ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Prediccions i tendències clau Ciberseguretat per al 2025

Informe elaborat per l'**Agència Nacional de Ciberseguretat d'Andorra**

ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Escenari complex i en evolució

En el 2025, la ciberseguretat es preveu com un àmbit crític i complex, caracteritzat per una evolució continua de les amenaces i les estratègies de defensa. A mesura que la tecnologia avança, també ho fan els ciberdelinqüents, que aprofiten eines emergents com la intel·ligència artificial (IA) i la computació quàntica per llançar atacs més sofisticats.

Tot seguit, s'analitzen de manera exhaustiva les tendències i les prediccions clau que marcaran el panorama de la ciberseguretat el 2025.

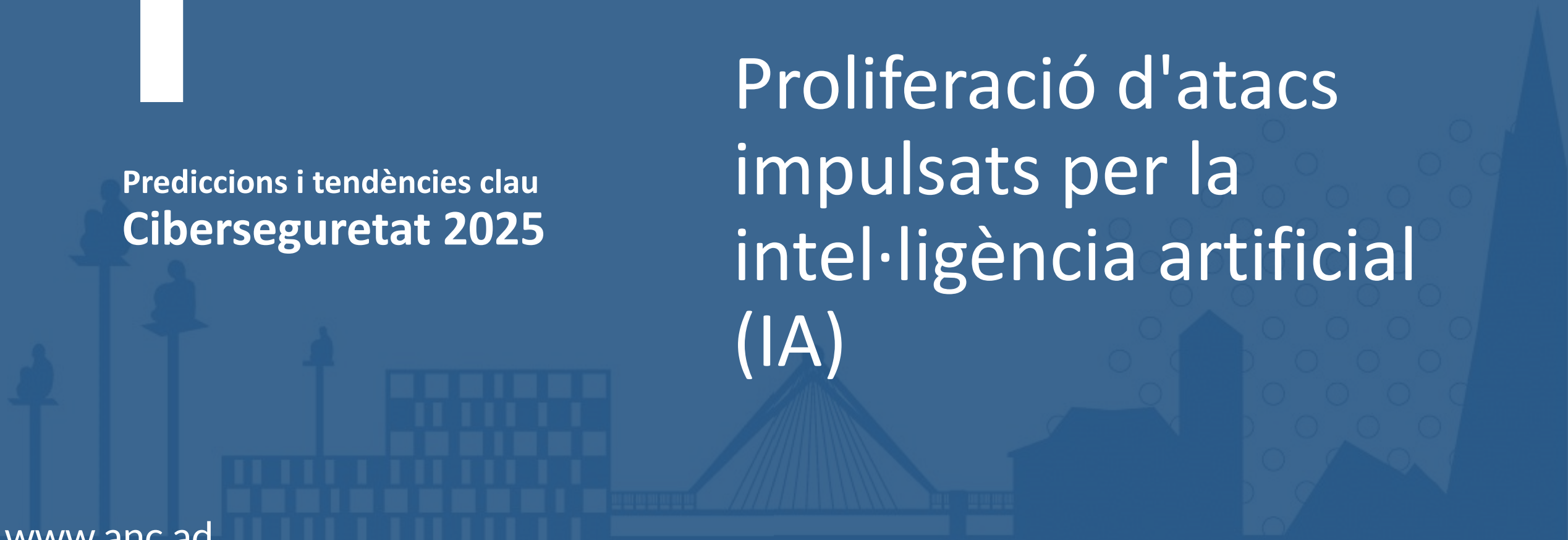
ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

1

Prediccions i tendències clau
Ciberseguretat 2025

Proliferació d'atacs impulsats per la intel·ligència artificial (IA)



ANDORRA DIGITAL

ANC-AD

1

Proliferació d'atacs impulsats per la intel·ligència artificial (IA)

La intel·ligència artificial s'ha convertit en una eina fonamental tant per millorar les defenses cibernètiques com per desenvolupar ciberatacs més sofisticats. El 2025 veurem una acceleració en l'ús de la IA per part dels ciberdelinqüents, que la faran servir per a:

Automatitzar atacs de pesca a gran escala

i personalitzar missatges en temps real basant-se en dades robades.

Dissenyar programari maliciós adaptable

que aprèn i evoluciona per evadir els sistemes de detecció tradicionals.

Dur a terme anàlisis massives de dades

i identificar patrons i punts vulnerables a les xarxes complexes.

