

Informe de Ciberintel·ligència

Com adaptar-se a la nova era de la IA: quatre prioritats per a la ciberresiliència d'Andorra



TLP: WHITE

OCTUBRE 2026

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	19/10/2026	21/10/2026

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD
-------------------------	--------

ÍNDEX

1. METODOLOGIA	4
2. INTRODUCCIÓ	5
3. QUÈ ESTÀ CANVIANT?	7
3.1. De l'assistència a l'automatització de l'atac	7
3.2. Els agents de la IA com a nova superfície d'atac	8
3.3. La compressió del temps d'atac	10
3.4. Què s'ha demostrat a partir del que s'ha observat	11
4. COM ADAPTAR-SE: QUATRE PRIORITATS I CINCPRINCIPIS	13
5. PRIORITAT 1: AUTOMATITZAR LA DEFENSA	15
5.1. Per què és necessària	15
5.2. Què implica	15
5.3. Què no convé automatitzar	16
5.4. Mesures	17
6. PRIORITAT 2: REDUIR L'EXPOSICIÓ	19
6.1. Per què és necessària	19
6.2. Què implica	19
6.3. Els agents de la IA com a identitats	20
6.4. Mesures	21
7. PRIORITAT 3: PREPARAR-SE PER AL FUTUR QUÀNTIC	23
7.1. Per què és necessària	23
7.2. Quins actius i sistemes es veuen afectats	24
7.3. Què implica	25
7.4. Mesures	25
8. PRIORITAT 4: COORDINAR-SE COM A PAÍS	27
8.1. Per què és necessària	27
8.2. Què implica	28
8.3. Mesures	29
9. CONCLUSIONS	31
10. ANNEX	33
11. CLÀUSULA DE CONFIDENCIALITAT	40

1. METODOLOGIA

Aquest informe aplica els principis del Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi millor d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir TLP:RED quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a TLP:RED amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir TLP:AMBER quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a TLP:AMBER només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir TLP:GREEN quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a TLP:GREEN amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir TLP:WHITE quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació TLP:WHITE pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

El 21 de setembre de 2026, el DIVD (Dutch Institute for Vulnerability Disclosure) va patir un ciberatac; concretament, una intrusió a la seva xarxa. El DIVD és una organització dels Països Baixos sense ànim de lucre, formada per voluntaris, que localitza sistemes exposats a Internet i n'avisava els propietaris. L'atacant va encadenar dues vulnerabilitats fins aleshores desconegudes a la plataforma de gestió de tiquets de l'organització, i va passar d'una sessió segrestada a tenir el control total del servidor. **Segons el mateix DIVD, darrere del ciberatac no hi havia cap persona executant l'atac, sinó un agent de la IA que decidia per ell mateix què fer després de cada acció.**

El DIVD ho va descriure com «un atac que no havíem vist mai». La segmentació de la xarxa va limitar l'abast del ciberatac, però l'organització va confirmar posteriorment que se n'havien extret dades. En la data d'elaboració d'aquest informe, la investigació continua oberta, ningú no ha reivindicat l'atac i no s'hi ha identificat cap operador humà al darrere. Que l'atacant fos un agent autònom és una valoració del mateix DIVD a partir de la seva anàlisi forense, no un fet verificat per tercers.

L'informe del setembre recollia que Google encara no havia observat que hi hagués atacants que despleguessin cadenes d'atac totalment autònomes contra objectius reals. Aquell mateix mes, Anthropic va publicar el seu informe d'amenaçes, en el qual descriu campanyes reals en què els agents de la IA van fer gairebé tota la feina, des del robatori de credencials i l'escaneig fins a l'extracció de dades. Això no vol dir que l'amenaça hagi canviat d'un dia per l'altre, però sí que **la distància entre el fet demostrat en laboratori i el fet observat en intrusions reals s'està escurçant.**

Els dos informes anteriors es van centrar en l'amenaça: què poden fer els models de frontera i què canvia per a l'atacant. Aquest informe fa el pas següent i se centra en la resposta: **què ha de canviar en la manera de defensar una organització, i un país, quan part de l'atac s'executa a velocitat de màquina.**

Tot seguit, es mostra una taula sobre què cobrirà l'informe i què no:

Què cobreix aquest informe
Com està canviant l'amenaça amb la IA generativa i agentiva, a partir dels casos documentats el setembre i l'octubre del 2026.
Les quatre prioritats per adaptar-se: automatitzar la defensa, reduir l'exposició, preparar-se per al futur quàntic i coordinar-se com a país.
Mesures concretes per a cada prioritat, amb el seu horitzó temporal.
L'ús defensiu legítim i els seus límits.
Què no cobreix aquest informe
L'anàlitzat als informes de maig i setembre: capacitats de models concrets i polítiques dels proveïdors.

El catàleg d'atacs contra models de la IA, ja tractat a la documentació compartida prèviament.

Mètodes o instruccions d'ús ofensiu, i recomanacions de productes o fabricants concrets.

Taula 1 - Què cobreix aquest informe i què no

3. QUÈ ESTÀ CANVIANT?

L'apartat següent resumeix els tres canvis que justifiquen les prioritats de l'informe: l'atac s'automatitza, els agents de la IA obren una nova superfície d'atac dins de les organitzacions i els temps s'escurcen.

3.1. De l'assistència a l'automatització de l'atac

L'informe de setembre conclouïa que els atacants estaven incorporant la IA a poc a poc a la forma habitual de treballar. Aconsegueixen ser més ràpids i eficients, però les decisions de pes les continuen prenent persones. Aquesta conclusió continua sent vàlida per a la majoria dels casos, però ja no descriu tot allò que es veu.

Els diferents casos documentats entre juliol i octubre del 2026 permeten veure amb més detall què fa la IA i què continua fent una persona:

Cas	Qui ho documenta	Què va fer la IA	Paper de la persona
JadePuffer (juliol 2026)	Sysdig	Va executar un atac de programari de segrest complet. Va entrar aprofitant una vulnerabilitat coneguda d'una eina, va robar credencials, es va moure fins a una base de dades de producció, va xifrar més de 1.300 registres de configuració i va deixar una nota de rescat.	No identificat. Sysdig ho considera el primer cas documentat de programari de segrest executat per complet per un agent de la IA.
Afiliats de ShinyHunters	Anthropic	Avaluava l'entorn, escrivia i executava scripts i repetia fins a completar cada tasca. En un cas va passar d'un token de desenvolupador al control total de l'entorn <i>cloud</i> de la víctima en unes tres hores.	Fixar els objectius generals. Segons Anthropic, els agents de la IA van fer gairebé tota la feina.
Grup d'espionatge de parla xinesa	Anthropic	Un agent principal repartia el reconeixement i la postexploitació entre subagents, i tretze agents de recol·lecció funcionaven de manera programada. En un mes va identificar més d'una dotzena de possibles vulnerabilitats desconegudes.	Les intrusions directes sobre les víctimes les van dirigir persones.
Campanya hacktivista	Anthropic	Reconeixement, revisió de codi i desenvolupament i depuració d'un <i>exploit</i> per a una vulnerabilitat desconeguda. Va aconseguir accés intern almenys a 14 de les 42	Un únic operador. Segons Anthropic, tota la plataforma la va crear una sola persona.

		organitzacions objectiu identificades: partits polítics, mitjans i centres d'estudis europeus.	
Grup d'espionatge vinculat a Rússia	Anthropic	Quan els seus implants eren detectats, els agents modificaven i reconstruïen el codi maliciós de forma autònoma. Va atacar més de 20 organitzacions, principalment a Ucraïna i Europa.	Ajustar les instruccions que guiaven la feina dels agents.

Taula 2 - Casos documentats d'automatització de l'atac (juliol-octubre 2026)

Els quatre casos diferents documentats per Anthropic corresponen a l'activitat detectada a la seva pròpia plataforma i descrita pel mateix proveïdor.

De tots els casos documentats, se'n treuen 4 idees clau per a la defensa:

- **Una persona pot fer la feina d'un equip:** la IA ha reduït la distància en treball i eines.
- **La sofisticació ja no indica qui hi ha al darrere:** un atac tècnicament avançat no implica necessàriament un actor estatal. Segons Anthropic, la diferència passa a ser la intenció, no pas la capacitat.
- **Objectius abans marginals passen a ser rendibles:** les organitzacions petites i mitjanes, que abans podien quedar fora del focus perquè atacar-les no compensava l'esforç, entren al radar.
- **Autonomia no és el mateix que gravetat:** diversos dels compromisos més greus van tenir una persona dirigint cada pas.

Cap d'aquests casos demostra que l'atac totalment autònom ja sigui la norma. El que demostren és que el cost d'atacar està disminuint, i que la defensa ja no pot comptar que a l'atacant li costi esforç arribar-hi.

3.2. Els agents de la IA com a nova superfície d'atac

Fins ara, el risc de la IA dins d'una organització era sobretot un risc de dades, és a dir, un empleat que copia i enganxa informació delicada a un xatbot. Amb els agents canvia la naturalesa del problema. Un agent no només respon, també actua: té accés a eines, dades, API keys i credencials, i les executa en nom d'una persona. Mandiant, al seu informe especial sobre el risc de la IA del setembre del 2026, parla d'aquest pas: la IA empresarial ha passat d'eines de consulta a sistemes que anomenen API, canvien configuracions de producció i actuen sobre entorns *cloud*.

