



GUIA DE GESTIÓ DE CONTRASENYES

Índex

3 . . . Qui fem aquesta guia

5 . . . I aquesta guia, per a qui és?

5 . . . I aquesta guia, què busca?

6 . . . Aspectes legals i normatius

7 . . . Introduint les idees bàsiques

7 . . . Qui no ha fet servir mai una contrasenya?

8 . . . Perills que podem córrer amb contrasenyes dèbils

8 . . . Per què les contrasenyes ja existents en
equips que provenen de fàbrica són vulnerables?

8 . . . Estrenant ordinador

8 . . . Què pot passar si no canviem les
contrasenyes que provenen de fàbrica?

8 . . . Accés no autoritzat

8 . . . Denegació de servei

9 . . . Reencaminament de les comunicacions

9 . . . Pèrdua d'informació confidencial

9 . . . Per què cal definir una contrasenya robusta personalitzada?

9 . . . En quins escenaris desagradables
ens podem trobar?

9 . . . Pèrdua d'informació confidencial

9 . . . Suplantació d'identitat

9 . . . Idoneïtat en la utilització del desafiament pregunta/resposta

9 . . . Com es diu la teva àvia?

10 . . . En quins escenaris desagradables
ens podem trobar?

10 . . . Accés no autoritzat

10 . . . Suplantació d'identitat

10 . . . Utilització de comptes d'accés genèrics corporatius

10 . . . Contrasenyes sabudes per uns quants

10 . . . En quins escenaris desagradables
ens podem trobar?

10 . . . Accés no autoritzat

10 . . . Pèrdua d'informació confidencial

11 . . . Utilització de mecanismes de rotació de contrasenyes

11 . . . Exercitar la ment per a la seguretat de
la nostra informació

11 . . . En quins escenaris desagradables
ens podem trobar?

12 . . . Recomanacions

12 . . . Recomanacions per construir
contrasenyes robustes

12 . . . Recomanacions per preservar la privacitat
de les contrasenyes

13 . . . Recomanacions per preservar la vigència
de les contrasenyes

16 . . . Conclusions

17 . . . Glossari

17 . . . Referències i enllaços web

18 . . . Eines

18 . . . Recursos de suport en línia

Qui fem aquesta guia

El Centre de Seguretat de la Informació de Catalunya, CESICAT, és l'organisme executor del Pla nacional d'impuls de la seguretat TIC aprovat pel govern de la Generalitat de Catalunya el 17 de març de 2009. La missió d'aquest pla és la de garantir una Societat de la Informació Segura Catalana per a tots. Amb aquesta finalitat, es crea el CESICAT com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

La forma jurídica del CESICAT és la de "fundació del sector públic de l'administració de la Generalitat".

Amb l'objectiu de proporcionar unes bones pràctiques i uns coneixements mínims en seguretat de la informació, el CESICAT ofereix com a servei preventiu un conjunt de guies de seguretat adreçades a ciutadans, empreses, administracions públiques i universitats.

www.cesicat.cat

El Pla nacional d'impuls de la seguretat TIC a Catalunya s'estructura al voltant de quatre objectius estratègics principals que seran desenvolupats pel CESICAT:

- Executar l'estratègia nacional de seguretat TIC establerta pel Govern de la Generalitat de Catalunya
- Donar suport a la protecció de les infraestructures crítiques TIC nacionals
- Promocionar un teixit empresarial català sòlid en seguretat TIC
- Incrementar la confiança i protecció de la ciutadania catalana en la societat de la informació.

El contingut de la present guia és titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya i resta subjecta a la llicència de Creative Commons BY-NC-ND. L'autoria de l'obra es reconeixerà mitjançant la inclusió de la següent menció:



Obra titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya.


Llicenciada sota la llicència CC BY-NC-ND.

La present guia es publica sense cap garantia específica sobre el contingut.





L'esmentada llicència té les següents particularitats:


Vostè és lliure de:

 Copiar, distribuir i comunicar públicament la obra.