ANDORRA DIGITAL

ANC-AD

1

Proliferació d'atacs impulsats per la intel·ligència artificial (IA)

Per altra banda, les organitzacions recorreran a la IA per enfortir els seus sistemes de seguretat, implementar solucions que analitzin anomalies en temps real, anticipin possibles amenaces i reforcin la seva capacitat de resposta davant dels incidents. Tanmateix, la carrera entre defensors i atacants serà un camp de batalla dinàmic, on els ciberdelinqüents continuaran intentant superar les mesures més avançades.

La IA no només està canviant les regles del joc en termes de velocitat i precisió dels atacs, sinó també la capacitat dels atacants per personalitzar campanyes específiques basades en anàlisis de comportament. A més a més, els ciberdelinqüents estan començant a fer servir sistemes generatius com ara l'aprenentatge profund (el *deep learning*) per crear enganys més convincents, com ara imatges, textos o veus simulades. Per contrarestar aquesta amenaça, les organitzacions hauran d'invertir en sistemes de detecció basats en intel·ligència artificial que siguin capaços d'analitzar patrons i preveure moviments de l'atacant.

ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

2

Prediccions i tendències clau
Ciberseguretat 2025

Evolució del programari de segrest i amenaces a la cadena de subministrament

ANDORRA DIGITAL

ANC-AD

2

Evolució del programari de segrest i amenaces a la cadena de subministrament

El programari de segrest continuarà evolucionant com una de les amenaces més devastadores. El 2025 s'espera que els ciberdelinqüents adrecin els seus atacs cap a cadenes de subministraments crítiques, i facin servir tècniques cada vegada més avançades per interrompre operacions essencials. Els enfocaments nous inclouran:

Ús del 'programari de segrest com a servei' (RaaS)

i democratitzar l'accés a eines d'atac per a delinqüents sense experiència.

Implementació d'hipertrucatges

per manipular identitats i obtenir accés a sistemes restringits.

Campanyes adreçades a proveïdors de programari i maquinari

per introduir vulnerabilitats en els seus productes.

ANDORRA DIGITAL

ANC-AD

2

Evolució del programari de segrest i amenaces a la cadena de subministrament

La importància de protegir la cadena de subministrament serà fonamental, perquè un sol punt de fallada podria desencadenar conseqüències catastròfiques en múltiples sectors, inclosos el financer, l'energètic i el sanitari.

La professionalització del programari de segrest, combinada amb la manca de preparació de les petites i mitjanes empreses, encara exposa més les cadenes de subministrament crítiques. Els atacs dirigits als proveïdors menors poden desencadenar una reacció en cadena amb conseqüències globals. A més a més, la digitalització accelerada està creant noves dependències tecnològiques, cosa que subratlla la necessitat d'implementar estratègies de segmentació de xarxes i controls d'accés estrictes per minimitzar riscos.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

3

Prediccions i tendències clau
Ciberseguretat 2025

Creixement de vulnerabilitats en entorns de núvol i dispositius IoT

ANDORRA DIGITAL

ANC-AD

3

Creixement de vulnerabilitats en entorns de núvol i dispositius IoT

L'adopció massiva de serveis al núvol i dispositius de l'internet de les coses (IoT) continuarà expandint la superfície d'atac. Els ciberdelinqüents se centraran a explotar configuracions mal gestionades, credencials dèbils i falta d'actualitzacions. En aquest context, es preveuen reptes diversos:

La complexitat de gestionar infraestructures híbrides

que combinen solucions locals i al núvol.

L'augment d'atacs dirigits a dispositius IoT

que es fan servir en sectors crítics com ara la salut i la manufactura.

La necessitat d'implantar solucions de seguretat específiques

per a entorns multinúvol.

A més dels riscos de configuració, la proliferació de dispositius IoT no segurs està creant una xarxa de punts vulnerables que els ciberdelinqüents poden explotar. Molts dispositius no disposen d'estàndards de seguretat robustos, cosa que augmenta les possibilitats d'accés no autoritzat. Les organitzacions han de prioritzar eines de monitoratge que analitzin constantment els comportaments de xarxa a la recerca d'irregularitats i actualitzacions freqüents per mitigar aquests riscos.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

4

Prediccions i tendències clau
Ciberseguretat 2025

Amenaces emergents de la computació quàntica

www.anc.ad

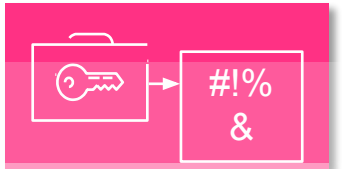
ANDORRA DIGITAL

ANC-AD

4

Amenaces emergents de la computació quàntica

Tot i que la computació quàntica encara està en una etapa inicial, el seu potencial per trencar els mètodes de xifratge actuals representa una preocupació significativa. En el 2025 es preveu un enfocament més gran en:



Desenvolupament d'algoritmes criptogràfics

resistents a la computació quàntica.