Hi ha 3 característiques que fan que un agent sigui diferent d'una aplicació tradicional:

- **Rep instruccions de fonts que no controla**
- **Actua amb credencials i permisos reals**
- **Depèn de peces de tercers**

Els diferents casos documentats el 2026 mostren com es combinen aquestes característiques.

Cas	Tipus	Què va passar	Què ho va fer possible
Assistent de programació segrestat (Mandiant)	Incident real	Un atacant va segrestar la sessió d'un assistent de programació a l'equip d'un desenvolupador. L'assistent va recomanar instal·lar un paquet enverinat, es van robar tokens de GitHub i es va desplegar un cuc en uns 100 repositoris interns de codi.	Confiança a les dependències recomanades per la IA, tokens de llarga durada accessibles i sortida a Internet sense restringir.
Bucle sense control (Mandiant, proveïdor de serveis financers)	Incident real, sense agressor.	Un agent amb accés de lectura i escriptura a bases de dades de facturació va entrar en un bucle en fallar una de les eines. En menys d'una hora va generar més de 15.000 trucades, una despesa d'uns 50.000 dòlars i bloquejos a la base de dades que van paralitzar les transaccions.	Sense límits de repetició ni de cost, i amb més privilegis dels necessaris.
Proveïdor de la IA compromès (Anthropic)	Incident real	Un grup de delinqüents va introduir instruccions a l'entorn d'avaluació automatitzat d'un proveïdor de la IA, que va acabar lliurant les credencials, incloses claus d'API de producció.	Un sistema automatitzat processava contingut extern amb les credencials de producció que tenia al seu abast.
SalesBleed (Zenity Labs, Salesforce Agentforce)	Investigació, ja corregida	Un formulari web públic amb instruccions ocultes. Quan un empleat va preguntar al seu agent pels darrers contactes comercials, l'agent va seguir aquestes instruccions i va extreure dades de clients.	Contingut d'un formulari públic tractat com a fiable, i un agent amb accés a més dades de les que requeria la tasca.
AWS AgentCore (Unitat 42, Palo Alto Networks)	Investigació	Un tiquet de suport amb instruccions ocultes va fer que l'agent executés un script que va llegir de memòria les credencials d'un compte de servei. Aquestes credencials es	Eina d'execució d'ordres activada per defecte, compte de servei amb privilegis amplis i sense control del trànsit de sortida.

		van reutilitzar des de fora per consultar dades personals de clients.	
--	--	---	--

Taula 3 - Casos documentats d'abús o error d'agents de la IA el 2026

Cap d'aquests casos no va requerir una vulnerabilitat al model de la IA com a tal. **El problema va estar als permisos, les credencials i la configuració del que envolta l'agent.** A gairebé tots coincideixen tres condicions: l'agent processa contingut que no és de confiança, té accés a dades o eines delicades i es pot comunicar cap a fora. Quan es donen totes tres, qui aconsegueixi escriure en tot allò que l'agent llegeix pot actuar amb els seus permisos.

En el cas d'AWS, el proveïdor va tancar l'informe indicant que els controls necessaris corresponen al client: la responsabilitat de configurar l'agent de manera segura recau en l'organització que el desplega.

3.3. La compressió del temps d'atac

Els apartats anteriors descriuen què està canviant. Aquest apartat se centra en una conseqüència concreta: el temps de què disposa un defensor per reaccionar s'està reduint tant abans de la intrusió com després, és a dir, entre que es coneix una vulnerabilitat i s'explota i entre que l'atacant entra i es mou per la xarxa.

A continuació, es recullen els principals indicadors publicats:

Indicador	Dada	Font	Període
Temps des que es detecta l'explotació d'una vulnerabilitat fins que es converteix en un atac funcional.	Mitjana molt per sota de 24 hores	Microsoft	2026
Vulnerabilitats explotades abans de la divulgació pública.	42 %	CrowdStrike	2025
Temps des de l'accés inicial fins que es traspasa a un altre grup (per exemple, un afiliat de programari de segrest).	Mitjana de 22 segons (més de 8 hores el 2022)	Mandiant	2025
Temps des del compromís inicial fins al primer moviment lateral, en ciberdelinqüència.	29 minuts de mitjana. El cas més ràpid, 27 segons	CrowdStrike	2025
Temps que triguen les organitzacions a corregir vulnerabilitats crítiques exposades a Internet.	Entre 30 i 60 dies	Microsoft	2026

Taula 4 - Indicadors de velocitat de l'atac i la resposta

La darrera filera és la més important i la que dona sentit a la resta. **L'atacant mesura els temps en minuts o hores i l'organització mesura els seus en setmanes.**

A més, Microsoft preveu diversos anys d'acumulació de vulnerabilitats conegudes sense corregir, perquè es descobreixen més de pressa del que es poden posar pedaçs. Aquestes dades s'han de llegir amb un matís: no tota l'acceleració és deguda a la IA. Les xifres de

Mandiant i CrowdStrike corresponen al 2025 i reflecteixen sobretot la industrialització de l'ecosistema delinqüent, amb grups especialitzats que es reparteixen les fases de l'atac. La IA se suma a aquesta tendència, però no l'ha creada.

3.4. Què s'ha demostrat a partir del que s'ha observat

Com a l'informe de setembre, convé separar allò que la IA ha demostrat poder fer en entorns controlats del que s'ha vist realment en intrusions. La distància entre tots dos s'ha escurçat, però no ha desaparegut.

Àmbit	Demostrat en entorns controlats	Observat en intrusions reals
Autonomia	Segons Microsoft, models de frontera van encadenar 32 fases d'atac contra una xarxa corporativa simulada sense defensors.	Casos en què un agent va executar la major part de la intrusió (JadePuffer, DIVD i campanyes descrites per Anthropic). Segons Microsoft, el volum és baix i la majoria de les intrusions complexes continuen tenint instrucció humana.
Qualitat de l'execució	Execució completa en un entorn sense defensors.	Execució amb errors. L'agent de DIVD va fer, segons la mateixa organització, «algunes coses força maldestres», com interferir en el seu propi atac. A JadePuffer, l'agent no va guardar la clau de xifratge.
Descobriments de vulnerabilitats	Milers de fallades trobades per models de la IA, com es va analitzar als informes de maig i setembre.	De les vulnerabilitats atribuïdes a descobriments assistits per la IA, l'1,3 % consta com a explotada, una taxa semblant a la de la resta.
Agents com a superfície d'atac	Investigacions que demostren l'extracció de dades i el robatori de credencials a través d'agents comercials (SalesBleed, AWS AgentCore).	Incidents reals: un assistent de programació segrestat que va acabar en un cuc en uns 100 repositoris, i un proveïdor d'IA que va lliurar les credencials de producció.

Taula 5 - El que s'ha demostrat en laboratori a partir del que s'ha observat en intrusions reals

El que està comprovat:

- Hi ha casos públics d'intrusions reals en què un agent de la IA va executar la major part de la cadena d'atac. A JadePuffer i DIVD, que l'autor fos un agent és la valoració de qui va investigar l'incident, no un fet verificat per tercers.
- Microsoft observa activitat orquestrada per la IA en entorns reals. Segons la mateixa Microsoft, el volum és baix, però no es limita a un únic sector o regió.

- Les intrusions més complexes i algunes de les més greus continuen tenint una persona dirigint cada pas.
- Agents de la IA desplegats per organitzacions legítimes ja han estat objecte d'abús, o han fallat per ells mateixos, amb impacte real.
- L'atacant mesura els temps en hores, minuts o segons, mentre que la correcció de vulnerabilitats crítiques exposades es mesura en setmanes.

El que valorem a partir d'aquí:

Valoració	En què es basa	Confiança
La distància entre la velocitat de l'atac i la capacitat de correcció continuarà augmentant a curt termini.	El volum de vulnerabilitats marca rècords, Microsoft preveu uns quants anys d'acumulació d'errors sense corregir i l'explotació ja es produeix en menys de 24 hores.	Alta
Els agents de la IA desplegats per les mateixes organitzacions seran una via d'entrada i de fugida de dades cada cop més rellevant, sobretot per permisos i configuració, més que per errors del model.	Tots els casos de la Taula 3 s'expliquen per permisos, credencials o configuració, l'ús d'agents creix i els proveïdors traslladen al client la responsabilitat de configurar-los.	Alta
Els atacs amb un alt grau d'automatització seran més freqüents els pròxims mesos, tot i que continuaran sent minoria davant dels dirigits per persones.	Els casos documentats es concentren entre juliol i octubre de 2026, el que s'ha demostrat al laboratori va per davant del que s'ha observat i Microsoft preveu que els límits actuals es redueixin.	Mitjana
Les organitzacions petites i mitjanes estaran més exposades a atacs automatitzats de baix cost.	Segons Anthropic, l'automatització fa viables objectius abans marginals i afavoreix operacions de més volum i menor intervenció.	Mitjana
Ara com ara, un atac executat per un agent no és necessàriament més difícil de detectar: deixa rastres característics.	A DIVD i JadePuffer es van observar comentaris en llenguatge natural dins del codi, correccions molt ràpides després de cada error i un comportament poc curós. Són només dos casos, i els atacants aprendran a amagar aquests senyals.	Baixa

Taula 6 - Valoracions de l'apartat

4. COM ADAPTAR-SE: QUATRE PRIORITATS I CINC PRINCIPIS

L'apartat anterior descriu una amenaça més barata, més ràpida i en part automatitzada, com també una nova superfície d'atac dins de les mateixes organitzacions. La resposta que proposa aquest informe s'organitza en quatre prioritats i cinc principis, que es detallen tot seguit.

