ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Prediccions i tendències clau Ciberseguretat per al 2026

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

ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

La ciberseguretat, un factor estratègic d'estabilitat, confiança i resiliència

La transformació digital s'ha consolidat com un dels motors principals de desenvolupament econòmic, eficiència operativa i innovació en els darrers anys. L'adopció generalitzada de serveis al núvol, la digitalització de processos administratius i productius, l'automatització avançada i l'ús creixent de la intel·ligència artificial han permès que organitzacions públiques i privades millorin la capacitat d'actuació, optimitzar recursos i oferir serveis més àgils i accessibles.

Tot i això, aquesta evolució tecnològica ha vingut acompanyada d'una ampliació significativa de la superfície d'exposició al risc digital. Els sistemes cada vegada són més interdependents, els fluxos d'informació més complexos i les fronteres tradicionals entre xarxes internes i externes han desaparegut pràcticament del tot. En aquest nou context, un incident de ciberseguretat ja no afecta únicament un sistema aïllat, sinó que es pot propagar amb rapidesa, impactant en serveis essencials, cadenes de subministrament, confiança institucional i estabilitat operativa.

L'entorn d'amenaces ha evolucionat en paral·lel. Els atacs ja no responen a patrons simples ni a accions oportunistes. Són campanyes planificades, persistents i orientades a l'impacte, dissenyades per maximitzar el dany econòmic, operatiu o reputacional. Els actors maliciosos combinen tècniques avançades, explotació d'identitats legítimes, enginyeria social sofisticada i coneixement profund dels processos de les organitzacions objectiu. En molts casos, el component tècnic de l'atac només és una part d'una estratègia més àmplia que inclou pressió psicològica, manipulació de la confiança i explotació de dependències entre organitzacions.

L'any 2026 es perfila com a punt de consolidació d'aquestes dinàmiques. Tecnologies emergents com ara la intel·ligència artificial, l'Internet de les Coses o l'automatització de processos crítics deixen de ser innovacions aïllades per esdevenir elements estructurals del funcionament quotidià. Aquesta integració aporta beneficis enormes, però també introdueix nous vectors de risc i obliga a replantejar els models tradicionals de protecció, detecció i resposta.

En aquest escenari, la ciberseguretat deixa definitivament de ser un àmbit exclusivament tècnic per convertir-se en un **factor estratègic d'estabilitat, confiança i resiliència**. La capacitat de garantir la continuïtat dels serveis públics, protegir infraestructures crítiques, salvaguardar la informació delicada i mantenir la confiança de la ciutadania depèn, en gran manera, de la preparació davant d'incidents de naturalesa digital.

L'experiència recent demostra que cap sistema no és completament immune i que la prevenció absoluta no és un objectiu realista. Per això, el focus es desplaça progressivament cap a la resiliència: la capacitat d'anticipar amenaces, detectar incidents amb rapidesa, limitar-ne l'impacte i recuperar l'operativa en terminis assumibles. Aquesta aproximació requereix una visió integral que combini tecnologia, organització, processos, persones i governança.

Així mateix, la gestió del risc digital adquireix una dimensió col·lectiva. El nivell d'exposició d'una organització no depèn únicament dels controls propis, sinó també del seu ecosistema: proveïdors, socis, operadors de serveis i tercers amb accés a sistemes o dades. La ciberseguretat esdevé així una responsabilitat compartida que exigeix coordinació, intercanvi d'informació i alineació estratègica entre actors públics i privats.

ANDORRA DIGITAL

Agència Nacional de Ciberseguretat d'Andorra

Aquest document té com a objectiu oferir una **visió estructurada de l'escenari de ciberseguretat que es consolida el 2026**, i identificar les tendències principals, els riscos emergents i les àrees prioritàries d'actuació. No es tracta d'un catàleg de solucions ni d'una aproximació prescriptiva, sinó d'un exercici d'anàlisi i anticipació que permeti reforçar la preparació de l'ecosistema digital i facilitar la presa de decisions informades.

Comprendre la naturalesa canviant de les amenaces, anticipar-ne l'impacte i adaptar de forma contínua les capacitats de protecció serà determinant per garantir un entorn digital segur, fiable i sostenible. La ciberseguretat del futur es construeix des d'una visió a llarg termini, basada en la col·laboració, la millora continuada i el compromís amb la resiliència.

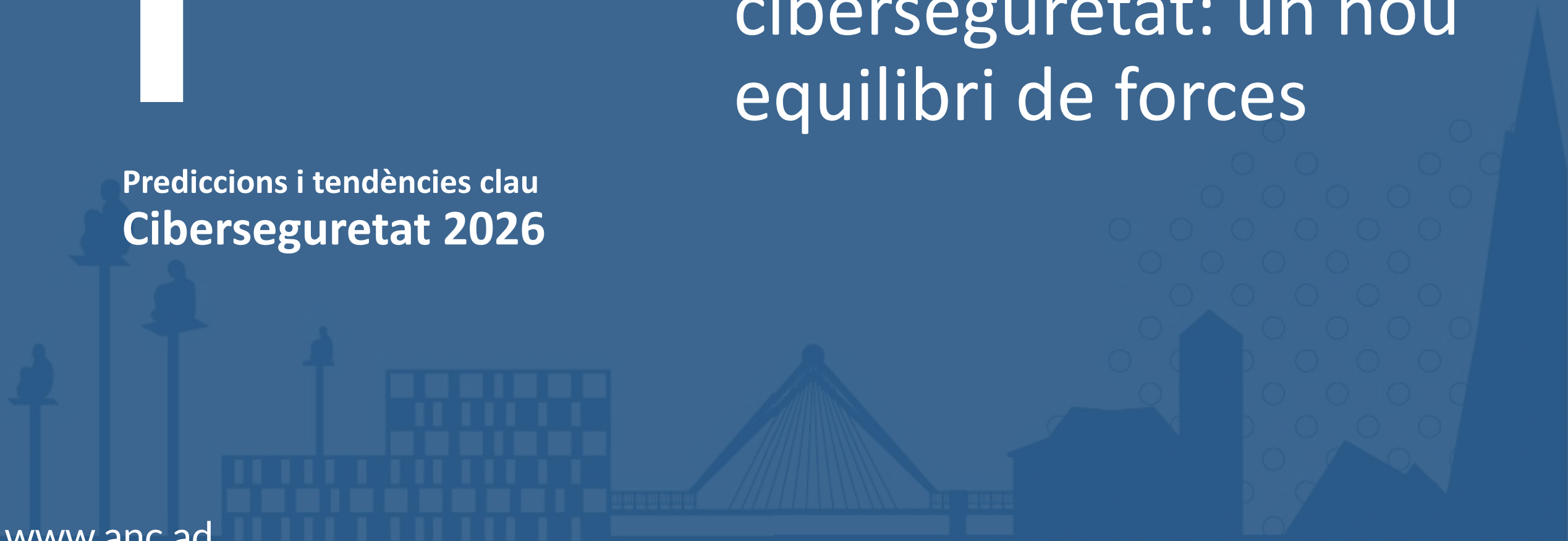
ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

1

Intel·ligència artificial i ciberseguretat: un nou equilibri de forces

Prediccions i tendències clau
Ciberseguretat 2026



www.anc.ad

ANDORRA DIGITAL

ANC-AD

1

Intel·ligència artificial i ciberseguretat: un nou equilibri de forces

La intel·ligència artificial es consolida el 2026 com un dels principals factors de transformació del panorama de la ciberseguretat. La seva integració generalitzada en processos digitals, sistemes d'anàlisi i plataformes operatives ha modificat substancialment la manera com es conceben, executen i defensen els ciberatacs. Ja no és una tecnologia emergent o experimental, sinó un component estructural de l'ecosistema digital.