Actualització de protocols de seguretat

en sectors com ara la banca, el comerç electrònic i les telecomunicacions.

Augment de la inversió en recerca

per preveure els riscos associats amb aquesta tecnologia.

La computació quàntica també planteja desafiaments en termes d'infraestructura, atès que les organitzacions han d'adaptar els seus sistemes a tecnologies que encara estan en evolució. Aquest canvi implicarà costos significatius en actualitzacions i formació tècnica. Els governs i les entitats privades hauran de col·laborar en estàndards globals per garantir que les solucions resistents a la computació quàntica siguin adoptades de manera uniforme i eficaç.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

5

Prediccions i tendències clau
Ciberseguretat 2025

Escassedat de talent en ciberseguretat

www.anc.ad

ANDORRA DIGITAL

ANC-AD

5

Escassedat de talent en ciberseguretat

La bretxa entre la demanda d'experts en ciberseguretat i l'oferta disponible continuarà essent un desafiament el 2025. Aquesta situació impactarà directament en la capacitat de les organitzacions per implementar mesures de seguretat efectives. Algunes estratègies clau per abordar aquesta problemàtica inclouen:

Invertir en programes de formació i certificació especialitzats en ciberseguretat.

Fomentar aliances publicoprivades per desenvolupar talent local als mercats emergents.

Incorporar intel·ligència artificial i automatització per cobrir parcialment la manca de personal especialitzat.

L'escassedat de talent no només afecta la resposta immediata davant d'incidents, sinó també a la capacitat d'innovació en ciberseguretat. Les empreses hauran de considerar la formació interna de personal no tècnic per cobrir certes funcions. A més, la diversitat i la inclusió en els programes de formació podrien ampliar la base de professionals, i atraure talents de disciplines diferents per abordar els desafiaments de manera creativa.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

6

Prediccions i tendències clau
Ciberseguretat 2025

Regulacions més estrictes i èmfasi en la ciberresiliència

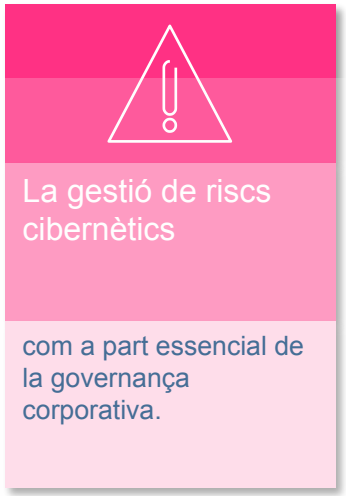
ANDORRA DIGITAL

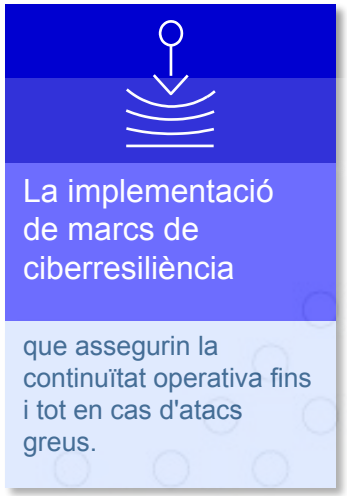
ANC-AD

6

Regulacions més estrictes i èmfasi en la ciberresiliència

La pressió creixent dels governs i organismes internacionals per enfortir la ciberseguretat farà que hi hagi l'adopció de regulacions més estrictes. En particular, les normatives, com ara la Directiva NIS2 a Europa, impulsaran un enfocament més rigorós en:





Aquestes normatives no només estableixen estàndards mínims de seguretat, sinó que també obliguen les empreses a redefinir les seves prioritats estratègiques al voltant de la protecció de dades. A més, el compliment d'aquestes regulacions s'està convertint en un diferenciador competitiu, atès que els clients i socis comercials prefereixen treballar amb organitzacions que demostrin un compromís sòlid amb la ciberseguretat. Els costos associats a la no conformitat, com ara multes i pèrdua de reputació, subratllen encara més la importància d'integrar la ciberresiliència en tots els nivells de l'organització.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

7

Prediccions i tendències clau
Ciberseguretat 2025

Automatització i professionalització del cibercrim

www.anc.ad

ANDORRA DIGITAL

ANC-AD

7

Automatització i professionalització del cibercrim

El cibercrim està evolucionant cap a un model de negoci altament organitzat, amb grups especialitzats que ofereixen serveis a cada etapa del cicle d'atac. Aquesta professionalització inclou:

L'ús d'eines automatitzades

que augmenten la velocitat i la precisió dels atacs.

