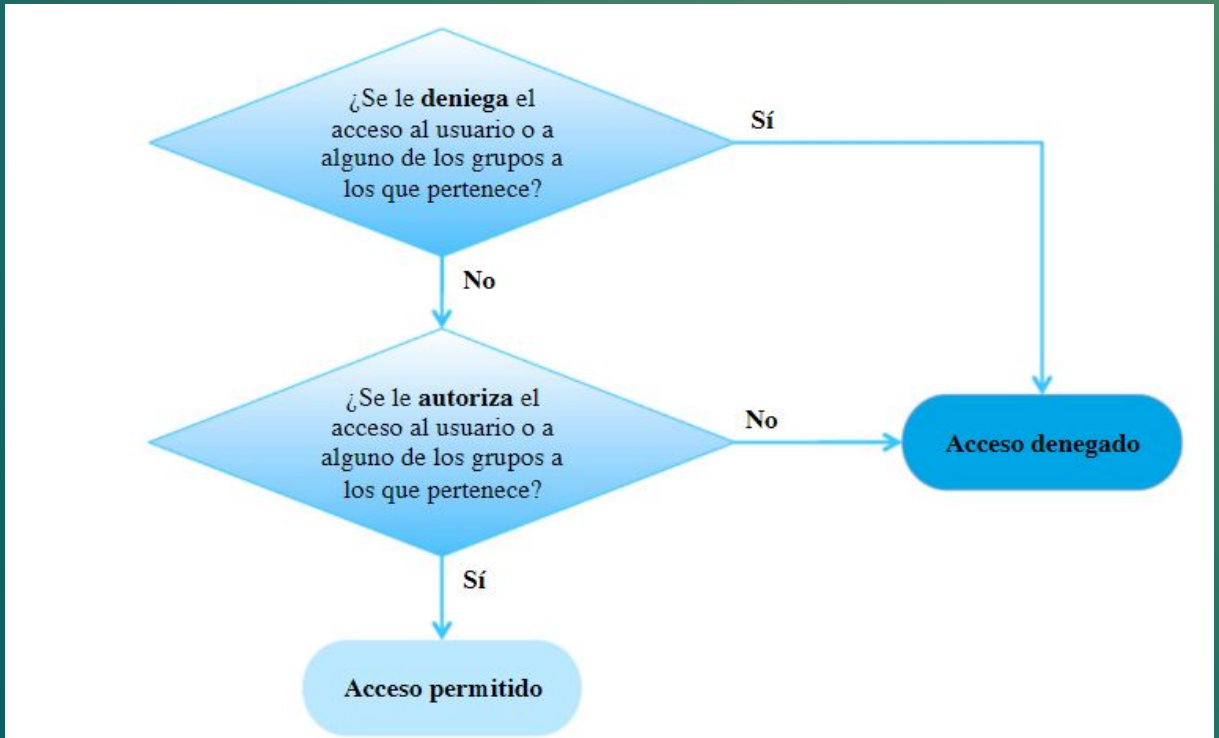
AUTENTICACIÓN: LISTAS DE CONTROL DE ACCESO

Permisos en Linux

Para realizar cambios se utilizan los comandos chown y chmod

AUTENTICACIÓN: LISTAS DE CONTROL DE ACCESO

Principio del funcionamiento de una lista de control de acceso (ACL)



Predominio de la denegación sobre la concesión

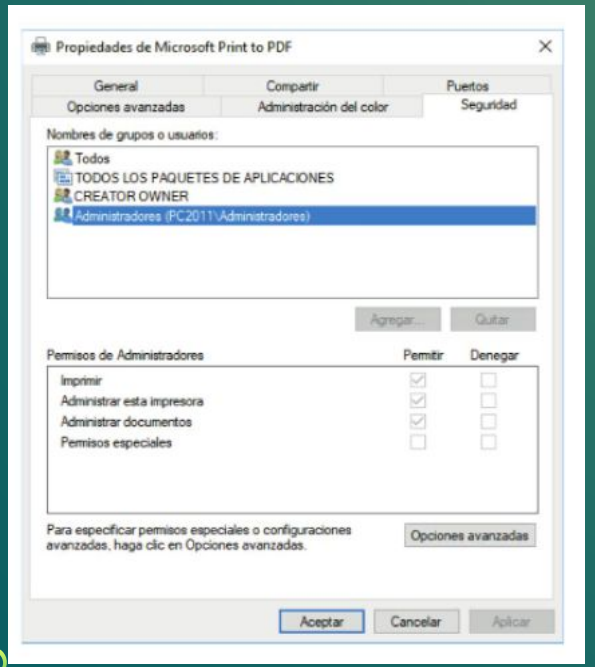
La denegación predomina sobre la concesión.
Ejemplo: tenemos un fichero con la siguiente ACL:

- Grupo “dirección” : permitir lectura.
- Grupo “contabilidad”: denegar lectura.

Si un usuario perteneciera a ambos grupos, no podría leer el fichero, pues la denegación tiene prioridad. Esto recibe el término inglés de ***deny-first*** .

AUTENTICACIÓN: LISTAS DE CONTROL DE ACCESO

Las ACL pueden controlar el acceso a otro tipo de recursos además de los ficheros y directorios como los que se han comentado anteriormente, este tipo de recursos pueden ser: dispositivos externos, impresoras, etc.



