



Pautes i pràctiques de tractament segur de la informació Part IV

PRINCIPIS DE LA SEGURETAT LÒGICA

La seguretat lògica

Consisteix en l'aplicació de barreres i procediments que resguardin l'accés a dades i només permeti l'accés a les persones que estiguin autoritzades per a fer-lo.

Principals amenaces

- ➔ Accés
- ➔ Modificacions no autoritzades a dades i aplicacions

Principi de seguretat lògica

”Tot el que no està permès ha d'estar prohibit”

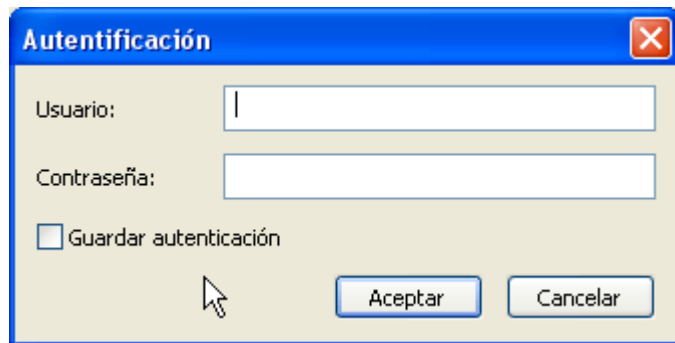
CONTROL D'ACCÉS LÒGIC

Control d'accés lògic

Prevenir l'ingrés de persones no autoritzades a la informació del sistema

El control d'accés comporta dos processos:

- ➔ Identificació: l'usuari es dona a conèixer al sistema
- ➔ Autenticació: verificació que realitza el sistema sobre la identificació



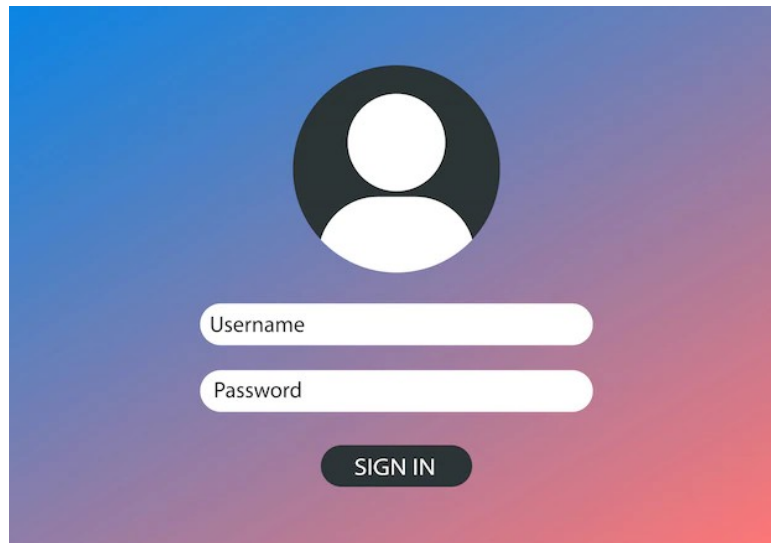
The image shows a standard Windows-style dialog box for authentication. The title bar is blue with the text 'Autenticación' and a red close button. The main area has a light beige background. It contains two text input fields: the first is labeled 'Usuario:' and the second is labeled 'Contraseña:'. Below these fields is a checkbox labeled 'Guardar autenticación'. At the bottom right, there are two buttons: 'Aceptar' and 'Cancelar'. A mouse cursor is pointing at the bottom left of the dialog box.

