ANDORRA DIGITAL

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

# AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

## CONSCIENCIACIÓ EN CIBERSEGURETAT

## CONCEPTES BÀSICS DE SEGURETAT DE LA INFORMACIÓ EN L'ÀMBIT LABORAL PER A PERSONES DISCAPACITADES

Document d'ús públic

1 QUÈ ÉS LA SEGURETAT DE LA INFORMACIÓ?

2 PER QUÈ M'HAIG DE PREOCUPAR PER LA SEGURETAT DE LA INFORMACIÓ QUE UTILITZO EN LA MEVA VIDA PERSONAL I LABORAL?

3 BONES PRÀCTIQUES DE SEGURETAT EN EL MANEIG DE LES TEVES CONTRASENYES.

4 BONES PRÀCTIQUES DE SEGURETAT AL TEU LLOC DE TREBALL.

5 BONES PRÀCTIQUES DE SEGURETAT EN L'ÚS DE LA DOCUMENTACIÓ EN PAPER.

6 BONES PRÀCTIQUES DE SEGURETAT EN L'ÚS DEL CORREU ELECTRÒNIC.

7 BONES PRÀCTIQUES DE SEGURETAT DAVANT D'ATACS D'ENGINYERIA SOCIAL.

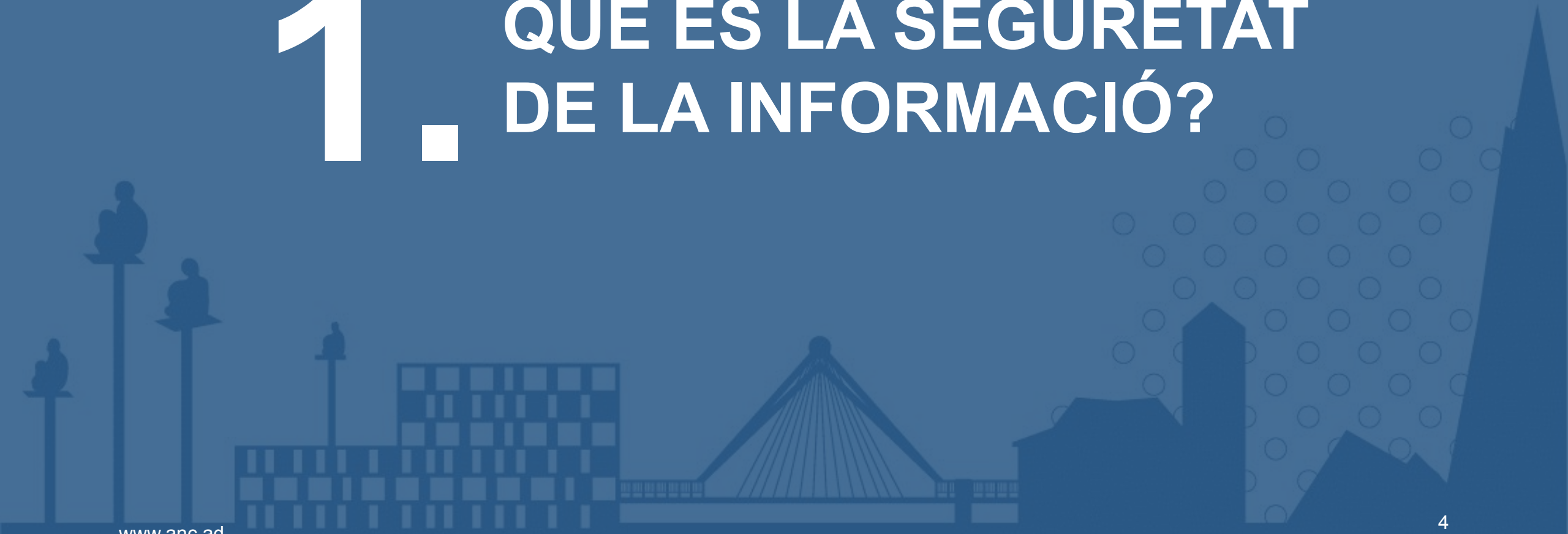
8 BONES PRÀCTIQUES DE SEGURETAT EN EL MANEIG DE LES XARXES SOCIALS (FACEBOOK, TIKTOK, INSTAGRAM…).