Des del punt de vista ofensiu, la intel·ligència artificial actua com un potent multiplicador de capacitats. Els actors maliciosos fan servir models avançats per automatitzar fases completes del cicle d'atac, des del reconeixement inicial fins a l'explotació i la persistència. L'anàlisi de grans volums d'informació pública i de semipública permet identificar relacions entre persones, sistemes, proveïdors i tecnologies exposades, i facilita la construcció de perfils detallats de les organitzacions objectiu.

Un dels àmbits on aquest impacte és més evident és l'enginyeria social. La generació automàtica de textos, veu i imatges permet crear comunicacions altament creïbles, adaptades a l'idioma, el context cultural i el rol específic de la víctima. Els missatges deixen de ser genèrics per convertir-se en interaccions personalitzades, coherents amb els processos interns de l'organització i difícils de distingir d'una comunicació legítima. Aquest grau de realisme incrementa significativament la probabilitat d'èxit dels atacs i redueix l'eficàcia dels controls tradicionals basats únicament en la detecció de patrons coneguts.

ANDORRA DIGITAL

1

Intel·ligència artificial i ciberseguretat: un nou equilibri de forces

www.anc.ad

ANC-AD

La generació de codi maliciós també es veu profundament afectada. L'any 2026, l'ús de la intel·ligència artificial permet crear eines adaptades a entorns específics, capaços de modificar-ne el comportament en funció de les defenses detectades. Els atacs esdevenen dinàmics i adaptatius, s'ajusten en temps real per evadir controls, canviar tècniques de persistència o modificar-ne l'empremta per dificultar l'anàlisi forense. Aquesta capacitat d'iteració ràpida redueix les barreres d'entrada per a actors amb un nivell tècnic més baix i contribueix a un augment del volum i la diversitat de les amenaces.

Paral·lelament, la intel·ligència artificial es converteix en un pilar fonamental de les capacitats defensives. Les organitzacions incorporen models avançats per analitzar grans volums d'esdeveniments, correlacionar senyals aparentment inconnexes i detectar desviacions subtils en el comportament dels usuaris, els sistemes i els processos. Aquest enfocament permet passar d'una detecció basada en indicadors aïllats a una detecció contextual, centrada a identificar comportaments anòmals amb impacte potencial.

La principal aportació de la intel·ligència artificial en defensa és la reducció del soroll operatiu. En entorns altament instrumentats, la capacitat de prioritzar incidents en funció de la seva criticitat real és essencial per evitar la saturació dels equips i garantir una resposta eficaç. L'automatització de tasques repetitives i de risc baix allibera capacitat humana per a l'anàlisi avançada, la investigació d'incidents complexos i la presa de decisions en situacions de crisi.

ANDORRA DIGITAL

1

Intel·ligència artificial i ciberseguretat: un nou equilibri de forces

www.anc.ad

ANC-AD

Tot i això, l'adopció massiva d'intel·ligència artificial introdueix també desafiaments i riscos nous. La qualitat i la integritat de les dades utilitzades per entrenar i alimentar els models es converteixen en un factor crític. Models entrenats amb dades incompletes, esbiaixades o manipulades poden generar decisions errònies, difícils de detectar i encara més difícils d'explicar. A més, l'opacitat inherent a alguns sistemes d'intel·ligència artificial planteja reptes rellevants des del punt de vista de la traçabilitat, l'auditoria i el compliment normatiu.

En aquest context, la supervisió humana pren una importància renovada. Delegar decisions crítiques en sistemes automatitzats sense mecanismes de control adequats pot generar una falsa sensació de seguretat. L'any 2026, l'equilibri entre automatització i control humà es consolida com un dels principals reptes estratègics en matèria de ciberseguretat.

La intel·ligència artificial no substitueix el criteri humà, sinó que l'amplifica. El seu valor rau en la capacitat de millorar la visibilitat, accelerar l'anàlisi i donar suport a la presa de decisions, sempre que s'integri dins un marc de governança clar, amb responsabilitats definides i límits ben establerts. Gestionar aquest nou equilibri de forces serà determinant per afrontar amb èxit l'escenari d'amenaces que es consolida els anys vinents.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

2

Prediccions i tendències clau
Ciberseguretat 2026

Programari de segrest (*ransomware*) i extorsió digital: evolució cap a un risc sistèmic

ANDORRA DIGITAL

2

Programari de segrest (*ransomware*) i extorsió digital: evolució cap a un risc sistèmic

www.anc.ad

El programari de segrest es consolida el 2026 com una de les amenaces més rellevants i persistents del panorama de la ciberseguretat. Lluny de ser una tècnica puntual o un fenomen conjuntural, s'ha transformat en un **model de negoci criminal molt estructurat**, amb rols especialitzats, processos optimitzats i una clara orientació a maximitzar l'impacte i la rendibilitat.

En aquesta nova fase de maduresa, el programari de segrest deixa de centrar-se exclusivament en el xifratge de sistemes per evolucionar cap a esquemes d'**extorsió múltiple i progressiva**. L'objectiu de l'atacant ja no és només impedir l'accés a la informació, sinó controlar el temps, la pressió i la narrativa de l'incident. El xifratge es converteix en una eina més dins una estratègia més àmplia que combina robatori selectiu de dades, amenaces de divulgació pública, pressió reputacional i, en alguns casos, afectació a tercers.

Abans d'executar l'atac visible, els actors maliciosos dediquen un esforç considerable a comprendre l'entorn de l'organització objectiu. Analitzen quins actius són més crítics, quins serveis no es poden aturar, quina informació té més valor estratègic i quines obligacions reguladores hi ha en cas de filtració o interrupció del servei. Aquest coneixement permet dissenyar atacs altament personalitzats, ajustats al perfil de risc i la capacitat de resposta de la víctima.

ANDORRA DIGITAL

2

Programari de segrest (*ransomware*) i extorsió digital: evolució cap a un risc sistèmic

www.anc.ad

La cadena de subministrament adquireix un paper especialment rellevant en aquest context. En lloc d'atacar directament organitzacions amb alts nivells de maduresa en ciberseguretat, els atacants busquen proveïdors o socis amb menys nivell de protecció, però amb accés privilegiat a múltiples entorns. El compromís d'un sol proveïdor pot amplificar l'impacte de l'atac, afectar simultàniament nombroses organitzacions i generar una pressió addicional difícil de gestionar.

El 2026, els models de programari de segrest com a servei es troben plenament consolidats. L'especialització de funcions -desenvolupadors de codi maliciós (*malware*), intermediaris d'accessos inicials, operadors d'infraestructura i negociadors- redueix les barreres d'entrada i augmenta el volum d'atacs. Aquest ecosistema delictiu opera amb mètriques clares d'eficiència, ajusta les seves estratègies en funció dels resultats obtinguts i s'adapta ràpidament a les defenses desplegades.