La idea central és que **l'avantatge serà de qui es pugui adaptar més de pressa**. Això no depèn només de la tecnologia: una eina de resposta automàtica serveix de poc si no hi ha processos definits per automatitzar, i la intel·ligència compartida no funciona sense una cultura de col·laboració.

Cada prioritat respon a un dels canvis descrits a l'apartat anterior:

Prioritat	Idea clau	A què respon	Es desenvolupa a
Automatitzar la defensa	Respondre a velocitat de màquina.	L'atac s'automatitza i els temps es comprimeixen (3.1 i 3.3). Un procés que depèn de revisions manuals no pot seguir aquest ritme.	Apartat 5
Reduir l'exposició	Menys superfície, menys impacte.	Apareixen més vulnerabilitats de les que es poden corregir a temps i noves identitats no humanes, com els agents de la IA, amb permisos excessius (3.2 i 3.3). Allò que no es pot corregir a temps no ha d'estar a l'abast de l'atacant.	Apartat 6
Preparar-se per al futur quàntic	Preparar-se abans que sigui urgent.	Un canvi diferent del de la IA: l'amenaça que la computació quàntica suposa per a bona part de la criptografia actual. La informació xifrada avui es pot emmagatzemar per desxifrar-la en el futur, i la transició requereix anys.	Apartat 7
Coordinar-se com a país	La resiliència serà col·lectiva.	L'atac automatitzat repeteix la mateixa tècnica contra molts objectius alhora, i objectius que abans eren marginals ara passen a ser rendibles (3.1). Cap organització pot seguir aquest ritme sola, i molt menys les petites.	Apartat 8

Taula 7 - Les quatre prioritats i el canvi a què responen

Les quatre prioritats es recolzen en cinc principis comuns:

Principi	Què significa	Per què ara
Anticipació	Preveure allò que altres encara no veuen.	Cal preparar les defenses abans de necessitar-les. La transició criptogràfica o la revisió dels agents de la IA ja desplegats són mesures que s'han de començar abans que el risc sigui immediat.

Velocitat	Reduir el temps de detecció i resposta.	L'explotació es produeix en menys de 24 hores i el moviment lateral, en minuts. El que cal mesurar és el temps fins a la mitigació, no el nombre d'alertes o de pedaços.
Simplicitat	Processos clars, automatitzats i mesurables.	Només es pot automatitzar amb garanties un procés que prèviament estigui ben definit. Automatitzar un procés confús només fa que els errors es produeixin més de pressa.
Col·laboració	Ningú es protegeix sol al món digital.	Els atacs automatitzats repeteixen la mateixa tècnica contra molts objectius. A l'informe d'Anthropic, un grup delinqüent va trobar una via d'atac que funcionava i la va repetir contra unes 30 empreses en quatre dies. Compartir a temps un indicador o una detecció protegeix diversos actors alhora.
Millora contínua	Aprendre, adaptar-se i evolucionar sempre.	Les capacitats canvien d'un mes a l'altre. En cinc mesos s'ha passat d'un model que el fabricant va decidir no publicar per les seves capacitats (maig) a models comercials amb capacitats ofensives rellevants (setembre) i als primers casos documentats d'intrusions reals executades en gran part per agents. Les mesures i els exercicis s'han de revisar al mateix ritme.

Taula 8 - Principis clau per a l'adaptació

5. PRIORITAT 1: AUTOMATITZAR LA DEFENSA

5.1. Per què és necessària

Com es va veure a l'apartat 3.3, l'explotació d'una vulnerabilitat es pot produir en menys de 24 hores, el moviment lateral en minuts i el traspàs de l'accés entre grups criminals en segons. Amb aquests temps, un SOC que revisa les alertes de manera manual, per torns i amb escalats per correu difícilment pot reaccionar a temps, per més que l'equip s'hi esforci.

La defensa ja s'ha començat a adaptar. Segons l'informe anual d'IBM sobre el cost de les bretxes de dades, publicat el juliol del 2026, la meitat de les organitzacions que van patir una bretxa ja fan servir agents de la IA per buscar amenaces, respondre-hi i contenir-les. Les que fan un ús intensiu de la IA i l'automatització en seguretat van tenir, de mitjana, un cost per bretxa d'1,93 milions de dòlars inferior. És important llegir bé aquesta dada: és una correlació, no pas una relació causa-efecte demostrada, ja que les organitzacions que més automatitzen solen ser també les més madures en altres aspectes. El mateix informe situa en 247 dies el temps mitjà per identificar i contenir una bretxa, molt lluny encara dels temps de l'atacant.

Tampoc no sembla que el problema sigui la manca d'eines. A l'enquesta anual de SANS sobre centres d'operacions de seguretat, el 79 % dels SOC afirma que ja fa servir eines de la IA, però només el 36 % les ha integrat en fluxos de treball definits. La majoria ja disposa de la tecnologia; el que queda pendent és decidir què s'automatitza, fins on i sobre quins processos.

5.2. Què implica

IA defensiva i analítica avançada: on més valor aporta avui la IA en defensa és a l'hora de revisar allò que un analista descarta per falta de temps. Mandiant descriu un cas del 2026 que ho il·lustra bé. Un sistema de triatge amb IA va escalar una ordre anòmla i poc freqüent que, segons la mateixa organització, un analista probablement hauria considerat de baixa criticitat. El sistema la va correlacionar amb el trànsit de sortida, va reconstruir la cronologia de l'atac i va permetre tallar l'accés d'una campanya d'espionatge dirigida contra operadors de telecomunicacions i organismes públics. Com ja s'indicava a l'informe de setembre, la IA és útil com a primera anàlisi i per reunir evidències, però la decisió final l'ha de continuar prenent una persona.

Resposta automàtica i orquestrada: consisteix a definir per endavant què fer davant de cada tipus d'incident i permetre que la contenció s'executi de manera automàtica quan la detecció és fiable (per exemple, aïllant un equip, tancant sessions, revocant tokens o bloquejant un indicador). En incidents que afectin agents de la IA, Mandiant recomana aturar tota la cadena d'execució, revocar els tokens de l'agent i capturar la memòria abans d'aïllar-lo. Actuar amb rapidesa no ha de suposar perdre evidències. Després del cas de DIVD, la Cloud Security Alliance recomanava copiar els registres abans d'aplicar pedaços, un pas que també es pot automatitzar com a inici de cada procediment.

Visibilitat 360 i telemetria: l'automatització només pot actuar sobre allò que veu. Això obliga a centralitzar la telemetria d'identitat, equips, xarxa, *cloud* i aplicacions SaaS i, cada cop més, l'activitat dels agents de la IA: quines instruccions reben, quines eines fan servir i a quines dades accedeixen. Mandiant proposa mesures concretes, com ara correlacionar els registres de les aplicacions amb el trànsit de sortida o generar una alerta davant el primer accés a un repositori sensible. El temps de retenció també és rellevant. Segons Mandiant, el 2025 la mitjana de temps entre l'entrada d'un atacant i la seva detecció va ser de 14 dies, i hi ha campanyes d'espionatge que es perllonguen durant anys.

Simulacions contínues: disposar de detecció i resposta no garanteix que funcionin a la velocitat real de l'atac, per la qual cosa cal comprovar-ho. Després del cas de DIVD, la Cloud Security Alliance recomanava verificar si les alertes són capaces de detectar cadenes d'atac que es completen en segons. Els exercicis haurien d'incloure escenaris amb agents de la IA, com ara un agent segrestat o una clau de la IA filtrada, i servir també per provar els procediments automàtics mateixos: si s'activen quan cal i si provoquen interrupcions no previstes.

5.3. Què no convé automatitzar

Automatitzar la resposta no implica que totes les accions s'hagin d'executar sense intervenció humana. Algunes es poden llançar de manera automàtica i d'altres convé que les confirmi una persona. Per distingir-les, el criteri més pràctic combina dos factors: la fiabilitat de la detecció i l'impacte de l'acció, especialment quan és difícil de revertir.

Tipus d'acció	Exemples	Tractament recomanat
Reversible, de baix impacte i amb detecció fiable	Aïllar un equip d'usuari, tancar sessions, revocar tokens, bloquejar un indicador confirmat, forçar un canvi de contrasenya.	Automàtic
Amb alt impacte en el servei o difícil de revertir	Aïllar servidors crítics o sistemes industrials, deshabilitar comptes privilegiats o de servei, esborrar dades, restaurar des de còpia, comunicar l'incident fora de l'organització.	Amb aprovació humana
Conclusions d'una eina de la IA	Tancar una alerta com a fals positiu, una anàlisi que conclou que no hi ha res maliciós, el resum d'un incident.	Revisió humana, almenys per mostreig.