Sota les condicions següents:

 **Reconeixement:** S'ha de reconèixer l'autoria de la obra de la manera especificada per l'autor o el llicenciador (en tot cas no de manera que suggereixi que gaudeix del seu suport o que dona suport a la seva obra).

 **No comercial:** No es pot emprar aquesta obra per a finalitats comercials o promocionals.

 **Sense obres derivades:** No es pot alterar, transformar o generar una obra derivada a partir d'aquesta obra.

Respecte d'aquesta llicència caldrà tenir en compte el següent:

■ **Modificació:** Qualsevol de les condicions de la present llicència podrà ser modificada si vostè disposa de permisos del titular dels drets.

■ **Altres drets:** En cap cas els següents drets restaran afectats per la present llicència:.

■ Els drets del titular sobre els logots, marques o qualsevol altre element de propietat intel·lectual o industrial inclòs a les guies. Es permet tan sols l'ús d'aquests elements per a exercir els drets reconeguts a la llicència.

■ Els drets morals de l'autor.

■ Els drets que altres persones poden tenir sobre el contingut o respecte de com s'empra la obra, tals com drets de publicitat o de privacitat.

Avis: En reutilitzar o distribuir la obra, cal que s'esmentin clarament els termes de la llicència d'aquesta obra.

El text complert de la llicència pot ser consultat a <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca>.

Introducció

I aquesta guia, per a qui és?

Aquesta guia està dirigida a usuaris d'universitats i centres de recerca, administracions públiques catalanes i pimes que utilitzen uns serveis telemàtics dins l'entorn professional que requereixen l'ús de contrasenyes d'accés.

Aquesta guia també està pensada per als administradors de sistemes, ja que ells són els encarregats de configurar els perfils d'accés i les polítiques de seguretat en els sistemes d'informació.

Els responsables de seguretat d'empreses i organitzacions la poden fer servir per conscienciar els treballadors i les persones de l'entitat en general sobre la importància de gestionar les contrasenyes de manera correcta.

Les organitzacions que en un futur pròxim vulguin implantar un Sistema de Gestió per a la Seguretat de la Informació (SGSI), poden tenir en compte les recomanacions d'aquesta guia durant la implantació prèvia a la superació del procés de certificació.

I aquesta guia, què busca?

Aquest document pretén proporcionar recomanacions genèriques a l'hora de crear i gestionar les paraules de pas per tal que aquestes impedeixin, en cas necessari, que una persona no autoritzada faci un ús il·legítim dels serveis d'un altre usuari.

Aspectes legals i normatius

La guia s'ha elaborat tenint en compte les recomanacions provinents de l'estàndard internacional ISO 27002, que queden recollides en els següents controls:

- 11.2.3 Gestió de les contrasenyes d'usuari
- 11.3.1 Ús de les contrasenyes
- 11.5.3 Sistema de gestió de les contrasenyes

El seguiment d'aquesta guia també afavoreix el compliment d'alguns aspectes del Reial Decret 1720/2007, associat a la Llei Orgànica de Protecció de Dades de Caràcter Personal.

Introduint les idees bàsiques

Qui no ha fet servir mai una contrasenya?

Avui dia necessitem contrasenyes per a moltes accions gairebé diàries. Tots sabem que les paraules de pas o contrasenyes són un mecanisme de control destinat a evitar que una persona accedeixi de manera il·legítima a uns recursos o a una àrea als quals no té accés ni autorització.

Normalment, quan volem accedir a un servei d'Internet hem d'omplir dos camps d'informació (traduint en llenguatge visual, dues caselles en blanc):

- L'identificador d'usuari, que permet saber qui està intentant accedir al recurs privat
- La contrasenya

Si la combinació identificador d'usuari – contrasenya introduïda coincideix amb l'existent als sistemes d'informació, es considera que l'usuari és legítim i se li concedeix accés al recurs o àrea.