Davant d'aquest escenari, la prevenció absoluta deixa de ser un objectiu realista. Fins i tot organitzacions amb nivells de maduresa elevats es poden veure afectades per un incident de programari de segrest. Per això, el focus estratègic es desplaça cap a la **resiliència operativa**: la capacitat de limitar l'abast de l'atac, mantenir els serveis essencials i recuperar l'activitat en terminis assumibles.

La resiliència davant del programari de segrest es construeix des de múltiples dimensions. A nivell tècnic, és fonamental disposar d'arquitectures segmentades, còpies de seguretat robustes i protegides davant de manipulacions, i controls estrictes sobre accessos privilegiats. A nivell organitzatiu, l'existència de plans de resposta específics, assajats periòdicament, marca una diferència substancial en la gestió de l'incident.

ANDORRA DIGITAL

2

Programari de segrest (*ransomware*) i extorsió digital: evolució cap a un risc sistèmic

www.anc.ad

ANC-AD

Igualment rellevant és la coordinació entre àrees tècniques, legals, de comunicació i direcció. El programari de segrest no és només un problema tecnològic, és una crisi que pot afectar la continuïtat operativa, la confiança de clients i ciutadans i el compliment normatiu. La capacitat de prendre decisions informades sota pressió, comunicar de manera coherent i gestionar l'impacte reputacional és tan crítica com la resposta tècnica.

El 2026, el programari de segrest es consolida així com un **risc sistèmic**, l'impacte del qual transcendeix l'organització individual i pot afectar sectors complets o serveis essencials. Abordar-ho de manera eficaç requereix una visió integral, basada en l'anticipació, la preparació i la col·laboració, més que en la reacció puntual davant de l'incident consumat.

ANDORRA DIGITAL

Agència Nacional de Ciberseguretat d'Andorra

3

Prediccions i tendències clau
Ciberseguretat 2026

Seguretat de la intel·ligència artificial: protegir els sistemes que prenen decisions

ANDORRA DIGITAL

3

Seguretat de la intel·ligència artificial: protegir els sistemes que prenen decisions

www.anc.ad

ANC-AD

A mesura que la intel·ligència artificial s'integra de forma creixent en processos crítics, el seu paper dins de les organitzacions deixa de ser auxiliar per esdevenir **determinant en la presa de decisions**. El 2026, models d'aprenentatge automàtic, motors de recomanació, sistemes de detecció de frau, assistents intel·ligents i agents autònoms influeixen directament en àmbits com ara la gestió del risc, l'optimització operativa, l'assignació de recursos o la interacció amb ciutadans i clients.

Aquesta evolució introdueix una nova realitat en l'àmbit de la ciberseguretat: la intel·ligència artificial mateixa es converteix en un actiu crític que ha de ser protegit. La seguretat ja no es pot centrar únicament en servidors, xarxes o aplicacions tradicionals. Cal ampliar el focus cap als models, les dades que els alimenten i els processos que en governen el funcionament.

Els sistemes d'intel·ligència artificial presenten **vectors d'atac específics**, diferents dels associats als sistemes convencionals. Un dels més rellevants és la manipulació de dades d'entrenament. Introduir informació esbiaixada, maliciosa o alterada als conjunts de dades pot degradar progressivament el comportament del model o induir decisions incorrectes de manera silenciosa. Aquest tipus d'atac és especialment perillós perquè els seus efectes no sempre són immediats i poden passar desapercebuts durant llargs períodes de temps.

Un altre vector crític és la manipulació d'entrades i contextos d'execució, especialment en models generatius i assistents conversacionals. A través de tècniques d'injecció d'instruccions o d'alteració del context, un atacant pot induir el sistema a ignorar restriccions, revelar informació delicada o executar accions no previstes. Aquests atacs exploten la mateixa lògica del model, sense necessitat de comprometre directament la infraestructura subjacent.

ANDORRA DIGITAL

3

Seguretat de la intel·ligència artificial: protegir els sistemes que prenen decisions

www.anc.ad

El robatori de models constitueix també una amenaça creixent. Mitjançant consultes repetides i anàlisi de les respostes, és possible reconstruir parcialment la lògica interna d'un sistema, apropiar-se de la propietat intel·lectual o descobrir patrons que facilitin atacs posteriors. En un entorn on els models representen un avantatge competitiu o una capacitat estratègica, la seva protecció adquireix una rellevància equivalent a qualsevol altre actiu crític.

Les conseqüències d'aquests atacs no sempre es manifesten com a incidents evidents. Un sistema d'intel·ligència artificial compromès pot continuar funcionant aparentment amb normalitat mentre pren decisions errònies, filtra informació delicada o introdueix biaixos que afecten l'equitat i la legalitat dels processos. Aquestes situacions poden derivar en pèrdues econòmiques sostingudes, incompliments reguladors o una erosió progressiva de la confiança, tant interna com externa.

El 2026, la protecció de la intel·ligència artificial s'aborda des d'una perspectiva de **cicle de vida complet**. Cada fase –recopilació de dades, entrenament, validació, desplegament, operació i manteniment– es considera un punt potencial d'exposició que requereix controls específics. La gestió d'accessos, la separació d'entorns, el monitoratge de comportaments anòmals i el registre detallat de decisions es converteixen en elements fonamentals.

La seguretat de la intel·ligència artificial no és només una qüestió tècnica. Té implicacions directes en la governança i la responsabilitat. Definir qui és responsable de les decisions automatitzades, com es validen els models, com es gestionen els canvis i com es garanteix l'explicabilitat dels resultats és essencial, especialment en contextos regulats o en casos d'ús amb impacte directe sobre persones o serveis essencials.

ANDORRA DIGITAL

3

Seguretat de la intel·ligència artificial: protegir els sistemes que prenen decisions

www.anc.ad

ANC-AD

Integrar la seguretat en el disseny i l'operació dels sistemes d'intel·ligència artificial no frena la innovació sinó que la fa sostenible. En un entorn on aquests sistemes adquireixen un pes creixent en la presa de decisions, la seva protecció i la governança es converteixen en condicions imprescindibles per mantenir la confiança i la resiliència de l'ecosistema digital.

ANDORRA DIGITAL

Agència Nacional de Ciberseguretat d'Andorra

4

Prediccions i tendències clau
Ciberseguretat 2026

Evolució dels models de detecció i resposta: del SOC reactiu al centre de decisions

ANDORRA DIGITAL

4

Evolució dels models de detecció i resposta: del SOC reactiu al centre de decisions

www.anc.ad

Durant anys, els models tradicionals d'operació de la ciberseguretat han estat basats en el monitoratge continu de les infraestructures i en la generació de grans volums d'alertes. Aquest enfocament, centrat en la detecció d'esdeveniments individuals, ha demostrat ser cada cop menys eficaç davant d'un entorn d'amenaces caracteritzat per la discreció, l'ús de credencials legítimes i la combinació de tècniques de perfil baix.

El 2026 aquest model arriba a un punt d'inflexió. L'acumulació de senyals de seguretat provinents de múltiples fonts –usuaris, identitats, dispositius, aplicacions, entorns *cloud*, xarxes i sistemes industrials– genera una complexitat que resulta difícil de gestionar mitjançant enfocaments purament reactius. El risc no resideix únicament en la manca d'informació, sinó en la dificultat per **interpretar-la de manera coherent i oportuna**.