9 BONES PRÀCTIQUES DE SEGURETAT EN EL MANEIG DEL TELÈFON MÒBIL.

10 BONES PRÀCTIQUES DE SEGURETAT QUAN ET CONNECTIS A UNA XARXA WIFI PÚBLICA.

11 DECÀLEG BÀSIC EN MATÈRIA DE SEGURETAT DE LA INFORMACIÓ.

# 1. QUÈ ÉS LA SEGURETAT DE LA INFORMACIÓ?



# SEGURETAT DE LA INFORMACIÓ

Anomenem «**seguretat de la informació**» al conjunt de mesures preventives que destinades a protegir la **confidencialitat**, la **disponibilitat** i la **integritat** de la informació.

Característiques de la informació:

- **Confidencialitat**: evita que la informació es divulgui a persones que no tenen autorització per conèixer el seu contingut.
- **Integritat**: intenta protegir el contingut de la informació i que aquesta no pugui ser modificada ni alterada de manera indeguda.
- **Disponibilitat**: evita que persones no autoritzades puguin accedir a la informació i que el seu contingut estigui disponible.

# 2. PER QUÈ M'HAIG DE PREOCUPAR PER LA SEGURETAT DE LA INFORMACIÓ QUE UTILITZO EN LA MEVA VIDA PERSONAL I LABORAL?

# RECOMANACIONS GENERALS PER A L'ÚS D'INFORMACIÓ CONFIDENCIAL

## 01 Amb seny

- Si estic treballant en una empresa i tinc accés a informació delicada i confidencial, és important **no divulgar-ne el contingut a altres persones.**
- La **pèrdua de dades o el robatori d'informació confidencial** de l'empresa podria ocasionar grans problemes a l'empresa on treballo.

## 02 Seguretat i protecció

- El respecte de les normes de seguretat de la informació per part de tots els treballadors és important de cara a **garantir la seguretat i la protecció de la informació de l'empresa.**
- La seguretat de la informació és **cosa de tots** i tots hem de protegir-la.

# 3. BONES PRÀCTIQUES DE SEGURETAT EN EL MANEIG DE LES TEVES CONTRASENYES

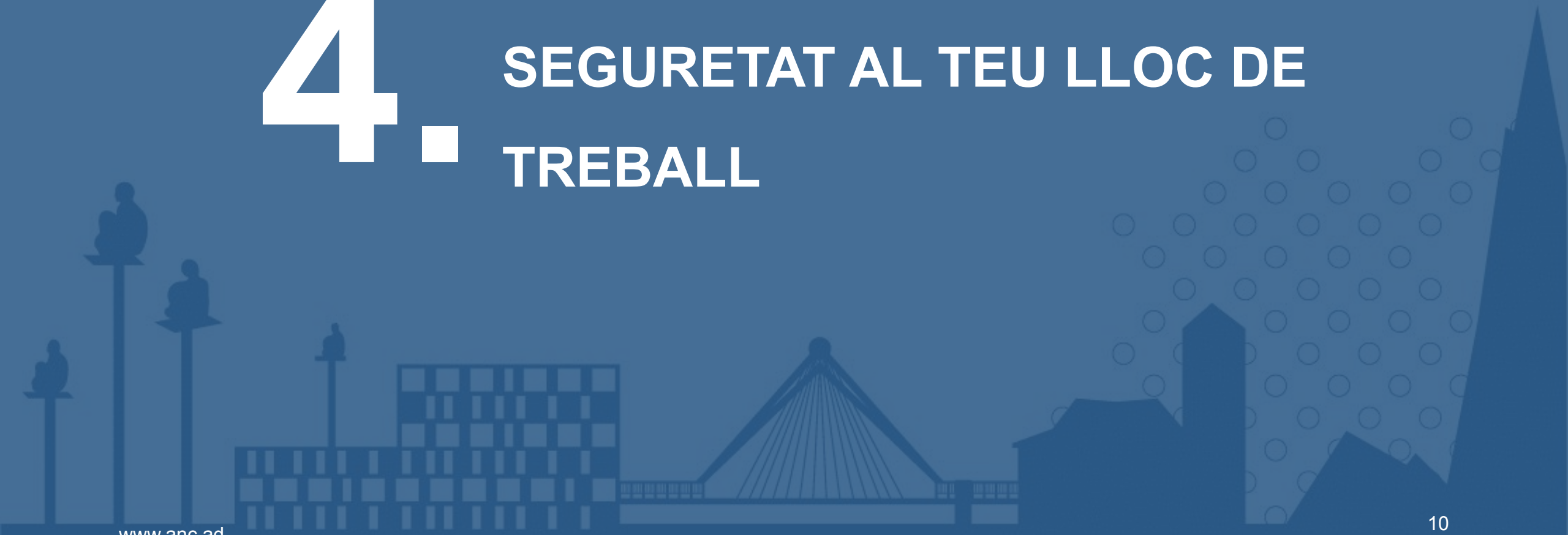
# RECOMANACIONS GENERALS PER L'ÚS DEL CORREU ELECTRÒNIC CORPORATIU

- És important que **canviïs les contrasenyes periòdicament**.
- **No enviïs les contrasenyes per correu electrònic ni per missatgeria**.
- **No escriguis mai les contrasenyes en un document** que estigui a la vista de tothom.