Identificació vs Autenticació

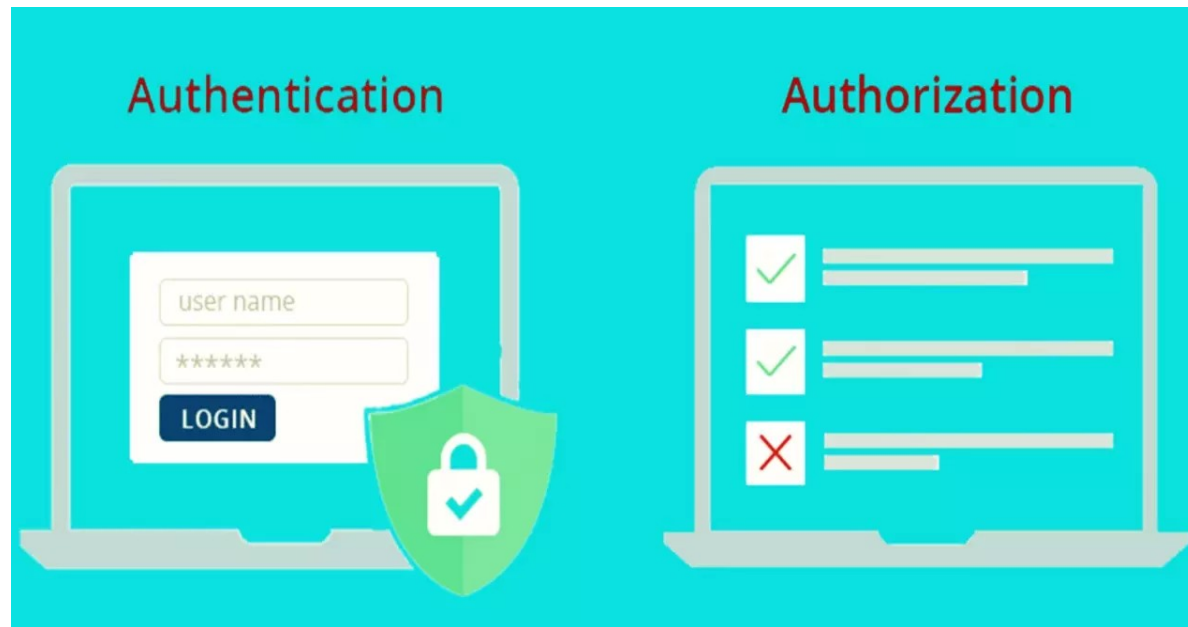
Usuari, password

Targeta , PIN

Petjada dactilar



Autenticació vs Autorització



BIOMETRIA

- **Definició:** Reconeixement inequívoc de persones basat en un o més trets conductuals o físics intrínsecs
- l'«autenticació biomètrica» o «biometria informàtica» és l'aplicació de tècniques matemàtiques i estadístiques sobre els trets físics o de conducta d'un individu, per a la seua autenticació, és a dir, **«verificar» la seua identitat**
- **(estàtiques)** Les empremtes dactilars, la retina, l'iris, els patrons facials,
- **(dinàmiques)** pas, tecleig, veu

Factors d'autenticació

- Alguna cosa que saps: Contrasenya
- Alguna cosa que tens: Token (tg, usb, dispositiu,...)
- Alguna cosa que eres: Tret físic, o dinàmic



- A2F (2FA)
- AMF (MFA)
- TOTP MFA ([video](#))



Algo que sabes

Algo que tienes

Algo que sos

CONTROL D'ACCÉS LÒGIC

Atacs més comuns als sistemes de control d'accés protegits per contrasenyes:

→ **Atac per força bruta:**

- ◆ Esbrinar la clau provant totes les combinacions possibles
- ◆ Quant més curta la clau => menys combinacions=>més senzill desxifrar-la

→ **Atac de diccionari:**

- ◆ Aconseguir la clau provant totes les paraules d'un diccionari o conjunt de paraules comunes
- ◆ No es recomana usar com a clau una paraula del propi idioma perquè sigui fàcil de recordar

Protecció

- Establir un nombre màxim d'intents (eg targetes SIM)
- Polítiques de contrasenyes (forçar característiques de contrasenyes)



CONTROL D'ACCÉS LÒGIC

POLÍTIQUES DE CONTRASENYES

Recomanacions per a contrasenyes segures:

- Establir una **longitud mínima**: cada caràcter augmenta exponencialment el grau de protecció que ofereixen (mínim 8 , convenient 14 o més)
- **Combinació de caràcters**: lletres majúscules, minúscules, números i símbols especials

Exemple de combinacions de força bruta:

- Contrasenya de 5 caràcters en minúscules $(27)^5 = 14.348\ 907$
- Contrasenya de 5 caràcters en minúscules i majúscules $(27 \cdot 2)^5 = 380.204.032$

Saps quant de temps es tarda en trencar la teua contrasenya?

CONTRASENYES FORTES

- Visita la pàgina <https://password.kaspersky.com/es/> i comprova la rapidesa amb la que pot ser trencada una contrasenya de longitud 4,6,8,10.
- Busca altres pàgines web que realitzen la mateixa funció
- Reflexiona: Estan gravant contrasenyes per a afegir-les a llistes de cerca?



kaspersky
password checker

Comprueba tu contraseña

POLÍTiques DE CONTRASENYES

Més recomanacions:

- ➔ No incloure seqüències ni caràcters repetits
- ➔ No utilitzar el nom de l'inici de sessió
- ➔ No utilitzar paraules del diccionari
- ➔ Utilitzar diverses contrasenyes en diferents entorns
- ➔ Evitar l'opció de contrasenya en blanc
- ➔ No revelar la contrasenya a ningú
- ➔ Canviar les contrasenyes amb regularitat



POLÍTIQUES DE CONTRASENYES

Més recomanacions:

<https://pages.nist.gov/800-63-3/sp800-63b.html> (ult act)



- ➔ A partir d'ara això de mesclar estils (majúscules, minúscules, símbols...) i això de canviar la contrasenya periòdicament ja no és una cosa que es considere «segur», entre altres qüestions.
- ➔ Haurien de requerir contrasenyes d'almenys 8 caràcters (15 si pot ser).
- ➔ Haurien d'admetre contrasenyes de fins a 64 caràcters.
- ➔ Haurien d'admetre's espais, caràcters ASCII i Unicode.
- ➔ No haurien d'imposar altres regles de composició («combinació d'estils», com majúsculas/ minúscules/ números).
- ➔ No haurien d'imposar canviar contrasenyes periòdicament, llevat que estiguen compromeses o hi haja hagut algun problema de seguretat concret.
- ➔ No haurien de mostrar «pistes» si no s'està autenticat.
- ➔ No haurien de suggerir contrasenyes o pistes per a canviar la contrasenya del tipus «el nom del teu gos».

POLÍTIQUES DE CONTRASENYES

Pràctica: Vegem quant es tarda en trencar una contrasenya 'feble' en un equip amb poques prestacions !!!!!