L'evolució natural és cap a models de detecció i de resposta orientats a la presa de decisions. En lloc de gestionar alertes aïllades, aquests enfocaments se centren en la identificació d'incidents rellevants, entesos com la correlació de múltiples senyals que, en conjunt, indiquen un comportament anòmal amb impacte potencial. La pregunta deixa de ser «què ha passat» per passar a ser «què significa i quin impacte pot tenir.»

L'anàlisi de comportament adquireix un paper central en aquest canvi de paradigma. En un context en què els atacants fan servir tècniques sense codi maliciós, moviments laterals discrets i credencials vàlides, és imprescindible comprendre com es comporten normalment els usuaris, els sistemes i els processos. Les desviacions subtils -accessos fora de patró, seqüències d'accions inusuals o usos anòmals de privilegis- es converteixen en indicadors clau d'activitat maliciosa.

ANDORRA DIGITAL

4

Evolució dels models de detecció i resposta: del SOC reactiu al centre de decisions

www.anc.ad

ANC-AD

La intel·ligència artificial i l'analítica avançada permeten correlacionar aquests senyals i prioritzar-los en funció de la criticitat. Aquest enfocament redueix significativament el soroll operatiu i millora la capacitat de detecció primerenca, la qual cosa evita que incidents rellevants quedin ocults entre milers d'esdeveniments de baix valor.

L'automatització exerceix un paper complementari però essencial. Les tasques repetitives i de risc baix, com l'enriquiment d'alertes, l'aïllament d'actius compromesos o el bloqueig temporal d'accessos, es poden executar de manera automàtica sota criteris prèviament definits. Això allibera capacitat humana per a la investigació avançada, la gestió d'incidents complexos i la coordinació en situacions de crisi.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

5

Prediccions i tendències clau
Ciberseguretat 2026

Infraestructures connectades i risc ciberfísic: quan l'impacte transcendeix el digital

www.anc.ad

ANDORRA DIGITAL

5

Infraestructures connectades i risc ciberfísic: quan l'impacte transcendeix el digital

www.anc.ad

ANC-AD

La convergència creixent entre tecnologies de la informació (IT), tecnologies operacionals (OT) i dispositius de l'Internet de les Coses (IoT) transforma de manera profunda la naturalesa del risc digital. El 2026, els sistemes digitals ja no es limiten a gestionar informació, sinó que controlen i supervisen processos físics essencials per a la producció, el transport, l'energia, la salut i altres serveis crítics.

Aquesta integració aporta beneficis importants en termes d'eficiència, automatització i capacitat de monitoratge. Tot i això, també elimina barreres que durant anys van mantenir relativament aïllats els entorns industrials i operatius. La connexió de sistemes OT a xarxes corporatives i serveis remots amplis de manera significativa la superfície d'atac i exposa infraestructures que no van ser dissenyades originalment per operar en entorns hostils des del punt de vista cibernètic.

Molts sistemes industrials tenen cicles de vida llargs, protocols específics i limitacions tècniques que dificulten l'aplicació de pegats freqüents o canvis ràpids en la configuració. La prioritat històrica d'aquests entorns ha estat la disponibilitat i seguretat física, no la protecció davant d'amenaces digitals sofisticades. Aquesta realitat genera una bretxa entre el nivell d'exposició i la capacitat de resposta, especialment en infraestructures crítiques i processos essencials.

El creixement de l'IoT intensifica aquest repte. Sensors, actuadors i dispositius encastats es despleguen de manera massiva per optimitzar operacions i recopilar dades en temps real. Tot i això, molts d'aquests dispositius no tenen mecanismes d'actualització segurs, fan servir configuracions per defecte o no estan inventariats correctament. El 2026, aquest conjunt heterogeni de dispositius configura un **perímetre invisible**, difícil de gestionar i atractiu per als atacants com a punt d'entrada cap a sistemes més crítics.

ANDORRA DIGITAL

5

Infraestructures connectades i risc ciberfísic: quan l'impacte transcendeix el digital

www.anc.ad

ANC-AD

L'interès dels actors maliciosos pels entorns ciberfísics respon múltiples motivacions. A més de l'impacte econòmic directe, entren en joc factors geopolítics, estratègics i fins i tot de sabotatge. Un atac que alteri un procés industrial, degradi la qualitat d'un servei essencial o que generi incertesa operativa pot tenir conseqüències desproporcionades en comparació amb la complexitat tècnica.

La gestió d'incidents en entorns ciberfísics planteja reptes específics. A diferència dels sistemes purament digitals, aïllar un actiu o interrompre un procés pot tenir conseqüències físiques, operatives o de seguretat per a les persones. Per això, les decisions de resposta s'han de prendre de manera coordinada entre equips de ciberseguretat, operacions, enginyeria i direcció, i s'han d'avaluar amb cura els riscos associats a cada acció.

L'any 2026, les organitzacions més madures aborden la seguretat d'infraestructures connectades des d'una perspectiva integral. El primer pas no sol ser la implantació d'eines avançades, sinó l'obtenció de visibilitat real sobre els actius, les comunicacions i les dependències existents. Sense visibilitat no hi ha control, i sense control no és possible gestionar el risc de manera eficaç.

La segmentació de xarxes, el monitoratge adaptat a protocols industrials, el control d'accessos remots i la definició de plans de resposta específics per a entorns OT i IoT es converteixen en pilars fonamentals de la protecció ciberfísica. Aquests plans han de ser assajats periòdicament mitjançant simulacions realistes que permetin identificar febleses i millorar la coordinació entre equips.

ANDORRA DIGITAL

5

Infraestructures connectades i risc ciberfísic: quan l'impacte transcendeix el digital

www.anc.ad

ANC-AD

La convergència entre el digital i el físic converteix la ciberseguretat en una qüestió directament relacionada amb la seguretat i la continuïtat dels serveis essencials. En aquest escenari, la protecció d'infraestructures connectades es consolida com una prioritat estratègica, l'impacte de la qual transcendeix l'àmbit tecnològic i afecta el conjunt de la societat.

El 2026, els processos de resposta deixen de ser procediments estàtics per convertir-se en fluxos estructurats, versionables i auditables. Definir per endavant com s'actua davant de determinats escenaris redueix la improvisació, millora la coherència de les decisions i facilita la traçabilitat, un aspecte cada cop més rellevant des del punt de vista regulatori i de governança.

Aquest model de centre de decisions reforça també la capacitat de coordinació amb altres àrees de l'organització. La detecció i resposta a incidents no es pot entendre com una activitat aïllada del context operatiu. La col·laboració amb àrees de tecnologia, negoci, comunicació i direcció permet avaluar l'impacte real de l'incident i prendre decisions alineades amb la continuïtat del servei i la gestió del risc.