Una contrasenya segura ha de tenir:

- Una longitud igual o superior a **8 caràcters**.
- Ha d'estar formada per **minúscules, majúscules, números i símbols especials** com, per exemple, ~!@#$ %^&*()_+=?>.

# 4. BONES PRÀCTIQUES DE SEGURETAT AL TEU LLOC DE TREBALL

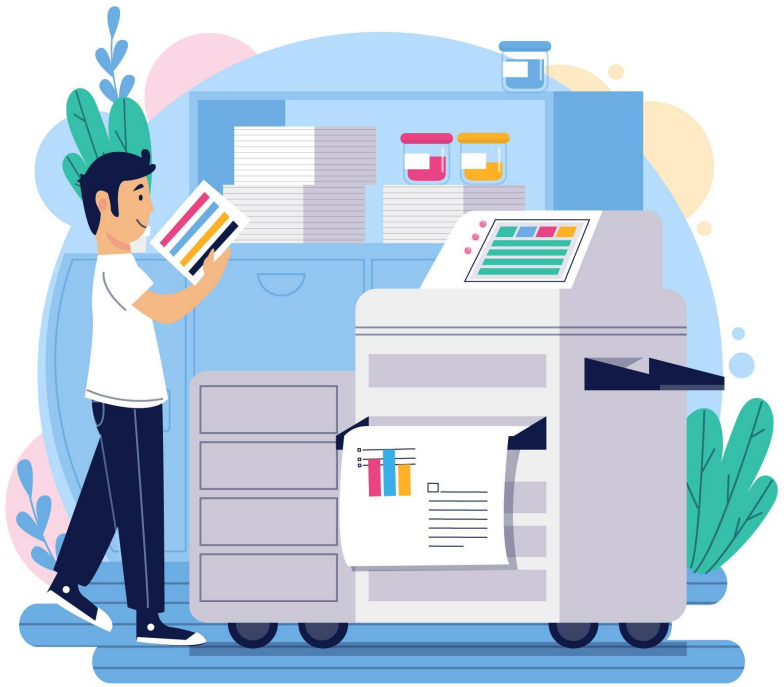


# ALTRES RECOMANACIONS I OBLIGACIONS A TENIR EN COMPTE

- **Utilitza els armaris i els calaixos del lloc on treballes** per desar els documents perquè no estiguin a la vista de la resta de treballadors.
- Mentre no estiguis a la teva taula de treball, **deixa sempre l'ordinador bloquejat.**
- No parlis de temes de feina confidencials **en llocs no apropiats** en què qualsevol et pugui sentir.

# 5. BONES PRÀCTIQUES DE SEGURETAT EN L'ÚS DE LA DOCUMENTACIÓ EN PAPER

# CONTROL DE LA IMPRESSIÓ DE LA DOCUMENTACIÓ



- **Controla la impressió de la documentació** que imprimeixes a la feina.
- **No imprimeixis documentació confidencial si no és estrictament necessari**. Les còpies dels documents en paper que continguin informació confidencial **s'han de destruir en les destructores de paper** facilitades per l'empresa.
- Si imprimeixes informació confidencial, **has d'estar a prop de la impressora** durant la impressió del document.

# 6. BONES PRÀCTIQUES DE SEGURETAT EN L'ÚS DEL CORREU ELECTRÒNIC

# RECOMANACIONS GENERALS PER L'ÚS DEL CORREU ELECTRÒNIC CORPORATIU

Ves molt amb compte amb els **fitxers adjunts i amb els enllaços que rebis en el correu electrònic**. Si et demanen que introdueixis dades personals, econòmiques o professionals, no ho facis **MAI**. I menys encara si no coneixes la persona que t'envia el correu electrònic.