Si volem assegurar-nos que la nostra contrasenya és segura, és important que aquesta compleixi amb un conjunt de recomanacions que evitin que pugui ser fàcilment endevinada i, per tant, comprometre els recursos als quals dóna accés.

Perills que podem córrer amb contrasenyes dèbils

Per què les contrasenyes ja existents en equips que provenen de fàbrica són vulnerables?

Estrenant ordinador

Quan comprem un ordinador, el programari que ja hi ha instal·lat inclou identificadors d'usuari i contrasenyes fàcils d'endevinar que ha introduït el mateix fabricant. Com que el fabricant necessita crear aquesta informació per instal·lar cadascun dels programes que hi haurà a l'ordinador, acostuma a fer servir paraules que no costin d'imaginar. De fet, moltes d'aquestes contrasenyes es poden trobar sense gaire esforç a través de la xarxa. Així, per exemple, se sap que les bases de dades SQL Server inclouen de fàbrica l'identificador d'usuari `sa` i la contrasenya en blanc.

Si l'administrador de sistemes d'una organització no modifica, com a mínim, la contrasenya per accedir amb l'identificador d'usuari vigent, correm el risc que qualsevol persona connectada a Internet pugui accedir sense cap tipus d'autorització prèvia al recurs informàtic en qüestió i que l'exploti o l'alteri en benefici propi.

El mateix passa amb els equips configurats in situ pels proveïdors. Posem un exemple: la instal·lació d'un encaminador (en anglès, router) sense fils. Aquests dispositius utilitzen una configuració bàsica, un identificador d'usuari i una contrasenya comuns associats al model del dispositiu. Aquestes dades són de lliure distribució a

Internet i permeten al propietari de l'encaminador disposar de la informació pertinent per accedir i modificar els paràmetres de configuració del dispositiu. Si no modifiquem aquesta informació, correm el risc que qualsevol persona pugui utilitzar lliurement el dispositiu per navegar a Internet o per accedir a la xarxa privada on es trobi el dispositiu.

Si voleu un exemple real, us podem parlar dels encaminadors sense fils de la marca Zyxel. Aquests aparells són instal·lats pels tècnics de les operadores amb identificador d'usuari `1234` o `adminll` i la contrasenya `1234`.

Què pot passar si no canviem les contrasenyes que provenen de fàbrica?

Accés no autoritzat

Si un equip s'instal·la en un entorn de producció corporatiu sense que se n'hagin modificat les contrasenyes que provenen de fàbrica o sense haver inhabilitat els comptes d'accés associats a aquestes contrasenyes, qualsevol internauta o treballador de l'organització que aconsegueixi contactar amb aquest dispositiu hi podrà accedir sense dificultat i explotar aquesta circumstància en benefici propi.

Denegació de servei

Si un equip ha resultat compromès perquè una persona no autoritzada hi ha pogut accedir, l'intrús podria apagar el dispositiu remotament o desconfigurar-lo i, en conseqüència, deixar-lo fora de servei.

Reencaminament de les comunicacions

Si l'equip que ha resultat compromès és un dispositiu de xarxa (encaminadors sense fils, encaminadors Ethernet...), l'intrús pot configurar el dispositiu per tal que les comunicacions que traspassin aquest dispositiu siguin redirigides o duplicades cap una màquina controlada per l'intrús, amb la consegüent pèrdua d'informació corporativa.

Pèrdua d'informació confidencial

Quan un dispositiu s'ha vist compromès per un atacant, aquest pot aconseguir accés a la informació emmagatzemada en el dispositiu afectat, o bé pot interceptar les comunicacions que traspassin aquest dispositiu.

Per què cal definir una contrasenya robusta personalitzada?

Ja fa molt de temps que sentim a dir que no hauríem de fer servir mai la data del nostre naixement o algun altre tipus d'informació del nostre entorn com a contrasenya. Però, qui de nosaltres no ho ha fet mai?