La venda de kits d'explotació en els mercats clandestins

que faciliten l'accés al cibercrim per a actors menys experimentats.

La col·laboració entre grups criminals

per maximitzar l'eficàcia de les operacions.

L'automatització està permetent que els ciberdelinqüents redueixin els costos operatius i augmentin la freqüència dels seus atacs. Per altra banda, la creació de xarxes clandestines ben organitzades, que operen com a autèntiques empreses, està facilitant el desenvolupament d'amenaces personalitzades per a objectius específics. Aquest model planteja reptes addicionals per a les organitzacions, que han d'adaptar les seves defenses per contrarestar tant els atacants com les operacions criminals altament estructurades.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

8

Prediccions i tendències clau
Ciberseguretat 2025

Integració d'amenaces físiques i digitals

www.anc.ad

ANDORRA DIGITAL

ANC-AD

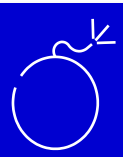
8

Integració d'amenaces físiques i digitals

La convergència entre les amenaces físiques i digitals serà una realitat el 2025. Exemples d'això inclouen:

Atacs combinats

que interrompen tant sistemes informàtics com infraestructures físiques.



L'ús de tàctiques d'intimidació física

per extorsionar empreses compromeses digitalment.

La necessitat d'estratègies de defensa integrades

que abordin ambdós tipus d'amenaces.

La digitalització d'infraestructures crítiques, com l'energia i el transport, les converteix en objectius d'alt valor. Els atacs híbrids, que combinen ciberatacs amb sabotatges físics, poden causar interrupcions massives i prolongades. A més, l'espionatge industrial està augmentant, on els adversaris combinen infiltració física i digital per extreure informació delicada. En aquest context, la integració d'estratègies de defensa física i cibernètica serà clau per garantir la seguretat general.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

9

Prediccions i tendències clau
Ciberseguretat 2025

Riscos associats a l'ús indegut de la IA

ANDORRA DIGITAL

ANC-AD

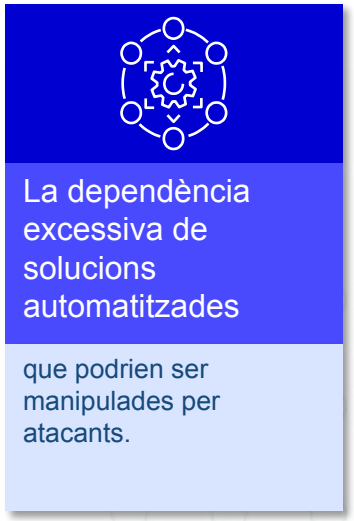
9

Riscos associats a l'ús indegut de la IA

L'adopció ràpida d'eines d'IA en processos empresarials comporta riscos, com ara:

L'exposició accidental de dades delicades

través de plataformes mal configurades.



La dependència excessiva de solucions automatitzades

que podrien ser manipulades per atacants.

La necessitat de marcs ètics i de governança clars

per garantir un ús segur i responsable d'aquestes tecnologies.

La manca de controls efectius sobre la IA també planteja riscos reguladors i ètics, especialment en sectors on la presa de decisions automatitzada pot afectar els consumidors. Per exemple, els errors en la IA que es fa servir per a processos financers o de salut poden generar conseqüències greus. Les empreses han de prioritzar la implementació d'auditories d'IA i establir polítiques clares per gestionar i supervisar aquestes tecnologies.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

10

Prediccions i tendències clau
Ciberseguretat 2025

Prioritat en estratègies de seguretat proactives

www.anc.ad

ANDORRA DIGITAL

ANC-AD

10

Prioritat en estratègies de seguretat proactives

En lloc de limitar-se a reaccionar davant d'incidents, les organitzacions haurien d'adoptar enfocaments proactius, com ara:

Les estratègies proactives només milloren la capacitat de resposta davant d'amenaces, si no que també redueixen significativament els costos associats als incidents de seguretat. A més, les simulacions avançades, com els exercicis de *Red Teaming*, permeten que les empreses identifiquin debilitats internes abans que els atacants les explotin. La inversió en anàlisi predictiva i en col·laboració amb equips especialitzats externs serà fonamental per mantenir una postura de seguretat sòlida.