Comprova les **adreces dels destinataris abans d'enviar el missatge.**

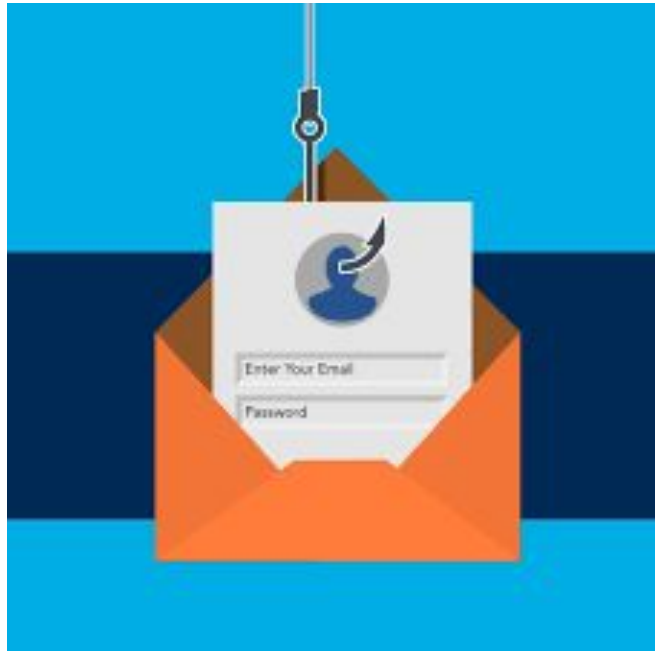
# 7. BONES PRÀCTIQUES DE SEGURETAT DAVANT D'ATACS D'ENGINYERIA SOCIAL

# ELS ATACS DE L'ENGINYERIA SOCIAL

- L'enginyeria social és la **manipulació psicològica que es fa sobre les persones**. La persona maliciosa («dolenta») intenta aconseguir que les persones facin coses per obtenir ella un benefici propi.

- L'enginyeria social **la practiquen persones que utilitzen l'engany** per aconseguir que els proporcionis les teves dades personals, econòmiques, professionals...

- Qualsevol persona és **susceptible de caure en un atac d'enginyeria social** i posar en perill les seves dades personals, laborals, econòmiques…



# 8. BONES PRÀCTIQUES DE SEGURETAT EN EL MANEIG DE LES XARXES SOCIALS (FACEBOOK, TIKTOK, INSTAGRAM...)

# RECOMANACIONS GENERALS PER AL BON ÚS DE LES XARXES SOCIALS

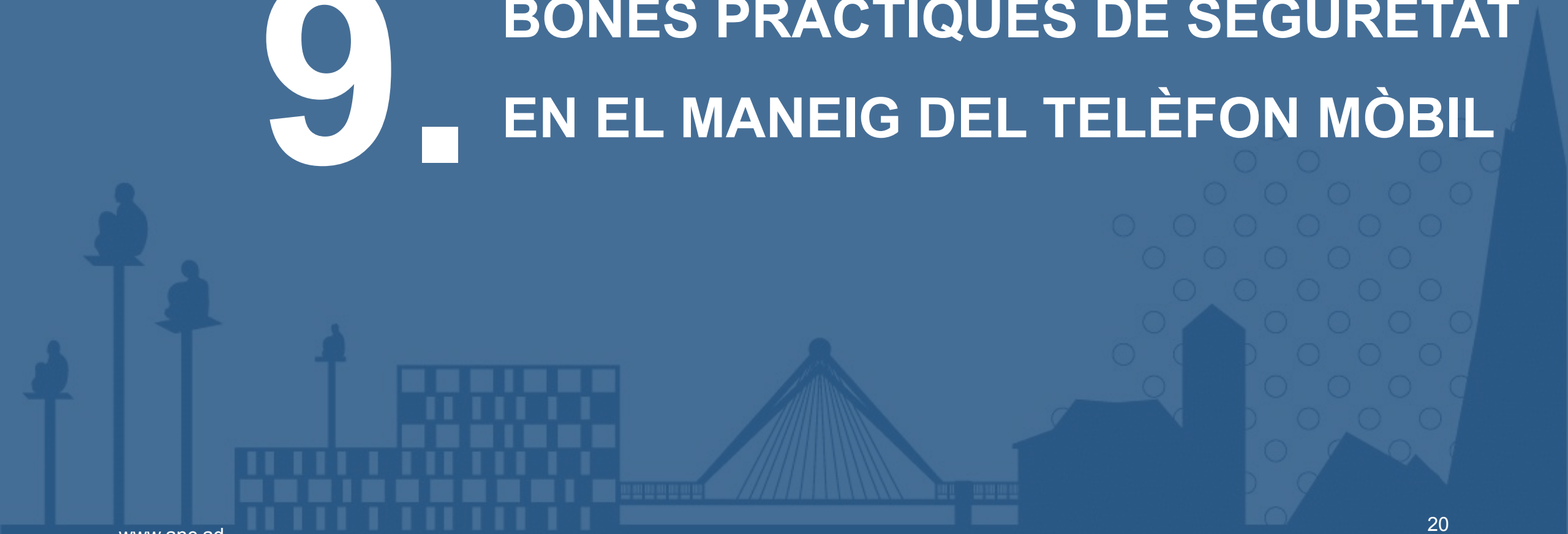
## 01 No parlis de l'empresa

- **Evita publicar informació a les xarxes socials** que pugui posar en perill la seguretat de l'empresa on treballes.
- **Ves amb compte a l'hora d'opinar públicament sobre l'empresa on treballes**. Això pot afectar la reputació de l'empresa i la teva pròpia imatge.
- **No facis servir el correu professional per entrar a les xarxes socials.** En aquests casos, sempre és millor que utilitzis la teva adreça personal.