És important saber que, amb les eines actuals, resulta relativament fàcil descobrir contrasenyes formades per paraules que apareixen en diccionaris lingüístics o mots col·loquials. Ni tan sols serveix canviar la llengua del nostre voltant per una d'estrangera.

En quins escenaris desagradables ens podem trobar?

Pèrdua d'informació confidencial

Quan un dispositiu s'ha vist compromès per un atacant, aquest pot:

- Aconseguir accés a la informació emmagatzemada en el dispositiu afectat
- Interceptar les comunicacions que traspassin aquest dispositiu

Suplantació d'identitat

Si una tercera persona no autoritzada és capaç d'accedir a un servei corporatiu fent servir el nostre compte d'accés, podrà utilitzar el servei en el nostre nom, és a dir, fent-se passar per nosaltres.

Idoneïtat en la utilització del desafiament pregunta/resposta

Com es diu la teva àvia?

Una gran quantitat de sistemes d'informació fan servir un mètode de recuperació de contrasenya basat en un desafiament de pregunta/resposta. Aquest mecanisme ens permet modificar la nostra contrasenya de manera autònoma en cas que l'haguem oblidada.

A vegades, aquests tipus de mecanismes utilitzen preguntes ja definides i nosaltres només n'hem d'escollir una. Aquestes qüestions poden demanar-nos des del nom de la nostra àvia fins el color que preferim passant per la ciutat on vam passar les millors vacances.

Així doncs, si oblidem la contrasenya podem arribar a canviar-la si contestem de manera correcta la pregunta que vam triar el dia que ens vam donar d'alta del servei.

En quins escenaris desagradables ens podem trobar?

Accés no autoritzat

Si la nostra resposta a la pregunta escollida resulta evident (perquè té a veure amb la nostra realitat més pròxima i coneguda), correm el risc que algú proper a nosaltres pugui aconseguir accedir al servei i, un cop a dins, modifiqui la contrasenya per una que no coneixem. Fent això, aconseguirà que no puguem accedir al servei en un futur. Per evitar mals de cap, doncs, és recomanable que les respostes siguin complexes i no tinguin relació amb la nostra vida més pública.

Suplantació d'identitat

Es produeix quan una tercera persona no autoritzada és capaç d'accedir a un servei corporatiu en el nostre nom. A través de la suplantació d'identitat poden dir o fer coses contràries a la nostra voluntat.

Utilització de comptes d'accés genèrics corporatius

Contrasenyes sabudes per uns quants

Moltes vegades, en entorns de treball, cal configurar un compte d'accés per a un grup de persones enlloc d'un accés personalitzat per a cada usuari. En aquests casos ens trobem davant d'una situació on més d'una persona utilitza un mateix identificador d'usuari i contrasenya per a un sol servei. Si bé no es pot tenir la certesa de qui està fent què amb aquell compte d'accés, sí que es pot controlar la gent que coneix la contrasenya per poder accedir al compte.

Hem de tenir en compte que les contrasenyes de grup

poden estar emmagatzemades per a la seva consulta en algun tipus de suport en paper o electrònic.

A causa de la manca de privacitat estricta (les coneixen més d'una persona, poden arribar a estar escrites) tenim entre mans contrasenyes altament vulnerables. Per aquest motiu, l'organització haurà de tenir-ne especial cura, sobretot si es permeten tasques a nivell d'administració de sistemes informàtics.

En quins escenaris desagradables ens podem trobar?

Accés no autoritzat

Les contrasenyes que s'emmagatzemen per poder ser consultades són més vulnerables, ja que poden ser descobertes per persones no autoritzades.

Hem de tenir present que cal canviar contrasenyes quan una persona abandona el grup o l'organització. Si no ho fem, correm el risc que l'usuari sortint pugui accedir al compte genèric en un futur.

Pèrdua d'informació confidencial

Un usuari capaç d'accedir a un sistema d'informació pot tenir accés a la informació confidencial que s'hi emmagatzemi. Aquest aspecte és especialment crític si qui hi accedeix no hauria de tenir els permisos per fer-ho.