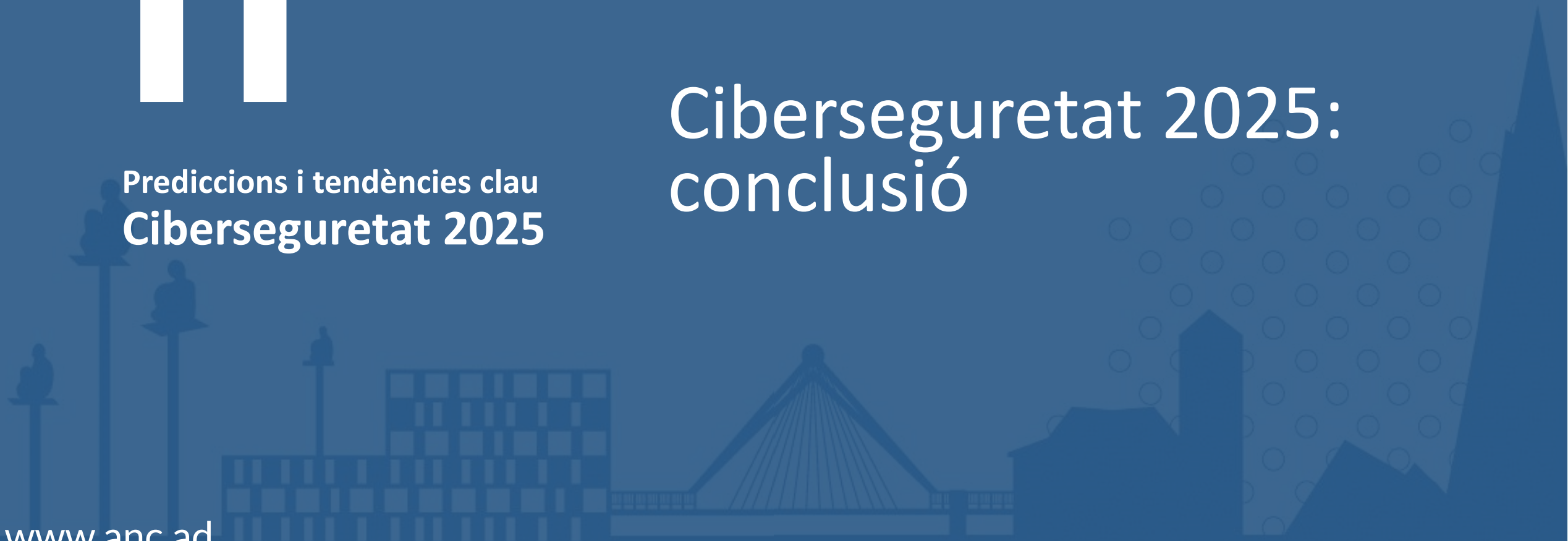
ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

11

Prediccions i tendències clau
Ciberseguretat 2025

Ciberseguretat 2025: conclusió



www.anc.ad

ANDORRA DIGITAL

ANC-AD

11

Ciberseguretat 2025: conclusió

L'any 2025 es perfila com un període crucial per a la ciberseguretat, on les amenaces seran més sofisticades i persistents que mai. La clau per superar aquests desafiaments serà una combinació d'innovació tecnològica, inversió en talent humà i col·laboració entre sectors per construir un ecosistema digital més segur.

Per garantir-ne la competitivitat, les organitzacions hauran d'integrar la ciberseguretat en el nucli de les seves estratègies empresarials. Això implica no només implementar solucions tècniques avançades, sinó també fomentar una cultura de seguretat en tots els nivells de l'organització. La capacitació continua dels professionals, combinada amb la sensibilització sobre les amenaces emergents, serà essencial per enfortir les baldes més dèbils de la cadena de seguretat.

A més, la col·laboració entre els sectors públic i privat jugarà un paper fonamental en la detecció i mitigació d'amenaces. Les iniciatives conjuntes per compartir informació sobre incidents i millors pràctiques permetran que les empreses s'avancin als atacs. Paral·lelament, els governs han d'adoptar un paper més actiu, promoure regulacions clares i fomentar la inversió en ciberdefensa.

En última instància, la ciberresiliència serà el factor diferenciador entre les organitzacions que prosperen en el panorama digital del 2025 i aquelles que queden endarrerides. Més enllà de prevenir atacs, les empreses han de ser capaces de recuperar-se ràpidament, i minimitzar-ne l'impacte a les operacions i la reputació. Aquest enfocament holístic garantirà no només la protecció dels actius, sinó també la confiança dels clients i socis, tot consolidant la seva posició com a líders en un món cada vegada més digital i connectat.

ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Prediccions i tendències clau

Ciberseguretat 2025

Informe elaborat per l'**ANC-AD**