Taula 9 - Què automatitzar i què no en la resposta a incidents

La tercera filera requereix una explicació. Les eines de la IA del SOC treballen amb contingut que controla l'atacant, com ara registres, correus o mostres de codi maliciós (*malware*). L'informe del setembre ja recollia casos de codi maliciós amb text dirigit als models que analitzen codi, pensat per interrompre l'anàlisi. Un estudi acadèmic publicat el maig del 2026 va anar més enllà i va introduir instruccions a camps dels registres que l'atacant pot manipular, com l'agent d'usuari o els URL. A les seves proves, sense cap protecció, una d'aquestes tècniques va aconseguir que el model descartés el 68 % dels registres maliciosos. Amb les millors defenses provades, la taxa mitjana d'èxit va baixar del 26,6 % a l'11,8 %, però no va desaparèixer. Es tracta d'un estudi preliminar, fet amb un model únic, per la qual cosa les xifres

no s'han de generalitzar. La seva conclusió de fons, però, és raonable: el contingut dels registres s'ha de tractar com a informació potencialment manipulada.

A la pràctica, les eines de la IA del SOC també són agents, i se'ls aplica tot allò que s'ha vist a l'apartat 3.2. A més, la mateixa automatització necessita límits. El cas de l'agent que va entrar en bucle i va generar uns 50.000 dòlars de despesa en menys d'una hora (Taula 3) mostra per què qualsevol automatització ha de disposar d'un topall d'execucions i de cost, i d'una manera senzilla d'aturar-la.

5.4. Mesures

En aquest apartat i en els següents, el curt termini fa referència als pròxims sis mesos, i el mitjà termini a un període d'entre sis i divuit mesos.

Mesura	Què aporta	Horitzó
Definir procediments de contenció automàtica (<i>playbooks</i>) per als escenaris més freqüents i amb detecció fiable, com ara el compromís d'un compte o programari maliciós en un equip d'usuari.	Redueix el temps de contenció d'hores a minuts en els casos més habituals.	Curt
Classificar les accions de resposta segons el seu impacte i la seva reversibilitat, i documentar quines requereixen aprovació humana.	Permet automatitzar sense posar en risc el servei.	Curt
Mesurar de manera contínua el temps fins a la detecció, la contenció i la mitigació, i fixar objectius per a cadascun.	Permet comprovar si els temps de resposta milloren.	Curt
Aplicar a les eines de la IA del SOC els controls de qualsevol agent: permisos mínims, tractar com a no fiable el contingut analitzat, establir límits d'execució i de cost, i enregistrar la seva activitat.	Redueix el risc que l'atacant manipuli les eines mateixes del SOC.	Curt
Incloure la captura automàtica d'evidències com a primer pas de cada procediment de resposta.	Permet actuar ràpidament sense perdre la capacitat d'investigar després.	Curt
Incorporar la IA al triatge i la correlació d'alertes, amb revisió humana per mostreig i retroalimentació dels analistes.	Permet revisar senyals que avui es descarten per manca de temps.	Curt (pilot) / Mitjà (desplegament)
Centralitzar la telemetria d'identitat, equips, xarxa, <i>cloud</i> , SaaS i agents de la IA, amb prou retenció per investigar intrusions llargues.	Dona a l'automatització i a l'anàlisi les dades que necessiten.	Mitjà
Realitzar exercicis periòdics que simulin atacs a velocitat de màquina, amb escenaris que incloguin agents de la IA, i	Permet comprovar que la resposta funciona abans d'un incident real.	Mitjà, i després de manera periòdica

que posin a prova els procediments automàtics mateixos.		
--	--	--

Taula 10 – Mesures de la prioritat 1

6. PRIORITAT 2: REDUIR L'EXPOSICIÓ

6.1. Per què és necessària

Com es recollia a l'apartat 3.3, es descobreixen més vulnerabilitats de les que es poden corregir, i Microsoft preveu diversos anys d'acumulació d'errors coneguts sense pedaços. Si no és possible corregir-ho tot a temps, l'alternativa és reduir allò que queda a l'abast de l'atacant i limitar allò que pot fer un cop a dins.

Les vies d'entrada principals apunten en la mateixa direcció. Segons l'informe de Verizon sobre bretxes de dades del 2026, el 31 % de les bretxes va començar amb l'explotació d'una vulnerabilitat, que ja supera el robatori de contrasenyes com a principal via d'entrada. Microsoft, per altra banda, atribueix el 20 % dels accessos inicials que observa a l'ús de comptes vàlids, i ho explica així: «**una credencial vàlida pot fer que una activitat maliciosa sembli un ús legítim**».

A això se suma el que s'ha vist a l'apartat 3.2: cada agent de la IA desplegat a l'organització és una identitat més, amb els seus permisos, credencials i accés a dades.

6.2. Què implica

Zero Trust per disseny: el principi és no donar per bo cap accés només perquè procedeixi de la xarxa interna o d'un compte vàlid. Cada accés es verifica en funció de qui ho sol·licita, des de quin dispositiu i amb quina finalitat, i es concedeix únicament allò que cal. El model de referència és l'arquitectura Zero Trust del NIST (SP 800-207). El maig del 2026, sis agències de ciberseguretat dels Estats Units, el Regne Unit, el Canadà, Austràlia i Nova Zelanda van publicar una guia conjunta sobre agents de la IA, i la seva primera recomanació va en la mateixa línia: gestionar el risc dels agents dins dels marcs de seguretat que l'organització ja aplica.

Gestió d'identitats i accessos privilegiats: quan un atacant aconsegueix entrar amb un compte vàlid, l'habitual és que intenti obtenir més credencials; Microsoft ho va observar en el 52 % de les intrusions d'aquest tipus. Els privilegis, a més, acceleren molt l'atac. En un dels casos descrits per Anthropic, l'atacant va passar d'un testimoni (*token*) de desenvolupador al control total de l'entorn *cloud* en unes tres hores. Les mesures conegudes continuen sent vàlides, especialment l'autenticació multifactor resistent a la pesca de dades (*phishing*) en accessos privilegiats i remots i la concessió de privilegis només quan es necessiten i durant el temps imprescindible. La novetat està en les identitats no humanes, com ara comptes de servei, claus d'API, tokens i agents. Segons IBM, menys de la meitat de les organitzacions les protegeix de manera activa. Mandiant, d'altra banda, assenjala les credencials de llarga durada com a causa de diversos dels incidents que va analitzar el 2026 i recomana substituir-les per credencials de curta durada.

Segmentació i microsegmentació: dividir la xarxa en zones limita fins a on pot arribar un atacant que ja ha entrat. En el cas de DIVD, la segmentació va limitar l'avenç de l'agent cap a

sistemes interns més profunds. Amb un temps mitjà de 29 minuts fins al primer moviment lateral, cada barrera interna aporta un marge valuós per a la detecció i la resposta. La segmentació també s'ha d'aplicar al trànsit de sortida: en diversos casos de la Taula 3, el dany va dependre que el sistema compromès pogués comunicar-se lliurement amb l'exterior.

Gestió d'actius i certificats: el punt de partida és saber quins actius hi ha i quins estan exposats, i l'inventari ja ha d'incloure les eines de la IA. JadePuffer va entrar per una instància de Langflow, una eina per crear aplicacions de la IA exposada a Internet, i VulnCheck assenyala que els productes de la IA s'estan convertint en una nova superfície d'atac. L'inventari també permet no perdre de vista els sistemes antics: segons Microsoft, el 58 % de les deteccions associades a les cinc vulnerabilitats més explotades que observa corresponen a Zerologon, una decisió del 2020. A partir d'aquest inventari, la priorització s'ha de basar en l'exposició i l'explotació real, com ja es recomanava al setembre. Això inclou un procediment de canvi d'emergència preautoritzat per a vulnerabilitats explotades en sistemes exposats, i mesures compensatòries (aïllar, restringir l'accés, vigilar) quan no sigui possible aplicar pedaços a temps.

En el cas dels certificats, el CA/Browser Forum, que fixa les normes dels certificats web de confiança pública, va aprovar el 2025 reduir de manera progressiva la seva validesa màxima: 200 dies des del 15 de març de 2026, 100 dies des del 15 de març de 2027 i 47 dies des del 15 de març de 2029. Amb aquests terminis, la renovació manual deixa de ser viable, per la qual cosa convé inventariar els certificats i automatitzar-ne la gestió. A més, aquest inventari servirà com a punt de partida de l'inventari criptogràfic de la prioritat 3.

Tercers i integracions: segons l'informe de Verizon de 2026, en el 48 % de les bretxes va intervenir un tercer, davant del 30 % de l'any anterior. Un cas del 2025 il·lustra molt bé aquest risc. Els atacants van robar els tokens d'accés de Drift, un xat amb IA integrat a Salesforce, i, segons les primeres estimacions, van accedir a les dades de centenars d'organitzacions clients. Un cop dins, van buscar en aquestes dades altres credencials, com ara claus d'AWS, contrasenyes o tokens de Snowflake. Per això, cal revisar els permisos concedits a cada integració amb la mateixa atenció que els d'un compte privilegiat.

6.3. Els agents de la IA com a identitats

Els agents d'IA es tracten per separat perquè concentren diversos riscos anteriors: són identitats, accedeixen a dades i API, depenen de components de tercers i es poden comunicar amb l'exterior. A més, el control sobre ells encara és escàs. Segons IBM, només el 40 % de les organitzacions aplica controls d'accés als models i dades de la IA, i, entre les que van patir un incident relacionat amb la IA, el 92 % no tenia controls d'accés adequats.

