

# Seguridad en los Sistemas Informáticos

## Tema 3: Seguridad de los sistemas operativos

Grado en Ingeniería Informática

Departamento de Ingeniería Informática  
Universidad de Cádiz

Curso 2019–2020

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

- 1 Control de acceso al sistema
- 2 Control de acceso a los datos
- 3 Copias de seguridad
- 4 Auditorías

## SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

- ① Control de acceso al sistema
  - Sistemas basados en algo conocido: contraseñas
  - Sistemas de autenticación biométrica
- ② Control de acceso a los datos
  - Modelo de control de acceso
  - Control por niveles de seguridad
- ③ Copias de seguridad
  - ¿Qué debemos copiar?
  - Tipos de copias de seguridad
  - Planificación de las copias de seguridad
- ④ Auditorías
  - Detección de ataques
  - Perfil de usuario
  - Perfil del intruso
  - Acciones puntuales
  - Guía para una auditoría eficiente

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

La seguridad de un sistema debe contemplar 3 aspectos fundamentales:

- Control de acceso al sistema.
- Control de acceso a los datos.
- Administración del sistema y de la seguridad.

Los sistemas operativos suelen proporcionar un mecanismo de control del acceso de los usuarios. Este suele constar de dos pasos:

- 1 Identificación del usuario.
- 2 Autenticación del usuario.

Los métodos de autenticación se suelen dividir en tres grandes categorías:

- 1 Algo que el usuario sabe.
- 2 Algo que el usuario posee.
- 3 Una característica física del usuario (**autenticación biométrica**).

# La elección de las contraseñas

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Principio general

Una buena contraseña debe ser difícil de adivinar (tanto por las personas como mediante métodos automatizados).

## Recomendaciones

- Deben ser lo más largas posible (mínimo 8 caracteres).
- Conviene combinar caracteres numéricos y alfanuméricos, letras mayúsculas, minúsculas y caracteres especiales ( %, \$, &, ... )
- Deben evitarse las palabras de cualquier idioma y los nombres propios.
- No deben utilizarse combinaciones simples de datos personales: iniciales del nombre, fecha de nacimiento, DNI, teléfono, matrícula del coche, etc.
- Utilizar contraseñas fáciles de recordar, para evitar tenerlas apuntadas.
- Son especialmente recomendables los acrónimos de frases que uno recuerde fácilmente.

## Precauciones a tomar por los usuarios

- No compartir nunca su contraseña.
- Cambiarla cada cierto tiempo.
- No escribir ni teclear su contraseña delante de otras personas.
- No enviar la contraseña por correo electrónico.
- Si la contraseña se guarda por escrito, hacerlo en un lugar de difícil acceso para otras personas y de forma que no pueda ser adivinada su función.



## Precauciones a tomar por el administrador

- No debe crear nunca cuentas sin contraseña.
- Cambiar la contraseña después de instalar el sistema.
- Proteger de forma adecuada el fichero del sistema donde se almacenan las contraseñas.
- Vigilar las cuentas de los usuarios accidentales, ya que son las más propensas a la penetración por parte de intrusos.

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Protección automatizada:

- Número limitado de intentos de acceso.
- Control de calidad de las contraseñas.
- Caducidad de contraseñas.
- Generación automática de contraseñas.
- Bloqueo de cuentas.
- Registro de entradas.

# Protección de las contraseñas (cont.)

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Protección del fichero de contraseñas

- Las contraseñas tienen que guardarse cifradas. El método criptográfico utilizado debe ser irreversible para que no sea posible descifrarlas.
- El fichero que contiene las contraseñas no debería ser visible a los usuarios.

## El sistema clásico

- Las contraseñas se guardaban cifradas en el fichero `/etc/passwd` (lectura pública).
- Formato del fichero:  
`login:passwd:UID:GID:varios:dir-entrada:shell`
- Problemas: Se podían adivinar contraseñas comparando palabras de un diccionario cifradas con las almacenadas en el fichero `/etc/passwd`.

# Las contraseñas en UNIX/Linux (cont.)

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Mejora de la seguridad de las contraseñas

- El fichero `/etc/passwd` no contiene la contraseña codificada.
- Esta se encuentra en el fichero `/etc/shadow` que no es de lectura pública.

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

- Pueden utilizar cualquier característica única y mensurable del individuo. Se han utilizado:
  - Iris del ojo.
  - Retina del ojo.
  - Huellas dactilares.
  - Geometría de la mano.
  - Firma.
  - Voz.

## Fases

- 1 **Captura** o lectura de los datos que el usuario presenta para su validación.
- 2 **Extracción** de ciertas características de la muestra.
- 3 **Comparación** de tales características con las guardadas en una base de datos.
- 4 **Decisión** de si el usuario es válido o no.