Utilització de mecanismes de rotació de contrasenyes

Exercitar la ment per a la seguretat

de la nostra informació

Encara que haguem creat una contrasenya robusta, és molt recomanable emprendre algun tipus de mesures de seguretat complementàries com ara el canvi periòdic de contrasenyes.

Tot i que resulta molest haver de canviar la clau d'accés contínuament, es tracta d'una acció necessària per tal de protegir la informació corporativa que s'emmagatzema als sistemes d'informació.

És important que aquests mecanismes siguin coherents amb el tipus d'informació corporativa que s'intenta protegir.

En quins escenaris desagradables ens podem trobar?

Les amenaces associades a aquest escenari són equivalents a les amenaces on una contrasenya s'ha vist compromesa, ja que finalment el que compta és que algú que no és l'usuari legítim té accés a uns recursos que no li corresponen.

Recomanacions

Cadascun dels escenaris plantejats en aquesta guia exposa un seguit d'amenaques que, si es materialitzen al llarg del temps, en major o menor mesura tindran efectes perjudicials per a l'usuari, l'administrador de sistemes o fins i tot l'organització a la qual pertanyen.

Per evitar que això succeeixi, o per minimitzar-ne l'efecte si és que l'amenaça no es pot eliminar del tot, a continuació us proporcionem un conjunt de recomanacions dirigides a usuaris i administradors que gestionen contrasenyes dins de l'àmbit professional.

Recomanacions per construir contrasenyes robustes

- La longitud de la contrasenya és important. Com més llarga sigui la contrasenya, més difícil d'endevinar serà. Es recomana construir contrasenyes de, com a mínim, vuit caràcters.
- No deixar contrasenyes en blanc ni basades només en espais.
- Si la contrasenya és prou llarga però repeteix un mateix caràcter diverses vegades, perdrà força perquè resultarà més fàcil d'endevinar. Per tant, hem d'evitar d'utilitzar contrasenyes de l'estil 111abcdell.
- Per millorar la fortalesa de la contrasenya, aquesta hauria de tenir una mica de tot:
 - Números
 - Lletres majúscules i minúscules
 - Caràcters especials (*, +, \$, %, &, @, !...)

- Les contrasenyes robustes es poden millorar si inclouen espais en blanc i caràcters que es generin fent servir la tecla ALT Gr.

- Si bé combinar caràcters de diferents grups (vegeu el punt immediatament superior) dóna una fortalesa considerable a la contrasenya, si els números es col·loquen al principi o al final del conjunt, seran més fàcils d'endevinar que si apareixen en d'altres posicions.

- Sempre és millor no utilitzar paraules que puguin trobar-se en un diccionari, amb independència de l'idioma emprat, ni tampoc informació personal que pugui ser deduïda fàcilment (data de naixement, DNI, nom de les mascotes, noms de familiars, etc.), ja que es poden endevinar amb facilitat. Tampoc no es recomana d'utilitzar paraules de la cultura popular, encara que no es trobin en diccionaris lingüístics.

- Si tenim una contrasenya complexa, per còmode que sigui, hem d'evitar reciclar-la afegint un nou dígit a la contrasenya actual.

Recomanacions per preservar la privacitat de les contrasenyes

- Mantenir les contrasenyes en secret. La contrasenya és d'ús exclusiu de l'usuari o grup al qual pertany. Ningú, a banda de nosaltres mateixos (o de les persones que pertanyen al grup en concret), ha de saber-la.

- Si és necessari emmagatzemar les contrasenyes en un registre, aquest ha d'estar xifrat, amb l'accés controlat i accessible només per a les persones autoritzades.

- Les contrasenyes no s'han d'enviar ni escriure per correu electrònic o mitjançant d'altres serveis telemàtics sense xifrar.

- Mai no hem de donar la contrasenya a un usuari administrador. Aquest disposa de les eines necessàries per canviar-la, sense necessitat de conèixer la contrasenya vigent.