La guia conjunta de les sis agències apunta a la mateixa direcció. Recomana no concedir als agents accessos amplis o sense restriccions, evitar que accedeixin a dades delicades o sistemes crítics, aplicar una gestió d'identitats sòlida amb mecanismes de supervisió i mantenir de manera contínua el modelatge d'amenaques i el monitoratge.

El primer pas és l'inventari: quins agents hi ha a l'organització, a quines dades i eines accedeixen i en nom de qui actuen. A partir d'aquí, convé recordar les tres condicions

identificades a l'apartat 3.2, que, quan coincideixen, permeten que un atacant actuï amb els permisos d'un agent. Trencar-ne qualsevol dificulta molt l'abús, encara que el més recomanable és actuar en les tres:

Condicció	Controls	Casos relacionats (Taula 3)
L'agent processa contingut que no és de confiança	Separar els agents que llegeixen contingut extern (correu, formularis, tiquets, web) dels que tenen accés a dades o sistemes delicats. Tractar tot aquest contingut com a no fiable.	SalesBleed, AWS AgentCore
L'agent té accés a dades o eines delicades	Una identitat pròpia per a cada agent. Permisos limitats a la seva tasca. Només les eines que necessita, i desactivar les que venen actives per defecte. Credencials de curta durada. Aprovació humana per a accions d'alt impacte. Límits d'execució i de cost.	AWS AgentCore, control de bucle sense fi
L'agent es pot comunicar cap a fora	Filtrar el trànsit de sortida, inclòs el DNS, amb una llista de destinacions permeses.	SalesBleed, assistent de programació segrestat

Taula 11 - Controls per trencar les condicions d'abús d'un agent

Hi ha tres controls més que completen el quadre:

- **Traçabilitat:** registrar quines instruccions rep cada agent, quines eines fa servir i quines dades consulta, i integrar aquests registres a la telemetria del SOC (prioritat 1). Sense aquest registre, investigar l'abús d'un agent és pràcticament impossible.
- **Components de tercers:** els connectors, extensions i servidors MCP (el protocol que fan servir molts agents per connectar-se a les eines) han de procedir d'una llista de components autoritzats. Mandiant recomana verificar-ne la signatura i l'origen, com també les dependències de programari que recomani la mateixa IA.
- **Claus de serveis de la IA:** s'han de tractar com a credencials crítiques, amb un abast limitat, rotació periòdica i vigilància dels consums anòmals. A l'informe d'Anthropic, un grup criminal, durant unes tres setmanes, va fer servir la clau robada a una víctima; per tant, un pic de consum sense explicació pot ser el primer indicatiu d'un robatori.

6.4. Mesures

Mesura	Què aporta	Horitzó
Mantenir un inventari continu dels actius exposats a Internet, incloses les eines i els agents de la IA.	Permet saber què hi ha a l'abast de l'atacant.	Curt
Establir una via ràpida, amb canvi d'emergència preautoritzat, per a vulnerabilitats amb explotació	Redueix la finestra entre l'explotació i la correcció.	Curt

confirmada en sistemes exposats, i mesures compensatòries quan no es pugui apedaçar a temps.		
Implantar autenticació multifactor resistent a la pesca de dades en accessos privilegiats i remots, i eliminar-ne els privilegis permanents.	Redueix el valor d'una credencial robada.	Curt
Inventariar els agents de la IA en ús (quines dades i eines fan servir i en nom de qui actuen) i assignar-los una identitat pròpia amb permisos limitats a la seva tasca.	Permet saber quins agents hi ha i limitar què poden fer.	Curt
Inventariar les identitats no humanes (comptes de servei, claus d'API, tokens, claus de la IA) i substituir de manera progressiva les credencials de llarga durada per altres de curta durada.	Tanca una de les vies d'abús més repetides en els casos analitzats.	Curt (inventari) / Mitjà (substitució)
Controlar el trànsit de sortida dels agents i de les càrregues de treball de la IA, inclòs el DNS, i exigir l'aprovació humana per a les accions d'alt impacte.	Dificulta que un agent manipulat extregui dades o actuï fora del seu àmbit.	Mitjà
Registrar l'activitat completa dels agents (instruccions, eines i dades) i integrar-la al SOC.	Permet la detecció i la investigació d'abusos.	Mitjà
Segmentar la xarxa i separar els entorns crítics, començant pels actius de més valor.	Limita el moviment lateral i guanya temps per a la resposta.	Mitjà
Inventariar les integracions i aplicacions de tercers amb accés (OAuth, API), revisar-ne els permisos i incloure en els contractes terminis de pedaç i de notificació d'incidents.	Redueix l'impacte d'un compromís en un proveïdor.	Mitjà
Inventariar els certificats i automatitzar-ne l'emissió i la renovació.	Prepara l'organització per a la validesa màxima de 47 dies prevista per al 2029 i serveix de base per a la transició criptogràfica.	Mitjà

Taula 12 - Mesures de la prioritat 2

7. PRIORITAT 3: PREPARAR-SE PER AL FUTUR QUÀNTIC

7.1. Per què és necessària

Un ordinador quàntic de mida suficient podria trencar la criptografia de clau pública (RSA i corbes el·líptiques) en la qual es basen les comunicacions xifrades, els certificats i les signatures digitals. Aquest ordinador encara no existeix i no se sap amb certesa quan existirà. L'última enquesta del Global Risk Institute, publicada el març del 2026 i duta a terme entre 26 experts, considera «bastant possible» (entre un 28 % i un 49 %) que aparegui en els pròxims deu anys, i «probable» (entre un 51 % i un 70 %) en els pròxims quinze.

El que sí que ha canviat és l'estimació de la mida de la màquina necessària. El maig del 2025, un investigador de Google va calcular que n'hi hauria prou amb menys d'un milió de qbits físics per trencar una clau RSA de 2048 bits en menys d'una setmana, unes vint vegades menys que l'estimació del 2019. El març del 2026, Google va publicar un càlcul equivalent per a la criptografia de corba el·líptica: menys de 500.000 qbits físics i uns minuts de càlcul, també unes vint vegades menys que les estimacions anteriors. Aquestes reduccions provenen de millores en els algorismes i en el disseny, i no pas d'avenços en el maquinari. Així i tot, indiquen que el llindar necessari per trencar la criptografia actual està baixant.

Hi ha dos motius per no esperar:

- «**Recopilar ara, desxifrar després**»: un atacant pot capturar avui comunicacions xifrades i desar-les fins que pugui desxifrar-les. El març del 2026, Google va afirmar que és probable que alguns atacants ja ho estiguin fent, de manera que el risc afecta des d'ara la informació que hagi de continuar sent confidencial durant anys.
- **La migració pot durar anys**: obliga a canviar protocols, certificats, biblioteques, dispositius i contractes amb els proveïdors. El full de ruta europeu reparteix el treball entre el 2026 i el 2035, i Google ha avançat al 2029 el seu termini de migració, donant prioritat als serveis d'autenticació.

Data	Fita	Font
Agost de 2024	El NIST publica els tres primers estàndards postquàntics: ML-KEM per a l'intercanvi de claus, i ML-DSA i SLH-DSA per a la signatura digital.	NIST
Final de 2026	Primers passos a la UE: inventaris criptogràfics, mapes de dependències (inclosa la cadena de subministrament) i plans nacionals de transició.	Full de ruta coordinat de la UE
2029	Termini que Google s'ha fixat per completar la seva migració.	Google
Final de 2030	A la UE, transició completada per als casos d'ús d'alt risc, en què els mecanismes de clau pública vulnerables deixen de poder-se fer servir sols.	Full de ruta coordinat de la UE

2030 i 2035	NIST proposa declarar obsolets RSA i les corbes el·líptiques a partir del 2030 i prohibir-los a partir del 2035. És un esborrany, encara no definitiu.	NIST (IR 8547, esborrany)
Final de 2035	A la UE, transició dels casos d'ús de risc mitjà i del nombre més gran possible de sistemes.	Full de ruta coordinat de la UE

Taula 13 - Calendari de referència per a la transició postquàntica

Tot i que Andorra no forma part de la Unió Europea, el full de ruta europeu marca el ritme de molts dels proveïdors i socis amb els quals treballen les seves organitzacions, com passa amb la regulació europea de la IA analitzada el setembre.

7.2. Quins actius i sistemes es veuen afectats

L'amenaça no afecta per igual tota la criptografia, ni es materialitza alhora en tots els casos:

Ús de la criptografia	Exemples	Què es posa en risc	Quan
Intercanvi de claus i xifratge de comunicacions	Web i API (TLS), VPN, SSH, correu xifrat.	La confidencialitat: el que es captura avui es pot desxifrar en el futur.	Ara: la captura pot estar passant actualment.
Signatures digitals i certificats	Infraestructura de clau pública, certificats, signatura electrònica, identitat digital i autenticació.	L'autenticitat: la suplantació d'identitats i la falsificació de signatures.	Quan hi hagi l'ordinador quàntic. Les arrels de confiança de llarga durada s'han de migrar abans.
Signatura de programari i microprogramari	Actualitzacions de sistemes, dispositius industrials i IoT.	La integritat: actualitzacions falses acceptades com a legítimes.	Igual que les signatures. És crític en equips amb una llarga vida útil.
Xifratge simètric i funcions hash	AES, SHA-2, SHA-3	Molt menys afectats.	Es mitiga fent servir claus de més longitud.