L'evolució dels models de detecció i resposta no es limita a adoptar noves tecnologies. Implica un canvi profund en la manera d'entendre l'operació de la ciberseguretat: menys centrada en el volum d'alertes i més orientada a la comprensió del risc, la presa de decisions informades i la resiliència del conjunt del sistema.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

6

Prediccions i tendències clau
Ciberseguretat 2026

Identitat digital i frau avançat: el nou perímetre sota pressió constant

ANDORRA DIGITAL

6

Identitat digital i frau avançat: el nou perímetre sota pressió constant

www.anc.ad

ANC-AD

La progressiva desaparició del perímetre tradicional ha situat la identitat digital al centre de la seguretat. El 2026, usuaris, aplicacions, serveis i sistemes accedeixen a recursos des de múltiples ubicacions, a través d'entorns híbrids i distribuïts, fet que converteix les credencials i els mecanismes d'autenticació en el punt de control principal… i, alhora, en un dels vectors d'atac més explotats.

Des de la perspectiva dels actors maliciosos, comprometre una identitat legítima resulta, en molts casos, més eficaç i menys visible que no pas explotar una vulnerabilitat tècnica. L'ús de credencials vàlides permet moure's dins dels sistemes amb aparença de legitimitat, endarrereix la detecció i augmenta l'impacte potencial de l'atac. Aquesta realitat explica perquè molts incidents greus no comencen amb tècniques sofisticades, sinó amb l'abús d'accessos existents.

L'enginyeria social, tradicionalment un dels principals mecanismes per obtenir credencials, entra el 2026 en una nova fase de sofisticació. L'ús de la intel·ligència artificial permet crear missatges, trucades i comunicacions altament creïbles, adaptades al context i al perfil de la víctima. Els hipertrucatges (*deepfakes*) de veu i vídeo faciliten suplantacions difícils de detectar, fins i tot per a usuaris experimentats, i es fan servir per pressionar emocionalment o accelerar la presa de decisions.

L'impacte d'aquestes tècniques es manifesta especialment en l'augment del frau corporatiu. Processos financers, canvis de comptes bancaris, autoritzacions excepcionals o accessos privilegiats es converteixen en objectius prioritaris. El component psicològic de l'atac –urgència, autoritat aparent, pressió– es combina amb el realisme tecnològic per augmentar la probabilitat d'èxit.

ANDORRA DIGITAL

6

Identitat digital i frau avançat: el nou perímetre sota pressió constant

www.anc.ad

ANC-AD

L'autenticació multifactor es manté com un control essencial, però el 2026 se n'evidencien les limitacions quan s'aplica de manera aïllada. Tècniques com la saturació de sol·licituds, el segrest de sessions o la manipulació de l'usuari permeten eludir mecanismes que, des del punt de vista tècnic, funcionen correctament. Això fa palès que no tots els factors d'autenticació ofereixen el mateix nivell de resistència davant d'atacs avançats.

En aquest escenari, la gestió d'identitats evoluciona cap a enfocaments més dinàmics i continus. La defensa ja no es pot basar únicament a verificar qui és l'usuari en el moment de l'accés, sinó també en **com es comporta**, des d'on accedeix i en quin context opera. La detecció d'anomalies de comportament es converteix en una eina clau per identificar accessos fraudulents que, altrament, semblarien legítims.

Les identitats privilegiades adquireixen una rellevància especial. Un únic compromís pot atorgar control sobre sistemes crítics, facilitar la persistència de l'atacant i permetre moviments laterals gairebé sense fricció. Per això, la gestió d'aquests accessos deixa de ser un projecte puntual per convertir-se en un procés continu de control, revisió i monitoratge.

El 2026, protegir la identitat digital exigeix una aproximació integral que combini tecnologia, processos i persones. Dissenyar fluxos d'accés segurs, limitar privilegis, aplicar controls adaptatius i formar els usuaris per reconèixer intents de frau sofisticats és tan important com desplegar mecanismes tècnics avançats.

La identitat es consolida així com el nou perímetre de seguretat. La seva protecció efectiva no només redueix el risc d'intrusió, sinó que reforça la confiança en els sistemes digitals i contribueix de manera decisiva a la resiliència de l'ecosistema en conjunt.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

7

Prediccions i tendències clau
Ciberseguretat 2026

Criptografia postquàntica: anticipar-se avui a un risc de llarg recorregut

www.anc.ad

ANDORRA DIGITAL

ANC-AD

7

Criptografia postquàntica: anticipar-se avui a un risc de llarg recorregut

www.anc.ad

La computació quàntica continua avançant de forma progressiva i, encara que el 2026 no representa encara una amenaça immediata per als sistemes criptogràfics àmpliament utilitzats, sí que introdueix un canvi rellevant en la manera de gestionar el risc a llarg termini. La preocupació no se centra en la capacitat actual de trencar els algorismes de xifratge, sinó en la **durabilitat de la confidencialitat de la informació** que es protegeix avui.

Determinades dades —informació governamental, registres personals, historials mèdics, contractes estratègics, propietat intel·lectual o secrets industrials— mantenen el valor durant dècades. En aquest context, la possibilitat que informació xifrada actualment pugui ser emmagatzemada per un adversari i desxifrada en el futur converteix la criptografia postquàntica en una qüestió de planificació estratègica més que no pas de reacció immediata.

Aquest enfocament, conegut com «recollir ara i desxifrar després», ja forma part de les consideracions de determinats actors avançats. Encara que els ordinadors quàntics capaços d'executar atacs criptogràfics a gran escala encara no estiguin disponibles, la protecció de la informació amb llarga vida útil exigeix anticipació i previsió.

La transició cap a algoritmes resistents a la computació quàntica presenta una complexitat significativa. La criptografia no és un component aïllat que es pugui substituir de manera senzilla. Està integrada a múltiples capes de l'arquitectura tecnològica: aplicacions, sistemes operatius, protocols de comunicació, infraestructures de clau pública, dispositius, certificats i serveis de tercers. En molts casos, les organitzacions no disposen d'una visió clara de quins algoritmes fan servir realment ni d'on es gestionen les claus criptogràfiques.

ANDORRA DIGITAL

7

Criptografia postquàntica: anticipar-se avui a un risc de llarg recorregut

www.anc.ad

ANC-AD

El 2026, el primer repte no és migrar, sinó **comprendre l'exposició real**. Inventariar els mecanismes criptogràfics existents, identificar dependències i classificar la informació en funció de la seva criticitat i vida útil és essencial per a qualsevol planificació coherent. Sense aquest coneixement previ, qualsevol intent de transició corre el risc de generar inestabilitat o deixar àrees crítiques desprotegides.

Les estratègies que comencen a consolidar-se en aquest període són deliberadament graduals. En comptes d'una substitució immediata, s'adopten enfocaments híbrids que combinen algorismes clàssics amb alternatives postquàntiques en entorns controlats. Aquestes proves permeten avaluar l'impacte en rendiment, compatibilitat i operativa sense comprometre l'estabilitat dels sistemes productius.

La criptografia postquàntica adquireix també una dimensió de confiança i compliment. La capacitat de demostrar que la informació delicada està protegida davant de riscos futurs es converteix en un element cada cop més valorat per reguladors, socis i ciutadans. Anticipar-se a aquest repte reforça la percepció de maduresa i responsabilitat en la gestió del risc digital.