En W10: Donar d'alta 8 usuaris amb contrasenyes febles (longitud <7)

(5 minúscules, 5 min-maj 5 min-maj-dig 5 min-maj-dig-simb

6 minúscules, 6 min-maj 6 min-maj-dig 6 min-maj-dig-simb)

Utilitzar el programa Hash Suite per a trencar per força bruta les contrasenyes

<https://hashsuite.openwall.net/>

Observar el temps utilitzat i el conjunt de claus utilitzat

Importar usuaris

Configurar paràmetres d'atac

Trencar contrasenyes

Exportar dades

Executa un Benchmark

POLÍTIQUES DE CONTRASENYES

Pràctica:

En W10: Donar d'alta 4 usuaris amb contrasenyes febles (longitud <7)

Utilitzar el programa John the Ripper per a trencar per força bruta les contrasenyes

<https://www.openwall.com/john/>

Observar el temps utilitzat i el conjunt de claus utilitzat

Pàgina exemple. <https://www.top-password.com/blog/crack-windows-password-with-john-the-ripper/>

Interfície gràfica per a John → Johnnny

<https://openwall.info/wiki/john/johnny>

<https://esgeeks.com/como-usar-johnny-la-gui-john-the-ripper/>

POLÍTIQUES DE CONTRASENYES

Exemples:

John per a extraure contrasenyes d'arxius zip

<https://dfir.science/2014/07/how-to-cracking-zip-and-rar-protected.html>

Contrasenyes d'usuaris en Linux

<https://www.redeszone.net/seguridad-informatica/john-the-ripper-crackear-contrasenas/>

Contrasenyes d'usuaris en Windows

<https://noticiasseguridad.com/tutoriales/john-the-ripper-crackear-contrasenas-de-windows/>

Força bruta sobre pdf, certificats digitals

<https://www.comunixgroup.com/blog/fuerza-bruta-sobre-ficheros/>

- keepass2john.exe
- putty2john.exe
- racf2john.exe
- rar2john.exe
- uaf2john.exe
- wpa2john.exe
- zip2john.exe

- bitlocker2john.exe
- dmg2john.exe
- gpg2john.exe
- hccap2john.exe
- john.exe

- office2john.py
- opcode.py
- openbsd_softraid2john.py
- openssl2john.py
- padlock2john.py
- pcap2john.py
- pem2john.py
- px2john.py
- pgpdisk2john.py
- pgpsda2john.py
- pgpwde2john.py

- kwallet2john.py
- lastpass2john.py
- libreoffice2john.py
- lotus2john.py
- luks2john.py
- mac2john.py
- mac2john-alt.py
- mcafee_epo2john.py
- message.py
- monero2john.py
- money2john.py
- mozilla2john.py

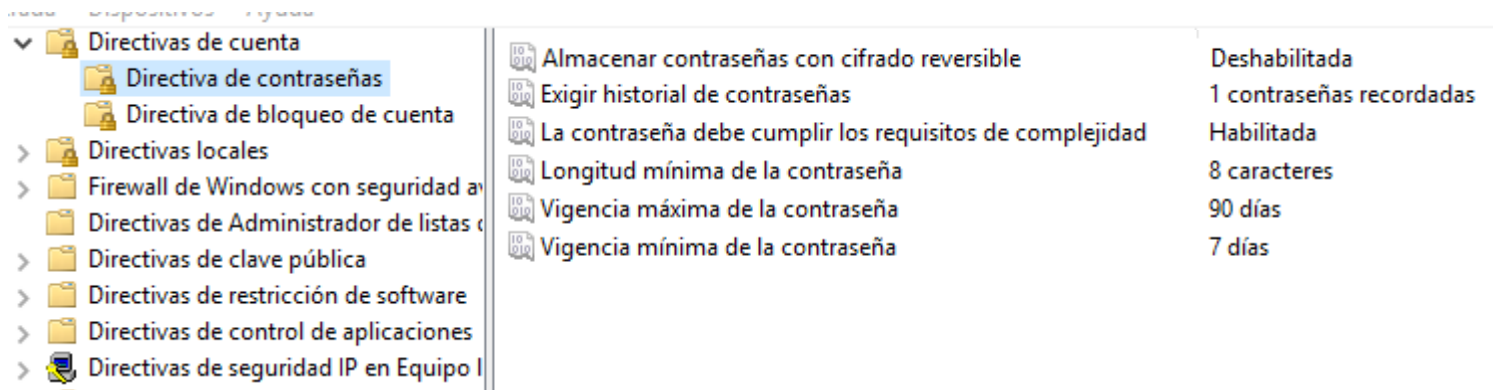
CONFIGURAR CONTRASEÑAS SEGURES

WINDOWS

Les directives de comptes permeten configurar el comportament dels comptes.
Permeten controlar d'una forma eficient la manera d'accedir al sistema.

secpol.msc

Directiva de seguretat de comptes



CONFIGURAR CONTRASENYES SEGURES







WINDOWS

Directives de contrasenyes (realitza la següent configuració en el teu servidor)