Taula 14 - Usos de la criptografia afectats per l'amenaça quàntica

Per prioritzar, se sol fer servir una regla senzilla, coneguda com a teorema de Mosca: si el temps durant el qual una informació ha de continuar protegida, sumat al temps que portarà migrar el sistema, supera el temps que falta perquè hi hagi un ordinador quàntic capaç, aquesta informació ja està en risc. Per exemple, unes dades que s'han de mantenir confidencials durant deu anys, en un sistema la migració del qual en portarà cinc, quedarien exposades si l'ordinador quàntic arriba abans de quinze anys, un escenari que l'enquesta del Global Risk Institute considera probable.

7.3. Què implica

Inventari criptogràfic: el primer pas és saber on i com s'utilitza avui la criptografia, cosa que inclou protocols, biblioteques, certificats, claus, dispositius i productes de tercers. És també la primera fita del full de ruta europeu, previst per a finals del 2026. Una part important del treball queda coberta amb l'inventari de certificats i d'actius exposats de la prioritat 2. El resultat s'hauria de mantenir actualitzat de manera contínua en allò que de vegades s'anomena CBOM (llista de materials criptogràfics).

Criptoagilitat: és la capacitat de canviar d'algorisme sense haver de redissenyar cada sistema, gràcies a una configuració centralitzada, biblioteques actualitzables i algorismes que no estiguin fixats al codi. Els nous algorismes fan servir claus i signatures força més grans (en el cas de les signatures, desenes de vegades més grans), la qual cosa pot afectar els protocols, els dispositius amb pocs recursos i la mateixa infraestructura de certificats. Per això convé fer proves abans que la migració sigui urgent.

Migració progressiva: els estàndards existeixen des de 2024, i la transició ha començat per la part que depèn dels grans fabricants. Segons Cloudflare, el setembre del 2026 al voltant del 70 % del trànsit generat per navegadors que rep ja utilitza intercanvi de claus híbrid (clàssic més postquàntic). En canvi, només al voltant del 15 % dels servidors de les organitzacions a què Cloudflare es connecta ho admet. És a dir, la part que actualitzen els navegadors avança ràpidament, mentre que la que depèn de cada organització va molt més lenta. El que és raonable és començar per les comunicacions que transporten informació que s'ha de protegir durant anys, continuar amb les arrels de confiança i els dispositius de llarga vida útil, i exigir als proveïdors un full de ruta postquàntic.

Vigilància i anticipació: les estimacions canvien amb rapidesa. En menys d'un any, dos treballs han reduït unes vint vegades els recursos necessaris per trencar l'RSA i les corbes el·líptiques. Convé seguir l'evolució dels estàndards i del calendari i revisar el pla almenys una vegada a l'any, prenent com a referència les avaluacions dels organismes públics i dels experts abans que els anuncis puntuals.

7.4. Mesures

Mesura	Què aporta	Horitzó
Designar un responsable de la transició criptogràfica i aprovar un pla de treball pluriennal.	Dona continuïtat a una feina de diversos anys.	Curt
Inventariar la criptografia dels serveis exposats a Internet, les VPN, la infraestructura de clau pública i els certificats, partint dels inventaris de la prioritat 2.	Permet saber què n'està afectat.	Curt

Classificar les dades i els sistemes segons quant de temps han de continuar protegits i la seva vida útil.	Concentra l'esforç on el risc ja és actual.	Curt
Incloure en les compres i els contractes requisits de criptoagilitat i un full de ruta postquàntic del proveïdor.	Evita adquirir avui sistemes que caldrà substituir abans d'hora.	Curt
Activar l'intercanvi de claus híbrid en serveis web, API i VPN quan els productes ja ho permetin.	Protegeix des d'ara mateix davant de «recopilar ara, desxifrar després».	Mitjà
Avaluar l'impacte dels nous algorismes (mida de claus i signatures, rendiment) a la infraestructura de certificats i als dispositius amb recursos limitats.	Permet anticipar problemes de compatibilitat i rendiment abans de migrar.	Mitjà
Planificar la migració de les signatures en arrels de confiança i en dispositius que seguiran en servei després del 2030.	Protegeix la integritat dels sistemes de vida útil més llargs.	Mitjà
Revisar el pla almenys una vegada a l'any segons l'evolució d'estàndards i estimacions.	Permet ajustar el ritme de la transició a l'evolució real del risc.	Recurrent

Taula 15 - Mesures de la prioritat 3

8. PRIORITAT 4: COORDINAR-SE COM A PAÍS

8.1. Per què és necessària

L'automatització fa que un mateix atac es pugui repetir contra moltes organitzacions. A l'informe d'Anthropic, un grup criminal va trobar una via d'atac que funcionava i la va repetir contra unes 30 empreses en quatre dies. En un escenari com aquest, que la primera organització afectada detecti l'atac i el comparteixi a temps pot permetre que les altres es protegeixin abans de ser atacades.

En un país de dimensions reduïdes, hi ha dos factors que reforcen aquesta necessitat:

- **Els proveïdors comuns:** segons Verizon, en el 48 % de les bretxes intervé un tercer, i el cas de Drift (apartat 6) mostra com una sola integració compromesa pot donar accés a centenars d'organitzacions. En un país petit és probable que moltes entitats comparteixin proveïdors de tecnologia i serveis, de manera que un sol incident podria afectar-ne diverses alhora.
- **Les organitzacions amb menys recursos:** com es va veure a l'apartat 3.1, l'automatització fa rendibles objectius que abans no ho eren. Per a les organitzacions petites i mitjanes serà difícil aplicar per si mateixes totes les mesures de les prioritats anteriors.

El mateix sector també reconeix aquesta necessitat. L'agost del 2026, OpenAI, Anthropic, Google, Microsoft i centenars d'organitzacions més van signar una crida a l'acció col·lectiva en ciberdefensa. Hi demanen als governs «coordinar la ciberdefensa en l'àmbit local, nacional i internacional», finançar-la començant pels serveis essencials que no disposen de prou personal ni pressupost, i accelerar els programes d'accés de confiança a la IA defensiva, especialment per a les cadenes de subministrament de les infraestructures crítiques.

En el cas d'Andorra, el marc per a aquesta coordinació ja existeix. L'octubre del 2021, el Govern va aprovar l'estratègia nacional de ciberseguretat i la creació de l'Agència, amb el CSIRT-AD com a equip de resposta a incidents, acreditat per Trusted Introducer des del 2023. La Llei 22/2022 va establir les obligacions de seguretat de les xarxes i dels sistemes d'informació. Segons les dades presentades pel Govern davant del Consell General, l'ANC-AD va gestionar 1.624 incidents el 2025, un 5,6 % més que l'any anterior. En presentar aquestes xifres, el Govern va advertir que s'havien d'interpretar amb cautela, atès que la llei només obligava a notificar les entitats essencials.

Per tant, la base per coordinar la resposta ja està construïda. El que canvia amb la IA és la velocitat i l'escala amb la qual ha de funcionar aquesta coordinació.

8.2. Què implica

Intel·ligència d'amenaques compartida: el valor de la informació que rep el CSIRT-AD depèn en bona part de la rapidesa amb què es pugui retornar a les organitzacions en forma d'indicadors, regles de detecció i context. Perquè arribi a temps, és important que es pugui processar de manera automàtica, en formats estàndard com ara el STIX/TAXII o el MISP que els SOC de les organitzacions puguin integrar sense intervenció manual, i amb la classificació TLP per indicar fins on pot circular. Convindria que aquesta intel·ligència inclogués també les amenaces específiques de la IA, com ara les eines de la IA exposades o vulnerables, agents manipulats, claus de la IA filtrades o els rastres característics dels atacs executats per agents.

Coordinació de l'ANC-AD amb els sectors crítics: es tracta de sumar capacitats, recursos i coneixement, per exemple, mitjançant regles de detecció per sector, guies de resposta comunes, formació i suport a les organitzacions que no en poden disposar pel seu compte. Inclou també la resposta coordinada, amb un procediment acordat per endavant per als incidents que afecten diverses organitzacions alhora, com el compromís d'un proveïdor comú, en què es defineixi qui avisa, quins accessos es revocuen i en quin ordre. Aquesta coordinació també es pot estendre a la relació amb els proveïdors de la IA. A l'informe del setembre es van analitzar els programes que reserven les seves capacitats defensives més avançades a entitats verificades, entre elles autoritats públiques i infraestructures crítiques.

Exercicis i simulacions conjuntes: seria recomanable que els exercicis nacionals incloguessin els escenaris descrits en aquest informe, com ara un atac automatitzat que afecta diverses organitzacions en poques hores, el compromís d'un proveïdor comú o un agent de la IA manipulat que extreu dades. Un dels indicadors més útils en aquests exercicis és el temps que transcorre des de la primera detecció fins que totes les organitzacions afectades estan protegides. A més, són una bona ocasió per provar els fluxos de notificació entre les organitzacions i el CSIRT-AD.