El 2026, la criptografia postquàntica no és encara una urgència operativa, però sí una **prioritat estratègica emergent**. Les organitzacions que ignorin aquest debat poden acumular un deute tècnic difícil de gestionar sota pressió en el futur. Per contra, les que comencin a analitzar-ne l'exposició, ordenar-ne l'arquitectura criptogràfica i planificar de manera progressiva estaran més ben preparades per afrontar un canvi que, amb el temps, serà inevitable.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

8

Arquitectures *Zero Trust*: de principi teòric a model operatiu consolidat

Prediccions i tendències clau
Ciberseguretat 2026

ANDORRA DIGITAL

ANC-AD

8

Arquitectures *Zero Trust*: de principi teòric a model operatiu consolidat

www.anc.ad

Durant anys, l'enfocament *Zero Trust* ha estat presentat com a paradigma de referència per a la seguretat en entorns digitals moderns. Tot i això, en moltes organitzacions la seva adopció s'ha quedat en iniciatives parcials o en interpretacions excessivament simplificades. El 2026, aquesta situació evoluciona de manera clara: *Zero Trust* deixa de ser un concepte amb aspiracions per convertir-se en un **model operatiu aplicat de manera progressiva i coherent**.

La raó de fons és estructural. El perímetre tradicional, basat en la distinció entre xarxes internes i externes, ha deixat d'existir. Usuaris que treballen des de múltiples ubicacions, aplicacions distribuïdes en diferents núvols, serveis SaaS, accessos de tercers i dispositius no gestionats fan inviable qualsevol model basat en la confiança implícita. En aquest context, assumir que alguna cosa és fiable per la ubicació suposa un risc inassumible.

Zero Trust parteix d'una premissa fonamental: **no confiar per defecte i verificar sempre**. A la pràctica, això implica que cada accés a un recurs ha de ser avaluat en funció de la identitat, el context i el nivell de risc associat, independentment d'on s'origini la connexió. L'any 2026, aquest principi es materialitza en controls continus i dinàmics, que van més enllà d'una autenticació inicial.

La identitat esdevé l'eix central de l'arquitectura. No només es gestionen identitats humanes sinó també identitats d'aplicacions, serveis, càrregues de treball i processos automatitzats. Cadascuna disposa de permisos específics, alineats amb el principi de privilegi mínim: accedir únicament a allò que sigui necessari, durant el temps imprescindible i sota les condicions adequades.

ANDORRA DIGITAL

ANC-AD

8

Arquitectures *Zero Trust*: de principi teòric a model operatiu consolidat

www.anc.ad

La microsegmentació és un dels pilars tècnics que permeten materialitzar aquest enfocament. En lloc de grans dominis de confiança, es defineixen segments lògics fins, adaptats a aplicacions, fluxos de comunicació o serveis concrets. Aquesta segmentació limita de manera efectiva el moviment lateral i redueix l'impacte d'un compromís inicial, fins i tot quan l'atacant aconsegueix accedir a un entorn legítim.

Un altre element diferenciador del *Zero Trust* madur és l'accés adaptatiu basat en risc. No tots els accessos presenten el mateix nivell d'exposició ni requereixen el mateix grau de control. En funció del comportament observat, la criticitat del recurs o l'existència de senyals d'amenaça actius, el sistema pot reforçar les mesures d'autenticació, limitar funcionalitats o bloquejar-ne l'accés temporalment.

El 2026 queda clar que *Zero Trust* no és un producte que s'adquireix ni una solució que s'implanta de manera puntual. És un **procés continu** que exigeix redissenyar fluxos d'accés, revisar permisos històrics, integrar múltiples capacitats tècniques i, en molts casos, canviar la mentalitat organitzativa al voltant de la confiança i el control.

L'adopció efectiva de *Zero Trust* és progressiva. Les organitzacions prioritzen actius crítics i casos d'ús d'alt impacte, per avançar de manera incremental cap a un model més consistent. Aquest enfocament permet equilibrar seguretat i operativitat, evita disrupcions innecessàries i facilita l'acceptació dels usuaris.

En un entorn caracteritzat per la complexitat i la interdependència, les arquitectures *Zero Trust* proporcionen una base sòlida per gestionar el risc de forma més predictible. La seva consolidació el 2026 reforça la capacitat de les organitzacions per operar amb més seguretat, millorar la visibilitat i establir les bases d'una resiliència digital sostenible.

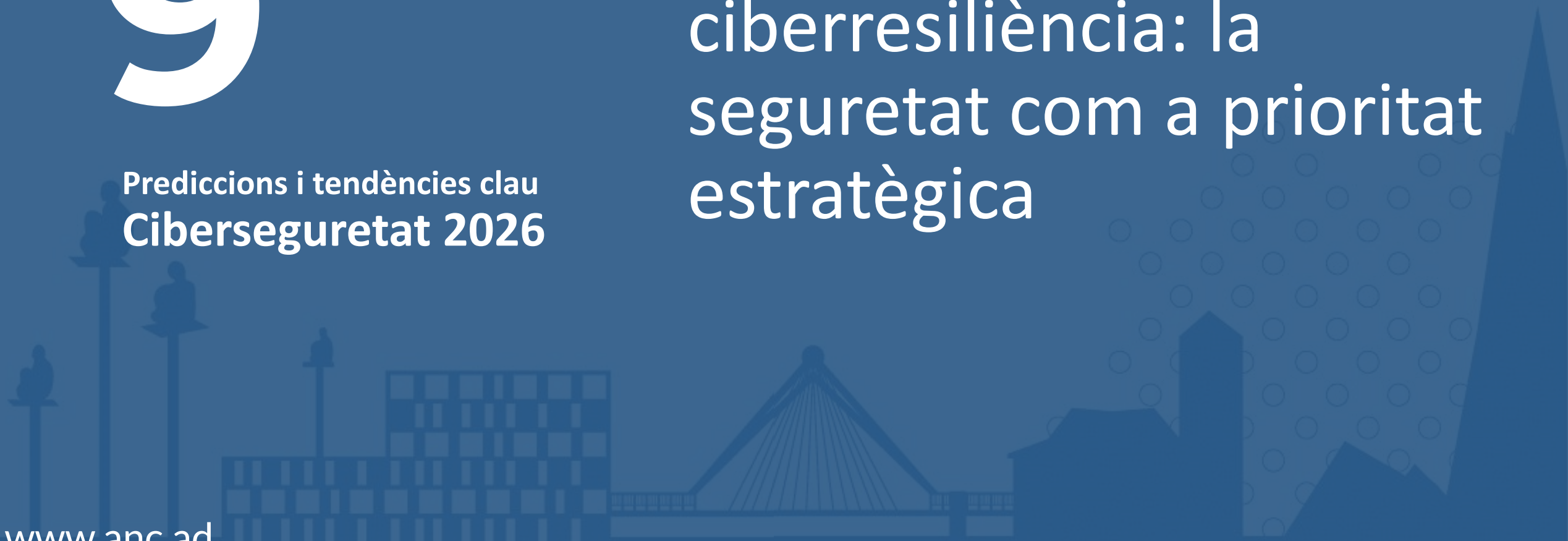
ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

9

Prediccions i tendències clau
Ciberseguretat 2026

Governança, notificació i ciberresiliència: la seguretat com a prioritat estratègica



www.anc.ad

ANDORRA DIGITAL

9

Governança, notificació i ciberresiliència: la seguretat com a prioritat estratègica

www.anc.ad

ANC-AD

El 2026, la ciberseguretat deixa d'avaluar-se únicament des d'una perspectiva tècnica per convertir-se en un **element central de la governança i la gestió del risc**. La pressió reguladora creixent, la visibilitat pública dels incidents i la interdependència entre organitzacions obliguen a demostrar capacitats reals, més enllà de declaracions d'intenció o del compliment formal de controls mínims.