## Problemas

- |                                 |   |
|---------------------------------|---|
| <b>Tasa de falso rechazo</b>    | Probabilidad de que el sistema de autenticación rechace a un usuario legítimo.  |
| <b>Tasa de falsa aceptación</b> | Probabilidad de que el sistema autentique correctamente a un usuario ilegítimo. |

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Ejercicio 3.1

Si un sistema de autenticación biométrica tiene una tasa de falso rechazo elevada:

- ¿Para quién sería más perjudicial, para los usuarios o para el sistema?
- ¿Y si fuera elevada la tasa de falsa aceptación?



SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

- Determinan qué información puede ser utilizada por cada usuario del sistema.
- Pueden constituir una segunda barrera ante los intrusos que consigan saltarse los mecanismos de control de acceso al sistema.

## Elementos básicos

**Sujeto** Es una entidad capaz de acceder a los objetos. En general, podemos equiparar el concepto de sujeto con el de proceso.

**Objeto** Cualquier recurso cuyo acceso deba controlarse, por ejemplo, ficheros, partes de ficheros, segmentos de memoria, etc.

**Derecho de acceso** La forma en que un sujeto accede a un objeto, por ejemplo, lectura, escritura y ejecución.

	Fichero1	Fichero2	Fichero3
Usuario A	r w	r	
Usuario B		r w	r
Usuario C			r w

## Listas de control de acceso

- Resultan de la descomposición por columnas de la matriz de acceso.
- Existe una por cada objeto del sistema y enumera los usuarios y los derechos de acceso de éstos al objeto.

## Listas de capacidades

- Resultan de la descomposición por filas de la matriz de acceso.
- Hay una por cada sujeto y enumera los derechos de acceso de éste a los objetos del sistema.

## Ejercicio 3.2

- Lea el documento titulado [Uso de listas de control de acceso en Linux](#).
- Indique qué ventajas presenta el sistema de listas de control de acceso sobre el sistema tradicional de bits de protección para los sistemas Linux.

## Acceso discrecional y obligatorio

**Acceso discrecional** Deja en manos de los usuarios la decisión de qué tipos de acceso permite para los ficheros que posee.

**Acceso obligatorio** Es el sistema el que toma todas las decisiones sobre el acceso a los datos basándose en unas reglas fijas y en un esquema de clasificación que establece los niveles de seguridad de los distintos sujetos y objetos que comparten el sistema. Esta política puede ser implementada por medio del denominado **control por niveles de seguridad**.

# Control por niveles de seguridad (cont.)

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

- Es apropiado para organizaciones que tienen requisitos elevados de seguridad y los usuarios operan de modo jerárquico y disciplinado (organizaciones militares, agencias de inteligencia, empresas con altos requisitos de seguridad).
- Cada sujeto y objeto tiene asociada una etiqueta.
- La etiqueta consta de dos partes: **Clasificación** y un conjunto de **Categorías**.
- Ejemplo de etiqueta:  
Secreto [Armas-Químicas Oriente-Medio]

# Control por niveles de seguridad (cont.)

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Niveles de seguridad en entorno militar

- 1 Alto secreto
- 2 Secreto
- 3 Confidencial
- 4 No clasificado

## Niveles de seguridad en entorno empresarial

- 1 Propietario
- 2 Directivo
- 3 Jefe de Departamento
- 4 Empleado
- 5 Público

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Categorías

- Las categorías no son jerárquicas.
- Representan las distintas áreas de información del sistema.
- Ejemplo de categorías en una empresa: Ventas, Personal, Producción, Marketing. . .

## Decisión:

- Etiqueta del sujeto
- Etiqueta del objeto
- Tipo de acceso que se quiere realizar



# Control por niveles de seguridad (cont.)

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Regla de lectura

Para leer un objeto, el nivel de seguridad del sujeto debe ser igual o superior al del objeto y además, el conjunto de categorías del sujeto debe incluir todas las del objeto.

## Regla de escritura

Para poder escribir en un objeto, el nivel de seguridad del objeto debe ser igual o superior al del sujeto y además, el conjunto de categorías del sujeto deben estar incluidas en las del objeto.

## Ejercicio 3.3

Considere los siguientes sujetos de un sistema con sus etiquetas:

**María** Público [Ventas]

**Pedro** Empleado [Ventas Personal]

**Jesús** Directivo [Ventas Marketing]

**Rosa** Propietario [Ventas]

- ¿Cuáles de estos usuarios pueden leer el fichero **Venta03** cuya etiqueta es **Directivo[Ventas Marketing]**?
- ¿Cuáles podrían escribir en el mismo fichero?

# Utilidad de las copias de seguridad

Único mecanismo para recuperar datos perdidos

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Casos en que son necesarias

- Un usuario o un administrador ha borrado de forma no intencionada alguna información que era importante.
- Un intruso ha borrado información importante.
- Fallo de hardware.
- Un robo.
- Desastres naturales: inundación, incendio...