Estàndards i bones pràctiques: per a tot això es poden aprofitar marcs internacionals ja consolidats, sense necessitat de crear-ne de nous.

La taula següent recull les referències principals per a cadascuna de les prioritats d'aquest informe:

Àmbit	Referència	Per què serveix
Gestió de la ciberseguretat	Marc de ciberseguretat NIST 2.0 (2024), ISO/IEC 27001:2022	Marc general per organitzar i mesurar la seguretat.
Govern i gestió de la IA	ISO/IEC 42001:2023, Marc de gestió de riscos de la IA del NIST (2023)	Govern i gestió del risc dels sistemes de la IA.
Agents de la IA	Guia conjunta de sis agències sobre l'adopció d'agents de la IA (2026), OWASP Top 10 for Agent Applications (2025)	Riscos i controls específics dels agents.

Confiança zero	NIST SP 800-207 (2020)	Arquitectura de referència per reduir l'exposició.
Transició postquàntica	Estàndards FIPS 203, 204 i 205 del NIST (2024), full de ruta coordinat de la UE (2025)	Algorismes i calendari de la migració.
Intercanvi d'informació	Protocol de semàfors 2.0 (FIRST, 2022), STIX/TAXII (OASIS)	Classificació i format de la intel·ligència compartida.

Taula 16 - Marcs i estàndards de referència per àmbit

8.3. Mesures

Mesura	Què aporta	Horitzó
Compartir intel·ligència d'amenaques en formats llegibles per màquina (STIX/TAXII o MISP), amb classificació TLP, perquè els SOC de les organitzacions la integrin de manera automàtica.	Permet que la informació arribi a temps per ser útil.	Curt (pilot amb sectors crítics) / Mitjà (extensió)
Incloure en la intel·ligència compartida les amenaces específiques de la IA: eines de la IA exposades, agents manipulats i claus de la IA filtrades.	Incorpora a la intel·ligència compartida els riscos associats a la IA.	Curt
Definir un procediment de resposta coordinada per a incidents que afectin diverses organitzacions alhora, com ara el compromís d'un proveïdor comú.	Evita respostes aïllades i tardanes davant d'incidents que afecten diverses organitzacions.	Curt
Retornar a les organitzacions una anàlisi agregada i periòdica dels incidents notificats.	Aporta valor a qui notifica i en reforça l'incentiu per fer-ho.	Mitjà
Oferir capacitats compartides a les organitzacions més petites: regles de detecció, guies i formació.	Ajuda les organitzacions amb menys recursos a aplicar les mesures bàsiques.	Mitjà
Explorar l'accés de l'ANC-AD i dels operadors crítics als programes d'accés de confiança dels proveïdors de la IA i al seu suport en incidents greus.	Facilita l'accés del país a capacitats defensives avançades.	Mitjà
Dut a terme un exercici nacional periòdic amb escenaris d'atac automatitzat, compromís d'un proveïdor comú i agents de la IA, mesurant el temps fins que totes les organitzacions estan protegides.	Permet comprovar-ne la coordinació abans d'un incident real.	Mitjà, i després anual
Coordinar un pla nacional de transició postquàntica, amb inventaris i prioritats comuns, prenent com a referència la fita europea de finals de 2026.	Facilita que les organitzacions avancin de manera coordinada.	Mitjà

Publicar una guia nacional de recomanacions que reculli els marcs de la Taula 16 i les mesures d'aquest informe, adaptades a la mida de les organitzacions andorranes.	Proporciona a totes les organitzacions un punt de partida comú.	Mitjà
--	---	-------

Taula 17 - Mesures de la prioritat 4

9. CONCLUSIONS

L'atac totalment autònom encara no és la norma, però ha deixat de ser només una demostració de laboratori. Atacar és cada cop més barat i més ràpid, i els agents de la IA que despleguen les mateixes organitzacions obren una nova via d'entrada. El model de defensa pensat per a atacs al ritme d'una persona comença a quedar curt.

Tot seguit, es mostren les conclusions principals:

- **L'atac automatitzat ja es veu en intrusions reals:** JadePuffer, DIVD i les campanyes descrites per Anthropic mostren agents de la IA executant la major part d'una intrusió. El volum encara és baix i les intrusions més complexes continuen tenint direcció humana.
- **Atacar costa menys, i això multiplica els objectius:** una sola persona pot fer la feina d'un equip, i les organitzacions que abans no compensava atacar passen a ser objectius rendibles.
- **Els agents de la IA són una nova superfície d'atac:** els incidents analitzats s'expliquen per permisos, credencials i configuració, no per errors del model. La responsabilitat de configurar-los de manera segura recau en qui els desplega.
- **La velocitat decideix el resultat:** l'explotació es produeix en menys de 24 hores i el moviment lateral, en minuts, mentre que corregir triga setmanes. El que cal mesurar és el temps fins a la mitigació.
- **L'amenaça quàntica no és immediata, però la preparació sí que ho és:** el que es xifra avui es pot desxifrar demà, les estimacions dels recursos necessaris per trencar la criptografia actual són cada cop menors i la migració triga anys.
- **Cap organització no pot seguir aquest ritme sola:** els atacs es repeteixen contra molts objectius i els proveïdors comuns multipliquen l'impacte. Andorra ja té un marc de coordinació. El repte és que funcioni a la velocitat i escala del nou atac.

A partir d'aquestes conclusions, la taula següent resumeix les mesures prioritàries de cada apartat:

Prioritat	Què fer ara (curt termini)	Què preparar (mitjà termini)
1. Automatitzar la defensa	Procediments de contenció automàtica per als escenaris més freqüents. Classificació de les accions de resposta segons el seu impacte i reversibilitat. Mesurament del temps fins a la mitigació.	Telemetria centralitzada, inclosa la dels agents de la IA. IA al triatge, amb revisió humana. Exercicis a velocitat de màquina.
2. Reduir l'exposició	Inventari d'actius exposats i d'agents de la IA. Via ràpida per a vulnerabilitats explotades. Autenticació resistent a la pesca de dades i fi dels privilegis permanents.	Credencials de curta durada per a les identitats no humanes. Control del trànsit de sortida i registre de l'activitat dels agents. Segmentació, revisió de tercers i automatització de certificats.

3. Preparar-se per al futur quàntic	Responsable i pla de transició. Inventari criptogràfic de serveis exposats, VPN i certificats. Requisits postquàntics en les compres.	Intercanvi de claus híbrides en serveis web, API i VPN. Migració de les firmes en arrels de confiança i dispositius de llarga vida útil.
4. Coordinar-se com a país	Intel·ligència compartida en format llegible per màquina, incloses les amenaces de la IA. Procediment de resposta coordinada davant del compromís d'un proveïdor comú.	Capacitats compartides per a les organitzacions petites. Exercici nacional periòdic. Pla nacional de transició postquàntica i guia nacional de recomanacions.

Taula 18 - Full de ruta resumit per prioritat

10. ANNEX

Totes les fonts es van consultar l'octubre del 2026. S'indica el tipus per poder distingir què declara un fabricant sobre el seu producte d'allò que han avaluat, investigat o observat tercers.

Tipus de font	Com s'ha de llegir
Proveïdor	Informació publicada per un fabricant sobre el seu producte o sobre l'activitat observada a la plataforma. Declarada, no verificada de manera independent.
Intel·ligència d'amenaçes	Observació d'activitat real d'atacants per equips de recerca i resposta a incidents.
Investigació de seguretat	Troballes d'investigadors demostrades en entorns controlats. No impliquen que s'hagin explotat en atacs reals.
Investigació acadèmica	Treballs de recerca d'universitats o laboratoris, inclosos <i>preprints</i> sense revisió per parells.
Estudi sectorial	Enquestes i estudis basats en mostres d'organitzacions o experts.
Organisme públic o regulador	Documentació oficial de les autoritats o les institucions públiques.
Organisme sectorial o de normalització	Organitzacions que elaboren estàndards o que agrupen el sector i els equips de resposta.
Anàlisi sectorial	Valoració dels analistes o de les organitzacions del sector sobre informació de tercers.
Prensa	Cobertura periodística, generalista o especialitzada.