- Hem de fer servir contrasenyes diferents per a cada àmbit. Si tenim una contrasenya per al correu personal i una altra per al de la feina i una de les dues contrasenyes es veu compromesa, l'altra continuarà sent segura.

Recomanacions per preservar la vigència de les contrasenyes

- Si ens trobem en un entorn crític, les contrasenyes han de tenir una vigència màxima de 90 dies. Si estem en un entorn amb informació poc delicada, es podrà especificar un període de temps més ampli segons les necessitats.

- En sistemes que estiguin exposats a xarxes públiques, la vigència de les contrasenyes ha de ser proporcional al risc i confidencialitat de les dades que protegeixen.

- Sempre que sigui tècnicament possible, s'avisarà a l'usuari que la contrasenya està a punt de caducar i que ha de canviar-la amb alguns dies d'antelació (per exemple: 5 dies abans).
 - Hem d'evitar reutilitzar les 10 darreres contrasenyes.
 - Si és tècnicament possible, el sistema validarà la qualitat de la contrasenya abans d'acceptar-la.
 - És aconsellable canviar la contrasenya amb la primera connexió que realitzem al sistema, i també quan l'administrador reinicialitzi la contrasenya.
 - Les contrasenyes s'hauran d'entregar de manera segura als usuaris. Aquí teniu alguns mètodes vàlids d'entrega:
 - Entrega personal
 - Per correu electrònic xifrat
 - Correu postal
 - Missatgeria amb canal xifrat
 - Correu intern precintat
 - Hem de canviar la contrasenya si sospitem que d'altres persones en puguin tenir coneixement. Quedaran exempts del compliment ISO 27002:2005 dels requeriments indicats en aquest apartat (vigència i canvi de contrasenya) els usuaris utilitzats per a tasques automàtiques (execució d'scripts, transferència de fitxers, etc.), així com entorns on l'usuari no pugui realitzar el canvi de contrasenya de forma automàtica. En aquests casos caldrà aplicar controls addicionals com:
 - Inhabilitar l'accés a la consola del sistema
 - Definir els mínims privilegis necessaris tant d'accés com d'execució
 - Mantenir un registre dels usuaris, indicant la persona o grup responsable dels mateixos
 - Per als entorns on l'usuari no pugui realitzar el canvi de forma automàtica, el responsable d'aquests haurà de sol·licitar un canvi de contrasenya de forma periòdica mitjançant els canals establerts.
 - La utilització de llavors facilita la creació i memorització de les contrasenyes. Aquí teniu alguns exemples orientatius:
 - Llabor basada en fórmules matemàtiques:
5per%=0,05U
 - Llabor basada en la memorització d'una frase:
 - Frase: Clau de la meva web per aquest any 2010
 - Clau de 14 caràcters: CdLmWpAa2010
- Hi ha un seguit de circumstàncies, pròpies de l'àmbit de sistemes, que podrien condicionar la vigència de les contrasenyes i que, per tant, els administradors i responsables de seguretat hauran d'observar particularment:
- Quan s'introdueixi la contrasenya en els sistemes, mai no ha d'aparèixer de manera visible o llegible a la pantalla
 - No és recomanable incloure contrasenyes sense xifrar dins del codi d'aplicacions o scripts. Com a

alternativa, es poden emmagatzemar aquestes contrasenyes en fitxers amb accés restringit només als usuaris amb privilegis d'execució

- S'aconsella habilitar un sistema de protecció de pantalla amb contrasenya que s'activarà després de més de 15 minuts d'inactivitat

- Els comptes d'usuari es bloquejaran després d'un número finit d'intents infructuosos d'accés.

Conclusions

Actualment, tenim contrasenyes per a gairebé tot: per accedir al mòbil, per desactivar l'alarma, fins i tot per engeggar el cotxe. Si ens traslладem del món real al virtual, ens trobem amb una multitud de serveis que requereixen aquest tipus de validació inicial.