ACL de una impresora, con los permisos específicos de este tipo de recurso.

Es responsabilidad del administrador del sistema asignar debidamente los permisos a todos los recursos, no solo a las carpetas y ficheros.

Los sistemas como Linux también definen permisos para otro tipo de recursos, pero lo hacen utilizando el directorio */dev* , donde todos esos recursos están representados en forma de ficheros virtuales.

CONTENIDO

- Introducción
- Autenticación
  1. Contraseñas
  2. Listas de control de acceso (ACL)
- **Amenazas para las contraseñas**

AMENAZAS PARA LAS CONTRASEÑAS

Los sistemas más habituales para averiguar las contraseñas son:

- **Sniffers**: programas que registran la actividad de un equipo informático y pueden interceptar las comunicaciones 'escuchando' para obtener contraseñas.
- **Keyloggers**: programas cuyo fin es capturar las pulsaciones en un teclado para obtener las contraseñas que se han escrito.
- **Ataques por fuerza bruta**: consisten en probar todas las combinaciones posibles de caracteres hasta encontrar la clave que permite acceder al sistema. Cuanto más larga más difícil el acceso
- **Ataques por diccionario**: consisten en generar diccionarios con términos relacionados con el usuario y probarlos como contraseñas. Más eficaces que los ataques por fuerza bruta ya que los usuarios suelen establecer contraseñas en su idioma. A igualdad de longitud, cuanto menos significativa sea, más difícil de detectar
- **Ataques por ingeniería social**: consisten en engañar a los usuarios para que proporcionen sus contraseñas a los intrusos haciéndose pasar por amigos, bancos, etc. Ejemplo: https://youtu.be/z8fZqQQ7TSU

POLÍTICAS DE SEGURIDAD EN MATERIA DE CONTRASEÑAS

Para evitar que las amenazas anteriores sean efectivas es esencial que los usuarios y empresas establezcan políticas de seguridad relativas a las contraseñas.

ESTABLECIMIENTO DE LAS CONTRASEÑAS

- Las contraseñas deben elegirse en función de su idoneidad para proteger la información y no en función de la facilidad para ser recordadas.
- Una política de seguridad adecuada debe prestar atención en fijar unas normas para la elección de contraseñas que dificulten los ataques por diccionario o por fuerza bruta.

POLÍTICAS DE SEGURIDAD EN MATERIA DE CONTRASEÑAS

Para ello, las normas básicas son las siguientes:

- No deben ser o contener palabras usuales ni relacionadas con el entorno del usuario, como nombres de mascotas, fechas de cumpleaños, DNI, etc.
- No deben ser palabras con significado. Debería ser una combinación de mayúsculas, minúsculas, números y otros caracteres. A mayor variedad de símbolos utilizada, mayor dificultad para averiguar la contraseña.
- La longitud de la contraseña debería ser de 8 caracteres como mínimo.
- Hay que evitar que el usuario utilice la misma contraseña en varios sitios; por ejemplo en la empresa, correo personal y redes sociales.
- Se deben cambiar las contraseñas proporcionadas por defecto al registrarse por internet en cualquier servicio.

ALMACENAMIENTO DE LAS CONTRASEÑAS

- No se deben anotar las contraseñas ni en papel ni en archivos de texto plano en el ordenador. Si se quieren almacenar contraseñas en el ordenador, se debe recurrir al uso de programas gestores de contraseñas.
- Cuando se lleva una política de contraseñas robusta, puede ocurrir que se pierda la contraseña del usuario administrador del sistema.
- En el caso de sistemas Linux, es posible regenerarla si se tiene acceso al sistema desde una consola. Para ello basta con reiniciar el sistema y seleccionar el modo de arranque en modo monousuario. Este modo proporciona acceso por consola como usuario root sin necesidad de contraseña, una vez arrancado, se modifica la contraseña de root desde el modo monousuario y se reinicia normalmente.
- Este es un ejemplo de por qué seguridad física y lógica deben ir de la mano.
- Establecer una política segura de contraseñas puede no servir de nada si el atacante tiene acceso físico a la consola del servidor.

PAPEL DEL ADMINISTRADOR DEL SISTEMA

Como administradores de sistemas hay que tomar medidas adicionales para el caso de que los usuarios no cumplan las normas, forzándoles a tomar ciertas medidas de seguridad:

- Establecimiento de un número máximo de intentos para acceder al sistema. Por ejemplo, si el usuario introduce 3 veces seguidas una contraseña incorrecta, el acceso se bloquea y solo puede ser desbloqueado por el administrador.
- Obligar al establecer contraseñas con un mínimo de 8 caracteres alfanuméricos que combinen, al menos, una mayúscula, una minúscula, un número y un signo de puntuación.
- Obligar al usuario a cambiar la contraseña cada cierto tiempo.
- Impedir al usuario repetir las 3 últimas contraseñas utilizadas.
- Las cuentas de usuario permiten al administrador gestionar las contraseñas de un sistema. Estas cuentas permiten conceder permisos y privilegios a cada usuario, el cual solo podrá utilizar los recursos del sistema en función del rol que el administrador le haya asignado.

Las políticas relacionadas con las contraseñas se gestionan, en los sistemas de Windows, desde la consola de Directivas de seguridad local.