Taula 19 - Tipus de font utilitzats a l'informe

Font	URL	Tipus	Data
Anthropic - «Detecting and countering misuse of AI: September 2026»	https://www.anthropic.com/threat-intelligence-report-september-2026	Proveïdor	09/2026
Cloudflare - «Is your domain using post-quantum encryption? Now you can see for yourself»	https://blog.cloudflare.com/post-quantum-visibility/	Proveïdor	29/09/2026
CrowdStrike - «2026 CrowdStrike Global Threat Report: AI Accelerates Adversaries and Reshapes the Attack Surface»	https://www.crowdstrike.com/en-us/press-releases/2026-crowdstrike-global-threat-report/	Intel·ligència d'amenaçes	24/02/2026

Mandiant - M-Trends 2026	https://cloud.google.com/security/resources/m-trends	Intel·ligència d'amenaces	23/03/2026
Verizon - 2026 Data Breach Investigations Report	https://www.verizon.com/business/resources/reports/dbir/	Intel·ligència d'amenaces	2026
VulnCheck - «State of Exploitation 1H 2026»	https://www.vulncheck.com/blog/state-of-exploitation-1h-2026	Intel·ligència d'amenaces	28/07/2026
Mandiant - «AI Risk and Resilience in 2026»	https://cloud.google.com/security/resources/ai-risk-and-resilience-2026	Intel·ligència d'amenaces	09/2026
Microsoft - Digital Defense Report 2026	https://www.microsoft.com/en-us/security/security-insider/threat-landscape/2026-digital-defense-report	Intel·ligència d'amenaces	01/10/2026
Unit 42 (Palo Alto Networks) - «Securing AWS AgentCore Harness credentials»	https://unit42.paloaltonetworks.com/securing-aws-agentcore-harness-credentials/	Investigació de seguretat	18/09/2026
Zenity Labs - «SalesBleed: 0-click data exfiltration on Agentforce»	https://labs.zenity.io/post/salesbleed-0-click-data-exfiltration-on-agentforce	Investigació de seguretat	24/09/2026
Gidney (Google Quantum AI) - «How to factor 2048 bit RSA integers with less than a million noisy qubits»	https://arxiv.org/abs/2505.15917	Investigació acadèmica	05/2025
Babbush y Neven (Google Quantum AI) - «Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly»	https://research.google/blog/safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly/	Investigació acadèmica	31/03/2026
Pandey y Bhujang - «Poisoning the Watchtower: Prompt Injection Attacks Against LLM-Augmented Security Operations Through Adversarial Log Content»	https://arxiv.org/abs/2605.24421	Investigació acadèmica	23/05/2026
Global Risk Institute - «Quantum Threat	https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/	Estudi sectorial	09/03/2026

Timeline Report 2025»			
IBM - «2026 Cost of a Data Breach: AI adversaries and enterprise risk»	https://www.ibm.com/think/x-force/2026-cost-of-a-data-breach-ai-adversaries-enterprise-risk	Estudi sectorial	29/07/2026
Elastic - «2026 SANS SOC Survey: A decade of cyber defense insights»	https://www.elastic.co/resources/security/report/sans-soc-survey-insights-2026	Estudi sectorial	2026
NIST - SP 800-207 «Zero Trust Architecture»	https://csrc.nist.gov/pubs/sp/800/207/final	Organisme públic regulador	11/08/2020
Govern d'Andorra - «Estratègia de Ciberseguretat d'Andorra. Creació Agència de Ciberseguretat d'Andorra»	https://www.altaveu.com/uploads/s1/79/26/15/1025-presentacio-age-ncia-ciberseguretat.pdf	Organisme públic regulador	25/10/2021
Consell General - Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació	https://www.consellgeneral.ad/fitxers/document/s/lleis-2022/llei-22-2022-del-9-de-juny-de-mesures-per-a-la-seguretat-de-les-xarxes-i-dels-sistemes-d2019informacio	Organisme públic regulador	09/06/2022
NIST - AI Risk Management Framework (AI RMF 1.0)	https://www.nist.gov/itl/ai-risk-management-framework	Organisme públic regulador	26/01/2023
NIST - Cybersecurity Framework 2.0	https://www.nist.gov/cyberframework	Organisme públic regulador	26/02/2024
NIST - «NIST Releases First 3 Finalized Post-Quantum Encryption Standards»	https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards	Organisme públic regulador	13/08/2024
NIST - IR 8547 (borrador inicial) «Transition to Post-Quantum Cryptography Standards»	https://csrc.nist.gov/pubs/ir/8547/ipd	Organisme públic regulador	12/11/2024
Comisión Europea - «A Coordinated Implementation Roadmap for the	https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography	Organisme públic regulador	23/06/2025

Transition to Post-Quantum Cryptography»			
CISA - «CISA and Partners Release Guidance on Adopting Agentic AI Services»	https://content.govdelivery.com/accounts/USDHSCISA/bulletins/41544ff	Organisme públic o regulador	01/05/2026
OASIS - STIX 2.1 y TAXII 2.1	https://oasis-open.github.io/cti-documentation/	Organisme sectorial o de normalització	06/2021
FIRST - Traffic Light Protocol 2.0	https://www.first.org/tlp/	Organisme sectorial o de normalització	08/2022
ISO - ISO/IEC 27001:2022	https://www.iso.org/standard/27001	Organisme sectorial o de normalització	25/10/2022
ISO - ISO/IEC 42001:2023	https://www.iso.org/standard/42001	Organisme sectorial o de normalització	12/2023
CA/Browser Forum - Ballot SC-081v3 «Introduce Schedule of Reducing Validity and Data Reuse Periods»	https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/	Organisme sectorial o de normalització	11/04/2025
OWASP GenAI Security Project - «OWASP Top 10 for Agentic Applications»	https://genai.owasp.org/2025/12/09/owasp-top-10-for-agentic-applications-the-benchmark-for-agentic-security-in-the-age-of-autonomous-ai/	Organisme sectorial o de normalització	09/12/2025
Trusted Introducer - Ficha de CSIRT-AD	https://www.trusted-introducer.org/directory/teams/csirt-ad-ad.html	Organisme sectorial o de normalització	10/2026
PQShield - «EU PQC Workstream publishes ‘A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography’»	https://pqshield.com/eu-pqc-workstream-publishes-a-coordinated-implementation-roadmap-for-the-transition-to-post-quantum-cryptography/	Anàlisi sectorial	24/06/2025
WaterISAC - «JadePuffer Ransomware – First Reported Use of	https://www.waterisac.org/tlpclear-jadepuffer-ransomware-first-reported-use-of-agentic-ransomware	Anàlisi sectorial	09/07/2026

Agentic Ransomware»			
«A call for collective action on cyber defense» (llamamiento firmado por OpenAI, Anthropic, Google, Microsoft y otras organizaciones)	https://openai.com/collective-cyberdefense/	Anàlisi sectorial	27/08/2026
Cloud Security Alliance - «Autonomous AI Agent Breaches DIVD via Chained Zammad Zero-Days»	https://labs.cloudsecurityalliance.org/research/csa-research-note-zammad-ai-agent-breach-20261001-csa-styled/	Anàlisi sectorial	01/10/2026
Sysdig - «AI agent exploits Zammad zero-days in DIVD breach: What we know and how to detect it»	https://www.sysdig.com/blog/ai-agent-exploits-zammad-zero-days-in-divd-breach-what-we-know-and-how-to-detect-it	Anàlisi sectorial	02/10/2026
DNSimple - «SSL Certificate Validity Changes (2026 - 2029)»	https://support.dnssimple.com/articles/announcement-ssl-certificate-validity-changes/	Anàlisi sectorial	2026
Help Net Security - «Hundreds of Salesforce customer orgs hit in clever attack with potentially huge blast radius»	https://www.helpnetsecurity.com/2025/08/27/hundreds-of-salesforce-customer-orgs-hit-in-clever-attack-with-potentially-huge-blast-radius/	Prensa	27/08/2025
SecurityWeek - «M-Trends 2026: Initial Access Handoff Shrinks From Hours to 22 Seconds»	https://www.securityweek.com/m-trends-2026-initial-access-handoff-shrinks-from-hours-to-22-seconds/	Prensa	23/03/2026
CSO Online - «Google: The quantum apocalypse is coming sooner than we thought»	https://www.csoonline.com/article/4150887/google-the-quantum-apocalypse-is-coming-sooner-than-we-thought.html	Prensa	26/03/2026
Alto Andorra - «Andorra Cybersecurity	https://www.alto.ad/business/2026/04/andorra-cybersecurity-investment-drop-minis	Prensa	17/04/2026

Incidents Rise 5.6% to 1,624 in 2025»			
BleepingComputer - «JadePuffer ransomware used AI agent to automate entire attack»	https://www.bleepingcomputer.com/news/security/jadepuffer-ransomware-used-ai-agent-to-automate-entire-attack/	Prensa	04/07/2026
Axios - «OpenAI, Anthropic, Microsoft warn of growing AI cyberattacks»	https://www.axios.com/2026/08/27/openai-anthropic-issue-dire-cyber-threat-warning	Prensa	27/08/2026
BleepingComputer - «Automated AI agent used to breach cybersecurity nonprofit DIVD»	https://www.bleepingcomputer.com/news/security/automated-ai-agent-used-to-breach-cybersecurity-nonprofit-divd/	Prensa	29/09/2026
Help Net Security - «AI is giving attackers a head start, Microsoft warns»	https://www.helpnetsecurity.com/2026/10/02/ai-cybersecurity-threats-microsoft-report/	Prensa	02/10/2026
Cybersecurity Dive - «Defending against AI-fueled cyberattacks requires focus on identity, data governance, Microsoft says»	https://www.cybersecuritydive.com/news/ai-cyberattacks-automation-identity-data-microsoft-report/832020/	Prensa	02/10/2026
eSecurity Planet - «IBM 2026 Cost of a Data Breach Report: Key Findings»	https://www.esecurityplanet.com/cybersecurity/ibm-2026-cost-of-a-data-breach-report-key-findings/	Prensa	2026
Expert Insights - «Supply Chain Breaches Surge 60% To Hit Half Of All Incidents»	https://expertinsights.com/news/supply-chain-breaches-surge-60-to-hit-half-of-all-incidents	Prensa	2026

Taula 20 - Fonts de l'informe

11. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat d'Andorra Digital. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés d'Andorra Digital.