Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Gestió segura de Contrasenyes

Conscienciació en ciberseguretat

Agost de 2022

Imatge: Freepik.com

ÍNDEX

1. Aspectes claus

Ridoc.com

És important saber que tota organització, sigui aquesta pública o privada, ha de tenir establerta i implementada una **Política per a la Gestió Segura de les Contrasenyes**, en la qual es detalli com els seus col·laboradors, empleats i usuaris han de **gestionar les seves contrasenyes de manera segura.**

Quan una organització estableix les normes per a la **creació**, **ús** i **cicle de vida** de les contrasenyes que utilitzen els seus empleats, està protegint un dels **actius més importants** que té l'organització: **la seva Informació**. Segons informes recents, el 80% de les **fugides d'informació** que es produeixen en les organitzacions es deuen a un ús incorrecte de les contrasenyes per part dels seus empleats (contrasenyes poc robustes i de fàcil accés pels ciberdelinqüents).

Per aquest motiu, és important que l'organització estableixi les **normes per la creació d'una contrasenya segura**, determinant **quins tipus de caràcters han de contenir i quants són mínimament necessaris** (us donarem en les següents diapositives una sèrie de recomanacions per a això), perquè ha quedat verificat que aquelles contrasenyes amb menys de 8 caràcters poden ser desxifrades fàcilment pels ciberdelinqüents en qüestió d'hores i, si només estan formades per números, en qüestió d'instants.

Triar una bona contrasenya en termes de **Ciberseguretat** és fonamental per a mantenir protegida no sols el nostre **compte professional o corporatiu**, sinó també els nostres **comptes personals i les dades personals** que emmagatzemem en aquestes.

ÍNDEX

2. Contrasenya segura

Es diu que una **contrasenya és segura** quan la seva longitud o extensió **és superior a 10 caràcters** i està formada per **símbols, caràcters especials ($%&!ç), majúscules, minúscules i números**.

Top contraseñas más usadas en 2021

RANGO	CONTRASEÑA	TIEMPO PARA DESCIFRARLA	RECUENTO
1	123456	< 1 Segundo	103.170.552
2	123456789	< 1 Segundo	46.027.530
3	12345	< 1 Segundo	32.955.431
4	qwerty	< 1 Segundo	22.317.280
5	password	< 1 Segundo	20.958.297
6	12345678	< 1 Segundo	14.745.771
7	111111	< 1 Segundo	13.354.149
8	123123	< 1 Segundo	10.244.398
9	1234567890	< 1 Segundo	9.646.621
10	1234567	< 1 Segundo	9.396.813

Tips per a crear una contrasenya segura:

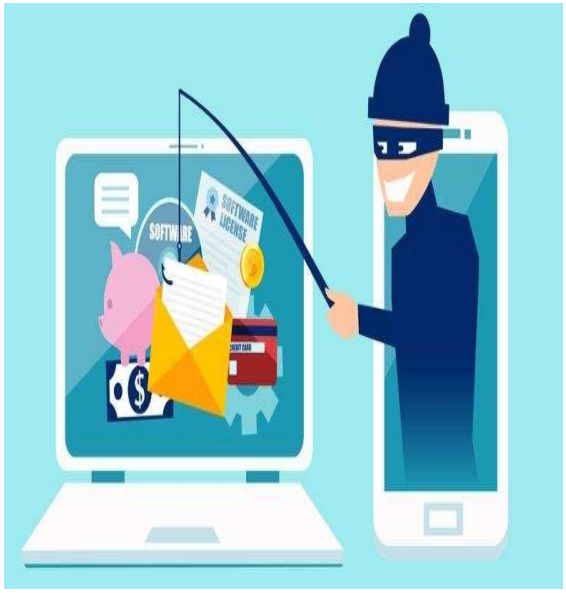
1. **Llarga:** Com més llarga és una contrasenya, més segura és. Una contrasenya segura haurà de tenir almenys 10 caràcters.
2. **Aleatòria**: Les contrasenyes segures utilitzen en una **combinació de lletres, números, majúscules i símbols** per a formar una **cadena impredictible de caràcters** que no s'assemblin a paraules o a noms continguts en el diccionari.
3. **Única**: Una contrasenya segura ha de ser **única per a cada compte**, perquè així es redueix la seva **vulnerabilitat** en cas de ser desxifrada.

ÍNDEX

3. Requisits mínims i obligatoris per a configurar una contrasenya segura

1 Les contrasenyes han de ser **robustes i fortes**, és a dir, difícils d'esbrinar. Els requisits mínims i obligatoris de les contrasenyes han d'aparèixer definits en la **Política de Gestió de Contrasenyes** que hagués estat determinada per l'organització.

2 En **l'àmbit corporatiu NO s'hauran d'utilitzar les mateixes contrasenyes que en l'àmbit personal**. L'usuari és responsable de canviar-les al menor indici d'haver pogut ser compromeses.



3 Les contrasenyes no han de compartir-se amb ningú, ja que hauran de tractar-se com a **informació confidencial**. No hauran d'incloure's en **comunicacions electròniques, qüestionaris o formularis** que rebi l'usuari per email o sms, ni emmagatzemar-se en mitjans **no segurs** com a **papers, stickers**...etc.

4 Les contrasenyes dels usuaris hauran de ser superiors a **10 caràcters i contenir símbols, caràcters especials ($%&!ç), majúscules, minúscules i números**.

ÍNDEX

4. Política de contrasenyes segures per a comptes privilegiats

Els **Comptes Privilegiats** són aquells que disposen de **permisos d'administració en sistemes i/o aplicacions**.

Cada sol·licitud que es faci per a un accés privilegiat haurà d'estar degudament justificat i determinat la **durada mínima de la seva expiració**. S'haurà de realitzar cada X temps una **revalidació dels accessos** dels comptes de privilegi que haguessin estat atorgats, així com **revocar-se** aquells accessos que no siguin ja necessaris.

Tots els **comptes d'accés privilegiat** han de ser protegits amb una **contrasenya robusta i única** que compleixi amb aquests requisits:

- ✓ *No es podran utilitzar les últimes 8 contrasenyes que s'haguessin utilitzat per a aquest compte, ni tampoc contrasenyes similars.*
- ✓ *Haurà de tenir una longitud mínima de 14 caràcters.*
- ✓ *La caducitat de la contrasenya serà de 1 any*
- ✓ *No ha de contenir el nom del compte o paraules fàcilment identificables.*

A més, haurà de complir aquests **criteris**:

- *Contenir una lletra majúscula.*
- *Contenir una lletra minúscula.*
- *Contenir un dígit.*
- *Contenir un caràcter especial (!, $, #, %).*

Està **estrictament prohibida la reutilització de la mateixa contrasenya utilitzada per un compte**. En cas de comptar amb múltiples comptes, tampoc es podrà reutilitzar les contrasenyes entre comptes.

La primera vegada que l'usuari accedeix a un compte privilegiat, l'administrador definirà una **contrasenya d'un sol ús (OTP – One Time Password)** que després l'usuari haurà de canviar en el seu primer accés. Mai l'administrador del sistema **haurà de conèixer quines són les credencials dels comptes privilegiats**, tret que siguin pròpies o tingui assignat la seva custòdia.

ÍNDEX

5. Gestors de contrasenyes

Un Gestor de contrasenyes o Administrador de contrasenyes és un programa que s'utilitza per a emmagatzemar una gran quantitat de parelles d'usuaris i contrasenyes. La base de dades on s'emmagatzema aquesta informació està xifrada mitjançant una única clau, de manera que l'usuari només haurà de memoritzar una única clau per a accedir a totes les altres. Això facilita molt l'administració de contrasenyes i fomenta que els usuaris triïn claus complexes, sense tenir por al fet que no podran recordar-les posteriorment.

Keepass Password Safe

És un gestor de contrasenyes de programari lliure que permet gestionar les contrasenyes de manera segura. De manera oficial, solament es pot instal·lar en sistemes operatius Windows, des de Windows 7 fins a Windows 11, i també en Sistemes operatius Linux, MacOS i FreeBSD. Hi ha contribucions oficials de KeePass que són compatibles també amb sistemes operatius Android i iOS. L'ús d'aquest programa és totalment gratuït.

Gestors de Contrasenyes

Altres Gestors de Contrasenyes recomanats

- **Freemindtronic**

Freemindtronic és una empresa especialitzada en el disseny de productes electrònics en Seguretat Informàtica i especialitzada sobretot a dissenyar proteccions elèctriques per sistemes informàtics, sistemes de control d'accés sense fil i sistemes de seguretat amb claus de xifratge segmentades.

- **Dashlane**
- **LastPass**
- **1Password**

ÍNDEX

Govern d'Andorra

6. Tipus d'atacs a contrasenyes

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

Atacs de Força Bruta

1.) Atac de diccionari

Aquests ciberatacs aprofiten la mala pràctica d'utilitzar una sola paraula com a contrasenya. El ciberdelinqüent utilitza un programari que li permet introduir contrasenyes de manera automàtica i va provant totes les paraules del diccionari com a possibles contrasenyes.

2.) Ompliment de credencials

L'ompliment de credencials és un atac de força bruta que utilitza credencials robades en forats de seguretat. S'aprofiten també de la reutilització de credencials d'aplicacions personals (per exemple, les de les xarxes socials i serveis en línia).

3.) *Password Spraying*

Es produeix quan un ciberdelinqüent utilitza un gran nombre de contrasenyes robades en un grup de comptes (per exemple, les del correu dels empleats) per veure si pot obtenir accés, valent-se per això de programes que poden limitar el nombre d'intents d'accés a un compte.