Durant anys, l'enfocament regulador s'ha centrat en l'existència de polítiques, procediments i mesures de protecció documentades. Aquest plantejament, però, és insuficient davant d'amenaces complexes i dinàmiques. A l'escenari actual, reguladors, socis i ciutadania demanen evidències pràctiques: capacitat de detecció primerenca, eficàcia en la resposta, plans assajats i traçabilitat en la presa de decisions.

La ciberresiliència es consolida així com un concepte clau. No es tracta únicament de prevenir incidents, sinó d'**absorbir-ne l'impacte, mantenir els serveis essencials i recuperar l'operativa en terminis acceptables**. Aquesta capacitat s'ha d'integrar a la gestió global del risc, al mateix nivell que altres riscos estratègics, financers o operatius.

Un dels àmbits on aquesta exigència es manifesta amb més claredat és la notificació (*reporting*) d'incidents. El 2026 moltes organitzacions estan obligades a notificar incidents rellevants en terminis molt ajustats, sovint d'hores o pocs dies. Complir aquestes obligacions requereix processos clars, rols definits i fluxos de decisió prèviament acordats. La improvisació, especialment en contextos de gran incertesa, incrementa el risc d'errors i missatges incoherents.

ANDORRA DIGITAL

9

Governança, notificació i ciberresiliència: la seguretat com a prioritat estratègica

www.anc.ad

ANC-AD

La coordinació entre àrees tècniques, legals, de comunicació i direcció és essencial. La gestió d'un incident ja no es pot abordar de manera aïllada des del punt de vista tecnològic. La capacitat de comunicar de manera transparent, precisa i alineada amb les obligacions regulatòries és tan important com la resposta tècnica pròpiament dita.

La cadena de subministrament digital adquireix també un paper central a la governança de la ciberseguretat. L'any 2026, la seguretat ja no s'avalua únicament dins els límits d'una organització. Proveïdors, socis tecnològics i tercers amb accés a sistemes o dades es consideren una extensió del mateix perímetre de risc. Un incident en un proveïdor crític pot generar conseqüències legals, operatives i reputacionals equiparables a un incident intern.

Aquesta realitat obliga a establir mecanismes sistemàtics d'avaluació, supervisió i gestió del risc de tercers. Exigir evidències mínimes de seguretat, definir clàusules contractuals clares i monitorar de manera contínua el nivell d'exposició de l'ecosistema esdevenen pràctiques indispensables.

Un altre canvi significatiu és la implicació de l'alta direcció. El 2026, la ciberseguretat s'integra de manera explícita a l'agenda dels òrgans de direcció i govern. La demanda de mètriques comprensibles, alineades amb l'impacte en negoci i serveis essencials, reforça el diàleg entre àrees tècniques i executives.

ANDORRA DIGITAL

9

Governança, notificació i ciberresiliència: la seguretat com a prioritat estratègica

www.anc.ad

ANC-AD

Indicadors com ara els temps de detecció, resposta i recuperació, l'impacte màxim tolerable o el grau de cobertura d'actius crítics permeten avaluar de manera objectiva el nivell de resiliència. Aquestes mètriques faciliten la presa de decisions estratègiques i reforcen la rendició de comptes.

La governança eficaç de la ciberseguretat no sols redueix el risc de sancions o incidents greus, sinó que reforça la confiança de ciutadans, clients i socis. En un entorn on la seguretat digital es percep com un element essencial de la fiabilitat institucional, la ciberresiliència es consolida com un **KPI estratègic de primer nivell**.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

10

Talent i cultura de seguretat: el factor humà com a element decisiu

Prediccions i tendències clau
Ciberseguretat 2026

ANDORRA DIGITAL

10

Talent i cultura de seguretat: el factor humà com a element decisiu

www.anc.ad

ANC-AD

En un context marcat per l'automatització, la intel·ligència artificial i la sofisticació tecnològica creixent, es podria pensar que el factor humà perd rellevància en la ciberseguretat. Tot i això, el 2026 passa exactament el contrari: **les persones es consoliden com a element decisiu** que determina l'eficàcia real de qualsevol estratègia de protecció i resiliència digital.

La tecnologia és imprescindible per gestionar la complexitat de l'entorn actual, però no n'hi ha prou per si sola. Les decisions crítiques, la interpretació del context, la gestió de crisis i la capacitat d'adaptació davant d'escenaris imprevistos continuen depenent del criteri humà. La ciberseguretat del futur es basa en sistemes avançats, però es construeix sobre equips preparats, processos clars i una cultura organitzativa sòlida.

El rol del professional de ciberseguretat experimenta una transformació significativa. L'automatització i la intel·ligència artificial assumeixen tasques repetitives i de baix valor afegit, com ara la gestió inicial d'alertes o l'execució d'accions estàndard de resposta. Això allibera temps i recursos per a activitats de més impacte, com ara l'anàlisi avançada, la investigació d'incidents complexos i la interlocució amb altres àrees de l'organització.

El 2026, els perfils evolucionen des de rols purament tècnics cap a **perfils híbrids**, capaços de connectar la ciberseguretat amb el negoci, les operacions i el context regulatori. Aquesta transversalitat és essencial per comprendre l'impacte real dels incidents, prioritzar adequadament les accions i comunicar el risc de manera comprensible a la direcció.

ANDORRA DIGITAL

10

Talent i cultura de seguretat: el factor humà com a element decisiu

www.anc.ad

ANC-AD

L'escassetat de talent especialitzat continua sent una realitat, però canvia l'enfocament. Més enllà de la captació de perfils altament tècnics, la **retenció** esdevé important, com també la formació contínua i el desenvolupament de capacitats internes. Invertir en el creixement professional dels equips no sols millora la capacitat tècnica, sinó que reforça el compromís i redueix la dependència de recursos externs en situacions crítiques.

La intel·ligència artificial actua com un amplificador de capacitats, no com un substitut del factor humà. Els sistemes de suport a l'anàlisi, els assistents de recerca i l'automatització de respostes permeten que els equips més reduïts gestionin entorns més complexos. Això no obstant, aquesta dependència tecnològica exigeix un nivell elevat de maduresa: la supervisió humana, la validació de decisions i la capacitat d'intervenir manualment continuen sent imprescindibles per evitar errors o abusos.

La cultura de seguretat es consolida com a element transversal. El 2026, les organitzacions més resilients són aquelles on la ciberseguretat no es percep com una responsabilitat exclusiva d'un departament, sinó com una **responsabilitat compartida**. Els empleats comprenen els riscos, coneixen el seu paper en la protecció de l'organització i disposen d'eines i de formació adaptades a la seva funció.

La conscienciació evoluciona des de formacions genèriques cap a programes específics per rol, amb continguts pràctics i escenaris realistes. Simulacions de pesca, exercicis de resposta a incidents i proves de gestió de crisis s'integren de manera habitual a la vida de l'organització. Aquests exercicis no només milloren la preparació tècnica, sinó que enforteixen la coordinació i la confiança entre equips.