Necessitem tantes contrasenyes que de vegades fem servir sempre les mateixes per evitar l'oblit momentani. Tot i això, hauríem d'anar amb més cura i deixar la mandra aparcada en un racó, perquè algunes comoditats acostumen a ser les causants de la manca de seguretat.

La contrasenya pertany a qui la fa servir. Només nosaltres l'hem de saber. Per això, sempre hem de desconfiar de correus electrònics o trucades que ens demanin validació o comprovació de clau.

Hem de tenir present que una contrasenya té la finalitat de protegir alguna cosa que és important per a nosaltres, però aquesta contrasenya no té sentit si no l'utilitzem de manera correcta.

Així que...

Una contrasenya per a cada cosa.

Totes les contrasenyes al nostre cap.

NOMÉS al nostre.

Glossari

Contrasenya. Tipus d'autenticació que utilitza informació secreta per controlar l'accés a un determinat servei, recurs o sistema que requereixi una validació prèvia.

Desafiaments pregunta - resposta. Conjunt de preguntes que l'usuari ha de respondre en un primer moment d'inicialització. En cas d'oblidar la contrasenya, si l'usuari contesta correctament les preguntes (introduint les mateixes respostes que va donar en el moment de la inicialització), el sistema li permetrà canviar la contrasenya sense haver d'introduir la contrasenya vigent.

Script. Conjunt d'instruccions tècniques a executar en un sistema de manera automàtica.

Referències i enllaços web

Per elaborar la guia actual s'ha utilitzat com a referència la Guia de contrasenyes, del Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (GE-GUI19-02).

A la xarxa es pot trobar informació rellevant relacionada amb la matèria desenvolupada en aquesta guia:

- La importancia de una clave segura, Associació d'internautes, Octubre de 2009

<http://www.internautas.org/html/1869.html>

- Sacando el máximo provecho de TI: diez consejos fundamentales para la seguridad de su empresa, Cisco, Juny de 2009

http://www.cisco.com/web/ES/solutions/smb/innovators/how_to/articles/secure_my_business/essential_security_tips.pdf

- Como cambiar la contraseña de la cuenta de servicios ofimáticos en red (Dominio Windows), Universidad Carlos III de Madrid, Juny de 2009

http://www.uc3m.es/portal/page/portal/informatica/Nos-Dedicamos/ServiciosCorporativos/DominioWindows/ComoCambiar_la_Contra_Cuenta_Dominio

- Recomendaciones para la creación y uso de contraseñas seguras, INTECO, Noviembre de 2007

http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/recomendaciones_creacion_uso_contrasenas

■ Ayude a proteger su información personal con contraseñas seguras, Microsoft, Març de 2006
<http://www.microsoft.com/latam/athome/security/privacy/password.msp>

■ Common Attacks and Possible Solutions, WindowSecurity.com, Gener de 2005
<http://www.windowsecurity.com/articles/Passwords-Attacks-Solutions.html>

■ Guía detallada de aplicación de directivas de contraseñas seguras, Microsoft TechNet, Setembre de 2004
<http://www.microsoft.com/spain/technet/recursos/articulos/strngpw.msp>

Eines

Associació d'internautes

Aplicació per generar contrasenyes segures.
<http://www.internautas.org/archivos/claves.zip>

Cryptix

Aplicació per generar contrasenyes segures.
<http://www.rbcafe.com>

Lame-industries software

Aplicació per generar contrasenyes segures.
<http://lame-industries.net>

Password Manager

Eina de pagament que permet guardar i gestionar contrasenyes de manera segura.
<http://www.cp-lab.com>

Password Safe

Eina lliure que permet guardar i generar contrasenyes de manera segura.
<http://passwordsafe.sourceforge.net/>

Recursos de suport en línia

Clave Segura

Generador de contrasenyes segures en línia.
<http://www.clavesegura.org/>

Password

Generador de contrasenyes segures en línia.
<http://www.password.es/>

Simple Password

Generador de contrasenyes segures en línia.
<http://www.simplepassword.com/>



Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat