ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

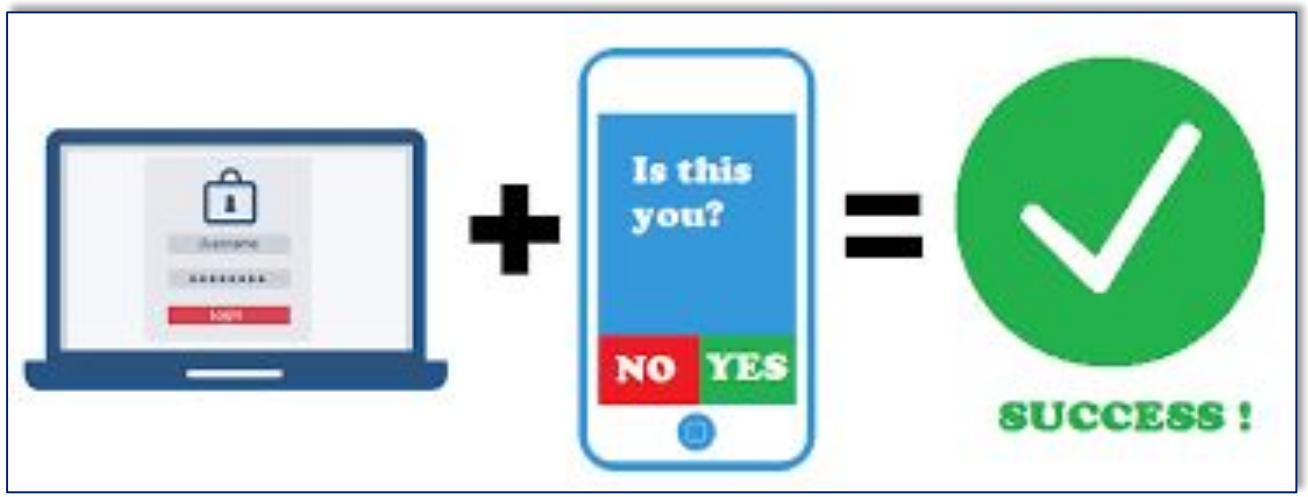
AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

AUTENTICACIÓ DE DOBLE FACTOR (2FA)

Març 2025
Document d'ús públic

1. CONTEXTUALITZACIÓ



L'ús de mecanismes d'**AUTENTICACIÓ FORTA** és un element **COMPLEMENTARI** i **INDISPENSABLE** per verificar la **IDENTITAT DE L'USUARI**, atès que es tracta d'un mètode de seguretat que permet afegir una **VERIFICACIÓ ADDICIONAL** al procés d'autenticació. Actualment, s'utilitza molt quan es treballa de manera remota i cal connectar-se als sistemes de l'empresa.

2. COM FUNCIONA?

Per aconseguir una **CAPA DE SEGURETAT ADDICIONAL:**

- **1r factor d'autenticació:** s'accedeix a un servei o plataforma en línia i s'hi introdueix la **CONTRASENYA.**
- **2n factor d'autenticació:** se sol·licita un **CODI DE VERIFICACIÓ** que s'envia per correu electrònic o per SMS, o bé una empremta dactilar o un altre mètode que s'hagi configurat prèviament.

Quan s'introdueix el segon factor d'autenticació, es verifica la identitat del titular del compte i es completa l'inici de sessió.

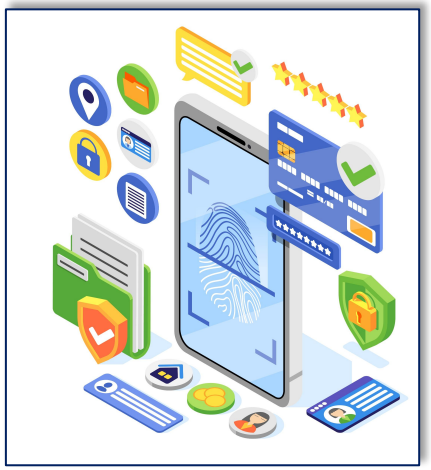
Primer factor d'autenticació

El primer mètode és una **CONTRASENYA SEGURA**; el segon mètode pot ser un **CODI** obtingut per mitjà d'un correu electrònic o un missatge de text, reconeixement facial, etc.

Com es pot crear una contrasenya segura

Una contrasenya segura ha de ser difícil d'endevinar o desxifrar:

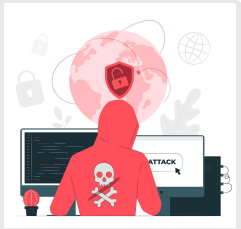
- **Llarga**: longitud mínima de dotze caràcters, però millor si en té quinze.
- **Aleatòria:** combinació de diferents lletres (majúscules i minúscules), números i símbols.
- **Única:** no s'ha d'utilitzar la mateixa contrasenya en dos llocs web o aplicacions diferents.
- Cal evitar **patrons típics** com «qwert» o «12345».
- Cal instal·lar un **administrador de contrasenyes** per generar i desar les contrasenyes segures.



Amenaces per vulnerar contrasenyes

Amenaces

Força bruta

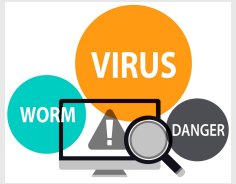


Programari que utilitza un «diccionari» carregat de contrasenyes molt utilitzades.

Pesca

Falsificació d'una entitat de confiança, com bancs i xarxes socials; el cibercriminal manipula la víctima perquè introdueixi les seves dades d'accés en un lloc web fals idèntic a l'original.

Virus



Programa dissenyat per dur a terme accions malicioses, com, per exemple, el robatori de contrasenyes i credencials d'accés.

Atacs a servidors

Vulneració d'un sistema informàtic emprat per emmagatzemar la base de dades de credencials d'accés d'un determinat servei.

Conductes insegures

Aquestes conductes de l'usuari també fan que sigui més fàcil vulnerar una contrasenya. Per exemple, fer servir la mateixa clau per a diferents serveis.

Què fa la doble autenticació per mitigar els atacs?

El cibercriminal roba la contrasenya utilitzant alguna amenaça informàtica.

Després introdueix la credencial robada i intenta accedir al sistema.

El sistema sol·licita el segon factor d'autenticació.

L'atacant no disposa del segon codi i el sistema no li permet l'accés.

Segon factor d'autenticació

El segon mètode d'autenticació pot ser un **CODI** obtingut a través de…

Empremta dactilar

Utilitza la teva empremta dactilar com a segon factor d'autenticació.

Codi enviat per SMS

L'usuari ha d'introduir el codi juntament amb la seva contrasenya.

Codi QR

L'usuari escaneja el codi juntament amb la seva contrasenya.

Preguntes de seguretat

Preguntes i respostes personals que prèviament ha escollit l'usuari.

Aplicacions mòbils

L'app genera un codi de verificació, vàlid entre trenta segons i un minut (Google Authenticator, Microsoft Authenticator, etc.).

Claus de seguretat USB

Els dispositius es connecten a l'ordinador o al telèfon mitjançant USB, que contenen una clau criptogràfica única per identificar-se.

Codi enviat al correu electrònic

L'usuari ha d'introduir el codi juntament amb la seva contrasenya o fer-hi clic.

3. AVANTATGES D'ACTIVAR L'AUTENTICACIÓ DE DOBLE FACTOR

1. Els sistemes d'autenticació de doble factor són molt **MÉS SEGURS** que el de les contrasenyes, atès que afegeixen una capa de seguretat extra.
2. **Ajuda a evitar ciberatacs**. Molts atacs que s'han fet públics no s'haurien produït si s'hagués implementat aquest sistema.
3. Aquest sistema, per descomptat, **NO ÉS INFAL·LIBLE**, però fa que els atacants hagin de treballar molt més, ja que aquest tipus de sistemes ofereix una **CAPA EXTRA** de protecció.

4. COM ES CONFIGURA LA 2FA ALS NAVEGADORS I A LES XARXES SOCIALS?

Els usuaris tenen cada vegada més informació delicada als seus comptes, la qual cosa fa que esdevinguin un **blanc perfecte i que els ciberdelinqüents destinin recursos per a robar-los les contrasenyes**. Per reduir aquests atacs, és molt important la **CONSCIENCIACIÓ** dels **USUARIS**, amb l'objectiu que protegeixin els seus comptes amb les següents configuracions de **doble autenticació.**

Configuració Compte Verificació en dos passos Selecciona «Activar» Establir codi (sis dígits) Afegir adreça electrònica.

Ves a Nom d'usuari Configuració Compte Gestionar configuració de seguretat Activa l'opció «Verificació en dues etapes per a inici de sessió».

Configuració Configuració del compte Seguretat Activa l'opció «Sol·licitar un codi de seguretat per accedir al meu compte des de navegadors desconeguts».

Paràmetres Configuració Comptes Una altra configuració del compte de Google Seguretat Verificació en dos passos Configuració o Editar.

Paràmetres Configuració Seguretat i privacitat Activa l'opció «Enviar peticions de verificació d'inici de sessió al meu telèfon».

Accedeix al portal El meu ID d'Apple Administrar el teu ID d'Apple Iniciar sessió Contrasenyes i seguretat.

Avís Legal

Aquest document conté informació pública.

El seu objectiu és la conscienciació en ciberseguretat pels ciutadans, empreses i entitats d'Andorra.