# ¿Qué debemos copiar?

Hay dos tendencias: copiar todo o solo una parte

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Copia completa

Copiamos todos los ficheros del sistema.

**Ventajas** La recuperación del sistema, en caso de tener que recuperarlo completo, es más sencilla.

**Inconvenientes** Consume más recursos (soporte y tiempo).

## Copia parcial

Copiamos aquello que sea específico de nuestro sistema: ficheros de usuarios, ficheros de configuración...

**Ventajas** Consume menos recursos.

**Inconvenientes** Si hay que recuperar todo el sistema, tendremos que empezar instalando el SO, todo el software adicional instalado (más parches...) y, por último, la copia de seguridad.

# Tipos de copias de seguridad

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

## Completas

Copia todos los ficheros de interés.

## Progresivas

Solo se copian aquellos ficheros que han sido creados o modificados desde la última copia completa o progresiva efectuada.

## Diferenciales

Solo se copian los ficheros que han sido creados o modificados desde la última copia completa realizada.

## Contenidos

- Tipos de copias que se van a realizar.
- Ciclos de copia y rotación de soportes.
- Frecuencia.
- Momento en que se van a realizar las copias.

## Otros aspectos a considerar

- Protección.
- Comprobación.
- Recursos para la realización de copias de seguridad.

## Ejercicio 3.4

- Considere los siguientes escenarios:
  - Copias completas y progresivas.
  - Copias completas y diferenciales.
- Explique cómo llevaría a cabo estas acciones en cada caso:
  - Recuperar el sistema completo.
  - Recuperar un fichero individual.

## Concepto de auditoría

Consiste en la monitorización del funcionamiento del sistema de forma automatizada y sistemática mediante el registro de los sucesos clave que se producen en este.

## Objetivos

- Revisar accesos por usuarios a los objetos del sistema.
- Revisar la efectividad de los mecanismos de seguridad del sistema.
- Descubrir intentos de saltarse los mecanismos de seguridad.
- Descubrir usuarios con privilegios excesivos.
- Servir de elemento disuasor para los atacantes.
- Ayudar a la recuperación de desastres informáticos.
- Proporcionar pruebas materiales de los ataques.



## Evento auditable

- Acciones que queremos que queden registradas en el sistema de auditoría.
- Ejemplos: Arranque o parada del sistema, conexión o desconexión de un usuario, cambio de privilegios de acceso a los objetos de un sistema, creación/modificación/borrado de un objeto...

## Información auditable

- Datos relacionados con el evento auditable que pueden ser útiles.
- Ejemplos: Fecha y hora en que se produce el evento, tipo de evento, éxito o fracaso, datos del usuario que lo desencadena...

## Tipos más comunes

- Intentos fallidos de entrada al sistema.
- Suplantaciones.
- Flujos de información prohibidos.
- Obtención de información restringida.
- Caballos de Troya.
- Virus.
- Abuso de recursos.

## Perfil de usuario

- Recoge las acciones que cada usuario realiza normalmente en el sistema.
- Si un intruso utiliza la cuenta de un usuario se puede detectar debido a que se aparta del perfil del usuario.
- Puede avisar de acciones legales que se aparten del perfil.

## Perfil de intruso

- Los intrusos suelen actuar de una forma similar cuando entran en un sistema ajeno: mirar quién está conectado al sistema, examinar el sistema de ficheros, moverse por los directorios tratando de obtener información, no suelen estar conectado mucho tiempo.

## Acciones puntuales

Hay ciertas acciones que por sí mismas denuncian la presencia de un ataque o intento de ataque:

- Intento de acceso a la administración del sistema.
- Intento de explotación de agujeros de seguridad conocidos.
- Uso de herramientas que detectan agujeros de seguridad.
- Uso de órdenes de otros sistemas operativos.

- Disponer de un administrador.
- Parametrizar de forma adecuada el sistema de auditoría:
  - Establecer los eventos y la información auditables.
  - Definir perfiles.
  - Proteger los ficheros de auditoría.
- Compresión y respaldo de los ficheros de auditoría.
- Determinar el método de análisis que se va a realizar sobre los ficheros de auditoría.
- Cuidar las implicaciones de tipo ético.

SSI T3

Grado en  
Ingeniería  
Informática

Control de  
acceso al  
sistema

Control de  
acceso a los  
datos

Copias de  
seguridad

Auditorías

- Uso de listas de control de acceso en Linux: <http://www.escomposlinux.org/iarenaza/articulo-acls/acls-linux-samba.html>
- Comprobador de contraseñas: <https://password.es/comprobador/>
- Tar: <http://www.gnu.org/software/tar/manual/>
- Clonezilla: <https://clonezilla.org>
- Unison: <https://www.cis.upenn.edu/~bcpierce/unison/>