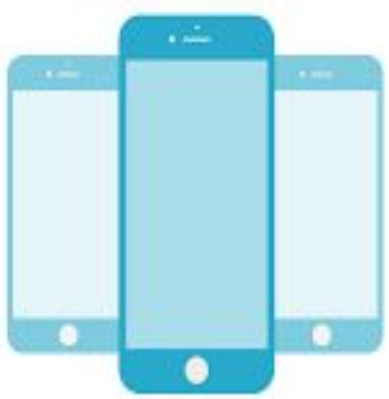
## 02 Informació delicada

- **No donis informació confidencial sobre la teva feina que pugui ser usada pels atacants** (és a dir, pels «dolents») per atacar l'empresa on treballes.
- **Ves amb compte amb la informació que dones sobre el teu lloc de treball** a altres persones que no treballen amb tu.

# 9. BONES PRÀCTIQUES DE SEGURETAT EN EL MANEIG DEL TELÈFON MÒBIL



# ÚS DEL MÒBIL A LA FEINA



- **Bloqueja sempre el telèfon mòbil**, amb contrasenya, PIN, imatge facial o empremta dactilar, per evitar que altres persones puguin tenir accés a la teva informació personal.
- **Instal·la aplicacions en el telèfon mòbil** només des de repositoris oficials (Apple Store, Google Store…)
- **Instal·la en el telèfon mòbil només les aplicacions que realment necessitis** i que utilitzis habitualment.
- **No emmagatzemis informació delicada i confidencial** en el telèfon mòbil.
- **Ves amb compte quan et connectis amb el telèfon mòbil a una xarxa wifi pública**.

# 10. BONES PRÀCTIQUES DE SEGURETAT QUAN ET CONNECTIS A UNA XARXA WIFI PÚBLICA

# CONNECTAR-SE A UNA WIFI PÚBLICA

L'ús de xarxes wifi públiques suposa múltiples riscos per als usuaris que s'hi connecten. Per què?

- Perquè et poden **robar les dades** que **transmets** a través del telèfon mòbil.
- Perquè et poden **robar les dades** que tens **emmagatzemades** en el telèfon mòbil.
- Perquè el telèfon mòbil et pot quedar **infectat amb un virus** que hagin llançat els atacants (és a dir, els «dolents»).


# 11. DECÀLEG BÀSIC EN MATÈRIA DE SEGURETAT DE LA INFORMACIÓ

# RECOMANACIONS I SUGGERIMENTS

- **No escriguis les contrasenyes en cap mena de suport o document** (per exemple, no escriguis les contrasenyes en un paper i després el deixis al costat del teu ordinador).

- **Navega de manera segura i evita les pàgines web que no siguin fiables**. En aquest sentit, fixa't sempre que la pàgina web a la qual vols accedir comenci per **https://** i no per http://. Assegura't també que a la barra superior aparegui un cadenat. Això vol dir que la navegació és segura i està protegida.

- Utilitza el correu electrònic de forma segura i **elimina els missatges que et semblin sospitosos**.

- **Evita les fuges d'informació**. No parlis de temes confidencials en llocs on hi hagi terceres persones que puguin escoltar la conversa.

- **Protegeix el teu lloc de treball i mantingues la taula «neta» de papers** que continguin informació confidencial.

- És recomanable que posis una **clau d'accés** (PIN, contrasenya, reconeixement per empremta dactilar o imatge facial) al teu telèfon mòbil i que activis l'opció de **bloqueig automàtic**.

- **No imprimeixis documentació confidencial** si no és estrictament necessari.

- Quan viatgis, no enviïs informació delicada a través de **xarxes wifi no fiables**.

- **No facis servir equips (ordinadors portàtils) que no siguin els que l'empresa on treballes t'hagi proporcionat per dur a terme la teva activitat laboral**. En cas que hagis d'utilitzar el teu ordinador personal per fer la teva feina, no l'usis per manejar informació laboral.

# Avís Legal

Aquest document conté informació pública.

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