- ➔ **No habilitar** emmagatzemar contrasenya usant xifratge reversible.
- ➔ **Forçar l'historial de contrasenyes**: estableix el nombre de contrasenyes a recordar, perquè els usuaris no puguin utilitzar la mateixa contrasenya quan caduca (valor mínim 1)
- ➔ Les contrasenyes han de complir els **requisits de complexitat**
 - ◆ 6 caràcters com a mínim
 - ◆ Contenir almenys tres de les següents classes: majúscules, minúscules, dígit, caràcters no alfanumèrics (!,\$,# o %), altres caràcters unicode
 - ◆ No contenir tres o més caràcters de compte d'usuari

CONFIGURAR CONTRASENYES SEGURES




- **Longitud mínima** de la contrasenya: 8
- **Vigència màxima** de la contrasenya (establir el nombre de dies màxim que una contrasenya va a està activa): 3 mesos
- **Vigència mínima** de la contrasenya (si és major que 0 els usuaris no poden canviar repetidament les contrasenyes per a eludir la directiva forçar contrasenyes):1 setmana

Directiva	Configuración de seguri...
 Almacenar contraseñas con cifrado reversible	Deshabilitada
 Exigir historial de contraseñas	1 contraseñas recordadas
 La contraseña debe cumplir los requisitos de complejidad	Habilitada
 Longitud mínima de la contraseña	8 caracteres
 Vigencia máxima de la contraseña	90 días
 Vigencia mínima de la contraseña	7 días

CONFIGURAR CONTRASENYES SEGURES

Directives de bloqueig de comptes

- ➔ **Durada del bloqueig de comptes** (estableix en minuts el temps que un compte pot estar bloquejada): 30 minuts
- ➔ **Restablir la contrasenya després de** (minuts que ha de passar per a restablir el compte de bloquejos, ha de ser menor que la durada del bloqueig de comptes)
- ➔ **Llindar de bloquejos del compte** (estableix el nombre d'intents fallits per a bloquejar l'accés a un compte)

Directiva	Configuración de seguri...
 Duración del bloqueo de cuenta	15 minutos
 Restablecer el bloqueo de cuenta después de	15 minutos
 Umbral de bloqueo de cuenta	3 intentos de inicio de s...

Crea un nou usuari i comprova que es complixen les restriccions

CONTRASENYES SEGURES LINUX

Servici PAM (Pluggable Authentication Module)

→ Arxius de configuració del comando **passwd**

- ♦ /etc/pam.d/passwd (crida a common-password)
- ♦ /etc/pam.d/common-password

```
/etc/pam.d$ sudo nano common-password
```

Una configuració possible per a contrasenyes segures és:

```
password required pam_unix.so obscure sha512
```

Per a rebaixar requisits, podriem canviar-la per

```
password required pam_unix.so minlen=4 sha512
```

Els efectes actuen immediatament, no fa falta reiniciar ni parar servici

CONTRASENYES SEGURES LINUX

Servici PAM (Pluggable Authentication Module)

- ➔ El mòdul **pam_cracklib** està fet per a determinar si es suficientment forta una contrasenya
- ➔ Per a instal·lar-lo `sudo apt-get install libpam-cracklib`
- ➔ Arxius de configuració del comando **passwd**
 - ◆ `/etc/pam.d/common-password`

Una configuració possible per a contrasenyes segures és: (s'afegeix automàticament al fitxer `common-password`)

```
password required pam_cracklib.so retry=3 minlen=8 difok=3
```

Podem personalitzar les restriccions amb:

```
lcredit=0 ucredit=1 dcredit=1 ocredit=2
```

Que significa esta configuració ?

CONTRASENYES SEGURES LINUX

Servici PAM (Pluggable Authentication Module)

- ➔ Edita el fitxer `/etc/pam.d/common-password` i afegix les següents restriccions
 - ♦ La contrasenya ha de contenir almenys 2 dígit
 - ♦ La contrasenya ha de contenir almenys 1 majúscula
- ➔ Crea un nou usuari amb el comando **adduser**
- ➔ Canvia la contrasenya de l'usuari i comprova que es compleixen les restriccions

Per a verificar els accessos al sistema i altres successos es guarden en arxius situats en la carpeta `/*var/*log`. La identificació d'usuaris la podem veure en

➔ `/var/log/auth.log`

```
GNU nano 2.9.3          auth.log.1
Sep 17 06:23:51 server sudo: pam_unix(sudo:session): session opened for user root by administrador($
Sep 17 06:23:53 server sudo: pam_unix(sudo:session): session closed for user root
Sep 17 06:24:00 server sudo: administrador : TTY=tty1 ; PWD=/usr/local/src/rkhunter-1.4.6 ; USER=root
Sep 17 06:24:00 server sudo: pam_unix(sudo:session): session opened for user root by administrador($
Sep 17 06:25:01 server CRON[3322]: pam_unix(cron:session): session opened for user root by (uid=0)
```

CONTRASENYES SEGURES LINUX

Servici PAM (Pluggable Authentication Module)

Caducitat de contrasenyes. /etc/login.defs

/etc/default/useradd **INACTIVE=**

```
PASS_MAX_DAYS    99999
PASS_MIN_DAYS     0
PASS_WARN_AGE     7
```

Encara que això és una directiva per a la creació d'usuaris.