ANDORRA DIGITAL

10

Talent i cultura de seguretat: el factor humà com a element decisiu

www.anc.ad

La implicació de l'alta direcció és determinant. Quan els líders participen activament en la gestió del risc digital i donen suport a les iniciatives de seguretat, es reforça el missatge que la ciberseguretat és una prioritat estratègica. El 2026, les organitzacions on la direcció lidera amb l'exemple mostren més capacitat de resposta i una millor gestió de les situacions de crisi.

Invertir en talent i cultura de seguretat no és una despesa operativa, sinó una **inversió en resiliència**. Les organitzacions amb equips preparats, alineats i compromesos cometen menys errors, responen millor als incidents i es recuperen amb més rapidesa. En un entorn d'amenaces cada cop més sofisticades, el factor humà continua sent l'element que marca la diferència.

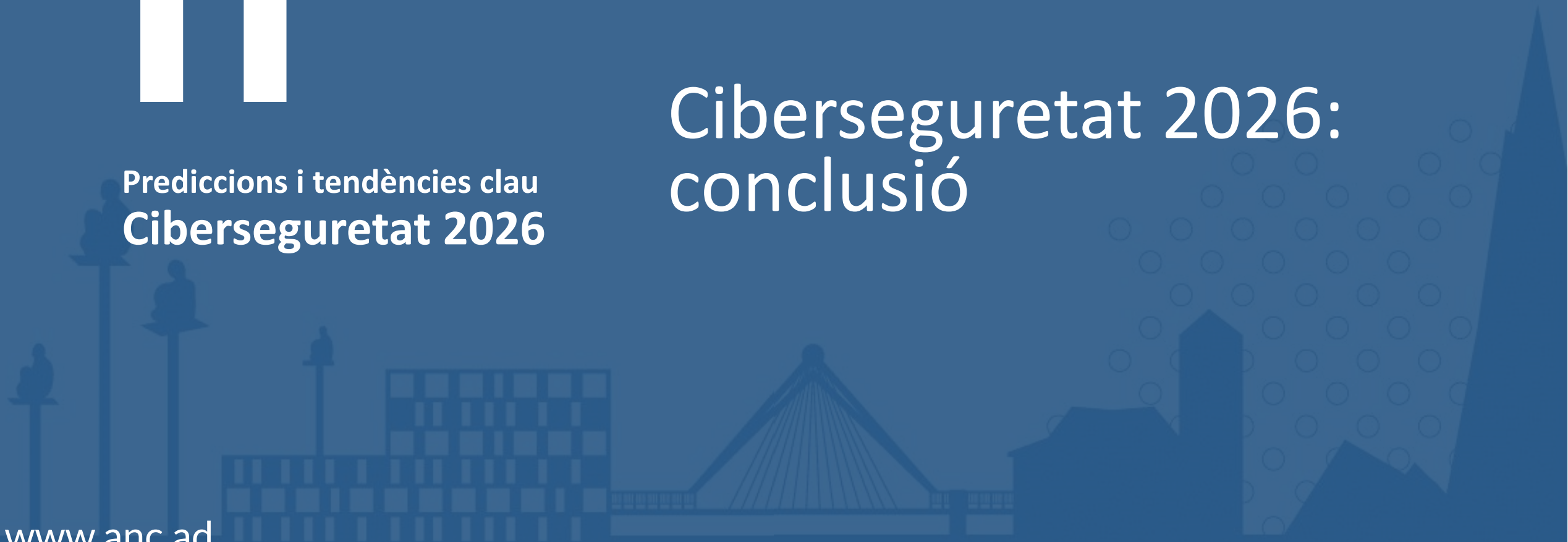
ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

11

Prediccions i tendències clau
Ciberseguretat 2026

Ciberseguretat 2026: conclusió



www.anc.ad

ANDORRA DIGITAL

11

Ciberseguretat 2026: conclusió

www.anc.ad

ANC-AD

L'anàlisi del panorama de la ciberseguretat el 2026 posa de manifest una realitat inqüestionable: el risc digital ha esdevingut un element estructural de les nostres societats i economies. La dependència creixent de sistemes interconnectats, la digitalització de serveis essencials i l'adopció de tecnologies avançades han ampliat de manera irreversible la superfície d'exposició i la complexitat de l'entorn d'amenaces.

Les tendències descrites en aquest document reflecteixen un canvi profund en la naturalesa dels riscos. Els ciberatacs ja no es limiten a comprometre sistemes aïllats ni provocar interrupcions temporals. El seu impacte pot ser sistèmic, i afectar la continuïtat de serveis essencials, la confiança de la ciutadania, l'estabilitat institucional i la competitivitat econòmica. En aquest context, la ciberseguretat deixa de ser un assumpte operatiu per consolidar-se com una **prioritat estratègica de primer nivell**.

L'experiència demostra que la prevenció absoluta no és un objectiu realista. Fins i tot les organitzacions amb més nivells de maduresa poden veure's afectades per incidents complexos i persistents. Per això, la resiliència es consolida com l'eix central de l'estratègia de ciberseguretat: la capacitat d'anticipar amenaces, detectar incidents amb rapidesa, limitar-ne l'impacte i recuperar l'operativa en terminis assumibles.

Construir aquesta resiliència requereix una aproximació integral. La tecnologia és un habilitador essencial, però no suficient per si sola. És necessari combinar capacitats tècniques avançades amb processos ben definits, marcs de governança clars i una cultura de seguretat compartida. La coordinació entre actors públics i privats, com també la gestió del risc al llarg de tota la cadena de subministrament digital, esdevenen factors determinants.

ANDORRA DIGITAL

11

Ciberseguretat 2026: conclusió

www.anc.ad

ANC-AD

Així mateix, el paper de l'alta direcció és clau. Integrar la ciberseguretat en la governança corporativa i en la gestió global del risc permet alinear les decisions tècniques amb els objectius estratègics i garantir una resposta coherent en situacions de crisi. La definició de mètriques clares i comprensibles facilita la presa de decisions informades i reforça la rendició de comptes.

Les persones continuen sent un element decisiu. En un entorn cada cop més automatitzat, el criteri humà, la formació contínua i la cultura de seguretat marquen la diferència entre organitzacions vulnerables i organitzacions resilients. Invertir en talent, conscienciació i preparació pràctica és una inversió directa en estabilitat i confiança.

Mirant cap al futur, el repte no resideix únicament a adaptar-se a les amenaces actuals, sinó a desenvolupar la capacitat d'evolucionar de manera contínua. La ciberseguretat és un procés dinàmic que exigeix revisió constant, aprenentatge i col·laboració. Anticipar els riscos emergents, planificar amb visió a llarg termini i reforçar la cooperació entre actors serà fonamental per afrontar amb èxit els desafiaments que es consoliden més enllà del 2026.

Garantir un entorn digital segur, fiable i sostenible no és una tasca puntual sinó un compromís permanent. La ciberseguretat s'erigeix així en un dels pilars fonamentals per a la continuïtat dels serveis essencials, la confiança de la ciutadania i el desenvolupament d'una societat digital resilient.

ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Prediccions i tendències clau

Ciberseguretat 2025

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