Atacs de Enginyeria social

1.) *Smishing, Vishing* i *Warshipping*

Aquests ciberatacs s'inicien per un email, SMS, trucada de tlf. o mitjançant dispositius :

- **Phishing**: Un correu electrònic que crida la teva atenció sobre alguna mena d'assumpte urgent procedent d'una entitat de la teva confiança com, per exemple, la teva entitat bancària. Aquests contenen un enllaç a un lloc web de manera que suplanten a la web legítima d'aquesta entitat i en el qual et demanaran les credencials per a iniciar sessió.
- **Smishing:** Consisteix en l'enviament d'un SMS per part d'un ciberdelinqüent a un usuari, simulant ser una entitat legítima (per exemple, a una xarxa social).
- **Vishing**: Es fa a través d'una trucada de telèfon, utilitzant tècniques similars a les anteriors.
- **Warshipping**: Un regal tecnològic contaminat que es connectarà a la nostra xarxa i robarà les nostres credencials i altres dades.

2.) *Shoulder surfing*

El Shoulder surfing és una tècnica d'enginyeria social en la qual els ciberdelinqüents aconsegueixen les contrasenyes espiant a la gent que utilitza els seus dispositius en públic mentre escriuen.

Altres atacs

1.) Atac de *Keylogger*

El *Keylogger* és un software espia que s'utilitza per rastrejar i registrar el que s'escriu per teclat. Els ciberdelinqüents s'aprofiten d'això per infectar intencionadament els dispositius vulnerables i gravar la informació privada.

2.) *Man in The Middle*

En aquesta mena d'atac el ciberdelinqüent intercepta la comunicació entre 2 o més interlocutors, podent suplantar la identitat d'un d'ells per a veure la informació que té i canviar-la al seu gust.

2.a) Intercepció del trànsit

En aquest cas, el ciberdelinqüent espia l'activitat de la xarxa per capturar contrasenyes i un altre tipus d'informació sensible, per exemple, interceptat connexions wifis no segures o utilitzant la tàctica de segrest de sessió.

ÍNDEX

7. Consell per un ús segur de les contrasenyes

Per aconseguir posar en marxa i desenvolupar en l'organització una **Política de Bons Hàbits en l'Ús de Contrasenyes Segures**, podríem esmentar les següents pautes a seguir:

1. Utilitzar contrasenyes complexes i actualitzar-les periòdicament.

2. Evitar reutilitzar les contrasenyes en diferents llocs i comptes, així com incloure les nostres dades personals en aquestes a l'hora de crear-les.

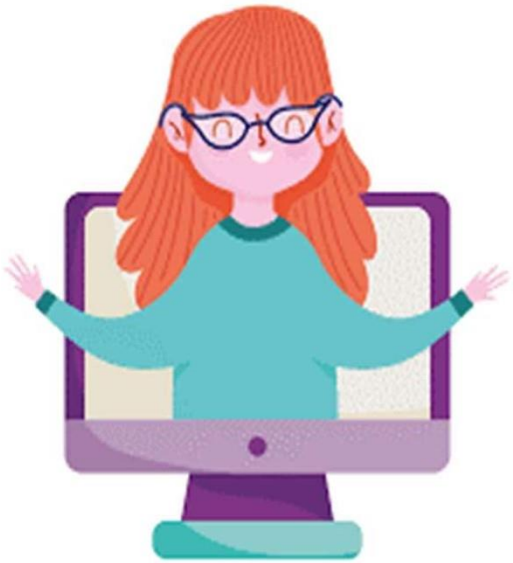
3. Utilitzar l'Autenticació Multifactor (coneguda com a MFA o inici de sessió única): L'autenticació multi factor requereix que l'usuari proporcioni **dos o més factors de verificació** per accedir al seu compte (per exemple, usuari + contrasenya + codi rebut per sms d'un sol ús o trucada de tlf.).

4. Utilització de l'Autenticació Biomètrica (reconeixement facial, reconeixement ocular o reconeixement d'empremtes dactilars). Aquest tipus d'autenticació s'està convertint en una solució robusta als sistemes d'autenticació multi factor i aquesta popularitzant-se cada vegada més.

5. Utilitzar un Administrador/Gestor de Contrasenyes: Adoptar un administrador de contrasenyes en l'organització proporcionarà una forma segura d'emmagatzemar, compartir i administrar les contrasenyes en un únic lloc.

6. Educar i formar als empleats en matèria de contrasenyes segures garantirà que la identitat personal de l'empleat i les dades de l'empresa estiguin degudament protegits en cas d'infracció.

7. Realitzar periòdicament en les organitzacions auditories relatives a l'ús i gestió de les contrasenyes que es fa per part dels empleats.



Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

ANDORRA
DIGITAL

Entitats col·laboradores

andorra
telecom

DAND
DIGITALAND
by Ibermática | TdA