Cada usuari porta la seva pròpia caducitat codificada en `etc/shadows`

Per a canviar la caducitat a un usuari utilitzarem el comando **chage**

```
$ chage -l <usuari>
```

```
Último cambio de contraseña          : nov 11, 2020
La contraseña caduca                  : nunca
Contraseña inactiva                   : nunca
La cuenta caduca                      : nunca
Número de días mínimo entre cambio de contraseña : 0
Número de días máximo entre cambio de contraseña : 99999
Número de días de aviso antes de que caduque la contraseña : 7
```


CONTRASENYES SEGURES LINUX

Servici PAM (Pluggable Authentication Module)

Caducitat de contrasenyes

Si volem que les claus hagin de canviar-se -per exemple- cada 80 dies(M), amb un avís previ de 7 dies(W), 10 dies de gràcia una vegada vençuda la clau(I) i un dia d'espera abans de tornar a canviar la clau(m), usem el següent comando per cada usuari existent:

```
# sudo chage -M 80 -W 7 -I 10 -m 1 <usuari>
```

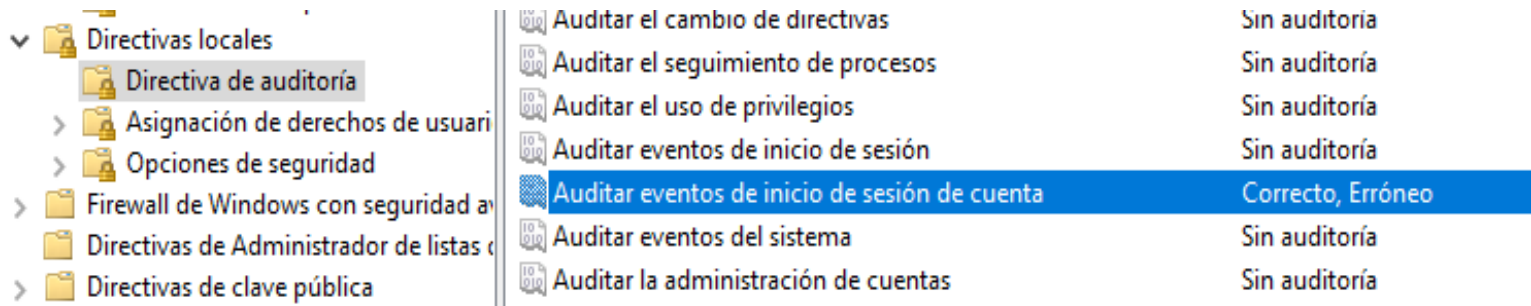
Això farà que molts usuaris quedin automàticament bloquejats perquè van canviar la seva clau fa més que 90 (80 + 10) dies. Solució: Forcem la data d'últim canvi a una data recent, idealment just perquè estiguin obligats a canviar la clau en el pròxim *login.

```
# sudo chage -d 2020-11-1 <usuari>
```

CONFIGURAR AUDITORIA

Control d'accessos indeguts

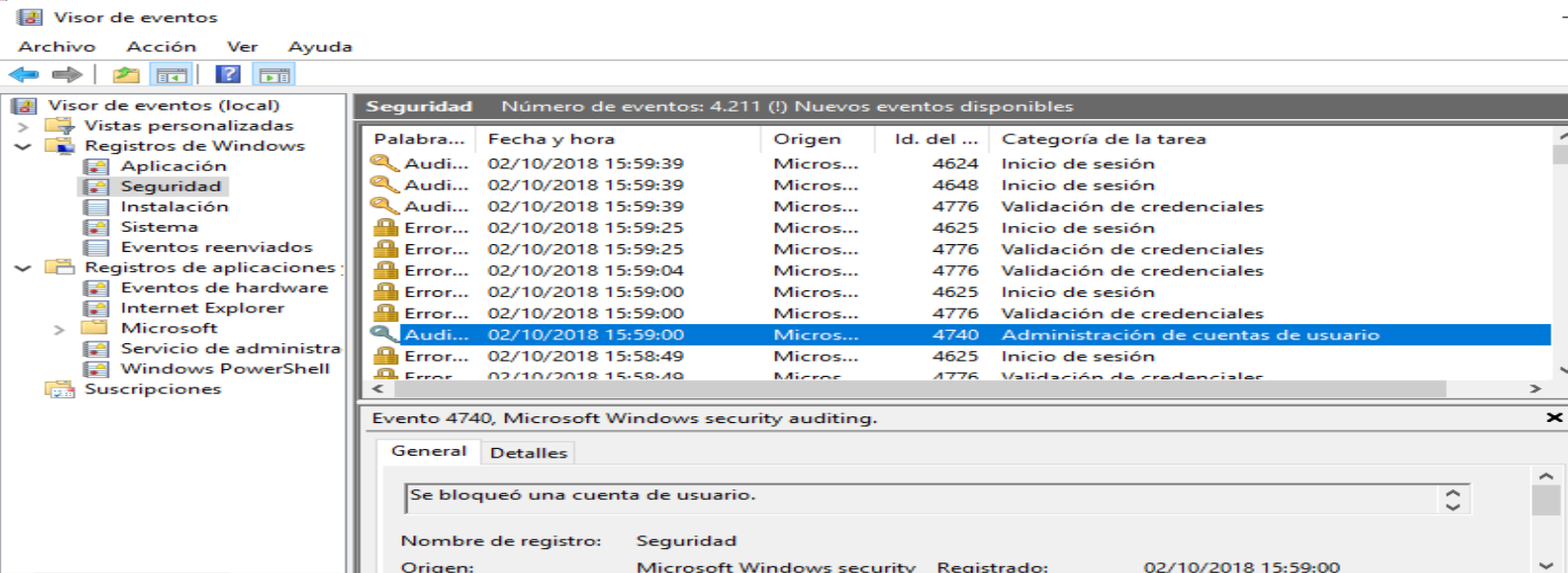
Per a controlar per part de l'administrador els accessos podem habilitar en *Directives locals/directiva auditoria /auditar successos d'inici i fi de sessió de compte*



CONFIGURAR AUDITORIA

Visor d'esdeveniments

En l'apartat de seguretat comprovar que s'ha bloquejat el compte



Visor de eventos

Archivo Acción Ver Ayuda

Visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
 - Aplicación
 - Seguridad
 - Instalación
 - Sistema
 - Eventos reenviados
- Registros de aplicaciones:
 - Eventos de hardware
 - Internet Explorer
 - Microsoft
 - Servicio de administr...
 - Windows PowerShell
- Suscripciones

Seguridad Número de eventos: 4,211 (!) Nuevos eventos disponibles

Palabra...	Fecha y hora	Origen	Id. del ...	Categoría de la tarea
Audi...	02/10/2018 15:59:39	Micros...	4624	Inicio de sesión
Audi...	02/10/2018 15:59:39	Micros...	4648	Inicio de sesión
Audi...	02/10/2018 15:59:39	Micros...	4776	Validación de credenciales
Error...	02/10/2018 15:59:25	Micros...	4625	Inicio de sesión
Error...	02/10/2018 15:59:25	Micros...	4776	Validación de credenciales
Error...	02/10/2018 15:59:04	Micros...	4776	Validación de credenciales
Error...	02/10/2018 15:59:00	Micros...	4625	Inicio de sesión
Error...	02/10/2018 15:59:00	Micros...	4776	Validación de credenciales
Audi...	02/10/2018 15:59:00	Micros...	4740	Administración de cuentas de usuario
Error...	02/10/2018 15:58:49	Micros...	4625	Inicio de sesión
Error...	02/10/2018 15:58:49	Micros...	4776	Validación de credenciales

Evento 4740, Microsoft Windows security auditing.

General Detalles

Se bloqueó una cuenta de usuario.

Nombre de registro: Seguridad

Origen: Microsoft Windows security Registrado: 02/10/2018 15:59:00

POLÍTICA D'USUARIS I GRUPS

Tasques de l'administrador

- ➔ Definir comptes d'usuari, assignar-les a perfils determinats, grups o rols
- ➔ Assignar privilegis sobre els objectes del sistema
- ➔ Determinar el nivell de seguretat de les dades i aplicacions
 - ◆ Classificar la informació
 - ◆ determinar el risc davant l'accés d'usuaris no autoritzats

CONTROL D'ACCÉS MITJANÇANT CONTRASENYES

Nivells dels mecanismes de control d'accés

- **1r nivell**: control de contrasenya d'arrencada i de la pròpia configuració de la **BIOS**
- **2n nivell**: Contrasenya de l'arrencada i de l'edició d'opcions proporcionades pels **gestors d'arrencada**
- **3r nivell**: control mitjançant usuari i contrasenya per part del **sistema operatiu**. El SO permet el control d'accés a dades i aplicacions mitjançant la configuració de privilegis als diferents perfils d'usuari o individualment a aquests
- **4t nivell**: Contrasenya i xifratge d'accés **dades i aplicacions**.

PERILLS DISTRIBUCIONS LIVE

Sistemes operatius en mode live

Arrancables des d'unitats extraïbles USB, CD, DVD) sense necessitat de formatar i instal·lar-los en el disc dur. Inclouen gran quantitat d'aplicacions de recuperació de dades i contrasenyes d'usuari.

Exemples de distribucions arrancables en manera Live

- ➔ **Ultimate Boot CD** (UBCD). Conté utilitats freeware per a Windows per a reparar, restaurar i diagnosticar diversos problemes informàtics.
- ➔ **Backtrack**. Conté eines d'auditories de seguretat Windows i GNU/Linux.
- ➔ **Ophcrack**. Conté l'aplicació amb el mateix nom per a extreure contrasenyes en Windows.
- ➔ **Slax**. Permet el muntatge i l'accés als sistemes de fitxers instal·lats en disc
- ➔ **Wifiway i wifislax**. Distribucions orientades a realitzar auditories wireless com a recuperació de contrasenyes



Aquestes distribucions poden accedir a les particions i fitxers de manera transparent pel que poden comprometre la seguretat de les dades i fitxers

CONTROL D'ACCÉS EN LA BIOS

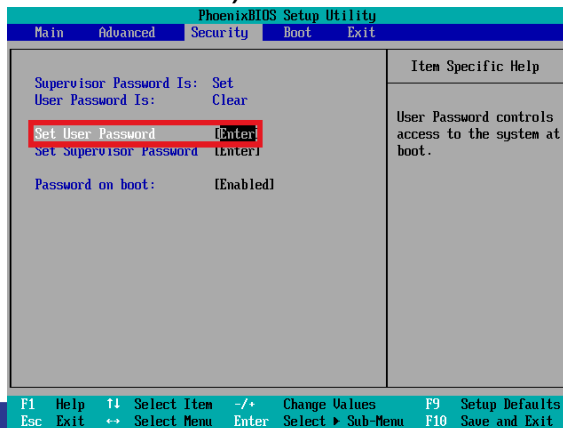
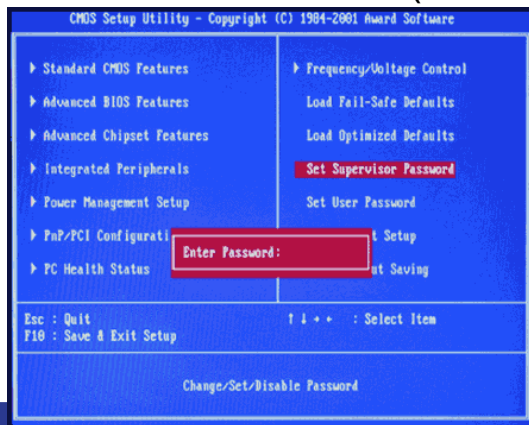
BIOS (Basic Input/Output System)

- ➔ Xicotet programa que es troba gravat en una memòria de la placa base. Guarda la configuració del nostre sistema
- ➔ Reconeix i localitza tots els dispositius necessaris per a carregar el sistema operatiu en la memòria RAM
- ➔ Important protegir la BIOS perquè només un Administrador o un usuari responsable puguin canviar valors de configuració

CONTROL D'ACCÉS EN LA BIOS

Segons els nivells de seguretat es poden classificar en :

- ➔ **Seguretat del sistema** (system): En cada arrencada del sistema ens demanarà que introduïm una contrasenya que prèviament s'ha configurat en la *BIOS. En cas que no sigui correcta el sistema no arrenca
- ➔ **Seguretat de configuració de la BIOS** (setup): Se solen distingir dos rols;
 - ◆ **Usuari** (sols lectura)
 - ◆ **Administrador** (lectura/modificacions):



CONTROL D'ACCÉS EN LA BIOS

Vulnerabilitats de la BIOS

1. ***Es pot reinicialitzar i tornar als seus valors de fàbrica*** (les contrasenyes, per tant desapareixeran) llevant la pila o a través del jumper CLR_CMOS

Recomanació: Protecció d'accés físic a la placa base (la forma més senzilla, amb cademat que assegure l'obertura de la torre i no permeta l'accés a la placa base

2. ***Es pot accedir i canviar la seva configuració*** si no està protegida per contrasenya

Recomanació: Sol·licitar cada vegada que s'arrenqui la màquina (setup) Si no s'introdueix correctament, el sistema no arrencarà.

3. ***Distribucions Live***

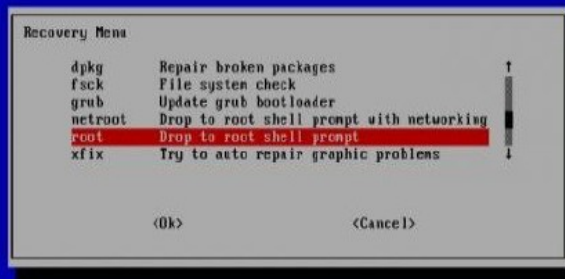
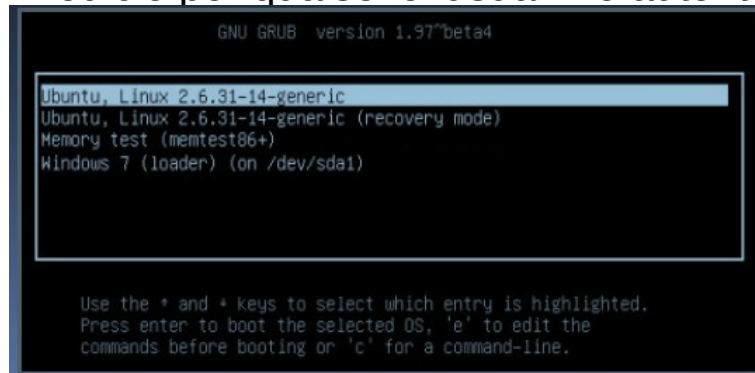
Recomanació: Establir com a primer dispositiu d'arrencada el disc dur on es troba els SO (system)

+ contrasenya BIOS

CONTROL D'ACCÉS AL GESTOR D'ARRANCADA

GRUB

- ➔ Gestor d'arrencada que permet seleccionar amb quin sistema operatiu arrencar quan tenim instal·lat diversos sistemes operatius en el disc dur
- ➔ Opció **recovery mode** per a la recuperació en cas de fallada del sistema. Pot modificar contrasenyes o accedir a la informació del disc dur
- ➔ **Recomanació**: Afegir **contrasenya encriptada** al menú d'edició (és a dir, impossibilitar l'edició per qualsevol usuari no autoritzat) i al **mode recuperació**



CONTROL D'ACCÉS AL GESTOR D'ARRANCADA

Aprofitar el gestor d'arrancada no securitzat (grub)

- ➔ Arrancar amb privilegis sense saber cap usuari ni contrasenya del sistema
- ➔ Realitzar modificacions significatives en el sistema

Pràctica

Utilitza grub per a arrancar en mode administrador (root)

<https://byte-mind.net/obtenir-acceso-root-desde-grub-linux/>

NOTA: Canvia la password de root, afegix un usuari amb privilegis

Activar grub en maquina virtual !!!

sudo nano /etc/default/grub

sudo update-grub

reboot

CONTROL D'ACCÉS AL GESTOR D'ARRANCADA

Afegir contrasenya encriptada al grub

- Impossibilita l'edició per qualsevol usuari no autoritzat
- Afegir usuaris en el fitxer `/etc/grub.d/00_header`

Pràctica

Realitza els passos de l'1 al 4 del següent enllaç

<https://geekland.eu/proteger-el-grub-con-contrasena/>

NOTA: Afegix un usuari amb contrasenya i altre sense

CONTROL D'ACCÉS EN EL SISTEMA OPERATIU

Mètodes d'accés

- ➔ Més segur: petjada digital
- ➔ Més usat : usuari i contrasenya

Vulnerabilitats

- ➔ Accés mitjançant la manera de recuperació (GNU/Linux) o a manera de prova de fallades (Windows)
- ➔ Arrencar amb una distribució Live per a recuperar/esborrar/modificar contrasenyes

Recomanacions:

- ➔ Ús d'eines d'auditoria de sistemes d'accés i nivell de fortalesa de contrasenyes
- ❖ **Ophcrack** (Windows)
- ❖ **John the Ripper** (GNU/Linux)

RECUPERACIÓ DE CONTRASENYES WINDOWS

Ophcrack

És una aplicació que permet recuperar contrasenyes de Windows. Es basa en el coneixement de com emmagatzema Windows les seves contrasenyes d'usuari (normalment en [windows/system32/config/SAM](#) (només accessible si s'arrenca l'equip amb una distribució Live). Empra una comprovació mitjançant força bruta i diccionaris que caldrà carregar depenent de la versió i l'idioma

Recomanació: **Ophcrack** té grans dificultats amb paraules separades amb espais i caràcters especials, per la qual cosa es recomana el seu ús
Altra defensa es la utilització del xifrat de disc (del SO)

[Ophcrack per a recuperar la contrasenya de Windows](#)

RECUPERACIÓ DE CONTRASENYES GNU/LINUX

- ➔ En **GNU/Linux** l'arxiu que controla usuaris i les seves contrasenyes encriptades és ***/etc/shadow*** visible tan sols per a l'usuari root

```
pollinate.*:17737:0:99999:7...  
sshd.*:17737:0:99999:7:::  
administrador:$6$X9i2CpK1MQ.aGtBL$IwojJynaXfRhIdmJODTQSmBI6AcJN8q1QsRpx2Ir/n6h.ItSUdfY5831qKMLSjk23$  
adela:$6$LjiP7r52$vjWV3zHfHuHTL1ci2vIgMoXzIM8Y7sXnnANB/dcDuB8djfbGT1j0jqThFczkVmFvD.AFL5QCmLY1axIM1$  
[ Read 31 lines ]
```

Recuperar la contrasenya amb [John the ripper](#)

MODIFICACIÓ DE CONTRASENYES

WINDOWS

- Totes les utilitats requereixen arrencar des d'una distribució live
- **'Ultimate Boot CD for Windows' o 'UBCD4Win'** és un CD de recuperació d'arrancada (Live CD) que conté programari utilitzat per a reparar, restaurar i diagnosticar diversos problemes informàtics.

GNU/Linux

- Si podem accedir al sistema de fitxers i modifiquem en **/etc/shadow** la contrasenya actual per una altra encriptada que coneguem podrem accedir amb la nova contrasenya
- A tenir en compte:
 - ♦ Hem de conèixer l'algorisme de xifratge (buscar en el fitxer **/etc/pam.d/common-password** la línia corresponent al mòdul **pam_unix.so**)
 - ♦ Emprar una ferramenta de xifrat

AMENAÇA: Keyloggers

TIPUS

- Entrada amb un Phishing
- Extensió d'un navegador
- Dispositiu Maquinari
- Enregistrador de teclat CSS (visitant una pàgina web)



Instal·la i prova l'extensió Fea KeyLogger en Chrome

RESUM

- ✓ **Mantingues el Sistema Operatiu actualitzat**
- ✓ **Instal·la antivirus i mantén-lo actualitzat (també plugins de seguretat en navegadors)**
- ✓ **Mantingues les aplicacions actualitzades**
- ✓ **Estableix una bona política de contrasenyes, i mantén-les secretes**
- ✓ **Estableix contrasenyes a tots els nivells (bios, arrencada, SO, aplicacions)**
- ✓ **Considera la utilització de mètodes d'accés alternatius o complementaris (petjada)**
- ✓ **Utilitza usuari amb privilegis SOLAMENT quan siga necessari**
- ✓ **Considera la utilització de xifratge de dades (partició, carpetes, arxius)**

RESUM

- ✓ **Considera la utilització d'eines d'esborrat segur**
- ✓ **Considera l'ús de gestor de contrasenyes**
- ✓ **Realitza escanejos periòdics de vulnerabilitats dels teus sistemes**
- ✓ **Desinstal·lar serveis no utilitzats (rdp, vnc, telnet, ssh, ...)**
- ✓ **Desinstal·lar aplicacions no utilitzades.**
- ✓ **Considera utilitzar un EDR (empresa)**
- ✓ **<https://geekflare.com/es/edr-tools/>**