ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

# Informe de Ciberintel·ligència

# La importància de la recerca, el desenvolupament i la innovació (R+D+I) a la ciberseguretat


TLP: WHITE

AGOST 2024

## FITXA DEL DOCUMENT

| Versió | Redactat/Revisat per | Aprovat per | Data aprovació | Data publicació |
|---|---|---|---|---|
| 1.0 | ANC-AD | ANC-AD | 19/08/2024 | 21/08/2024 |

| Registre de canvis | | | |
|---|---|---|---|
| Versió | Pàgines | Data Modificació | Motiu del canvi |
| | | | |

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

## ÍNDEX

# 1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo 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 món s'enfronta a un repte creixent en matèria de ciberseguretat que requereix una resposta urgent. Amb l'avenç continuat de la digitalització i la innovació tecnològica, les amenaces esdevenen cada vegada més complexes i sofisticades. Entre elles s'hi troben des de la ciberdelinqüència, que impacta tant les persones com les empreses, fins a l'espionatge, ei ciberterrorisme i els atacs maliciosos adreçats a infraestructures crítiques i dades delicades.

La recerca, el desenvolupament i la innovació (R+D+I) són vitals en els camps com ara la ciberseguretat, on l'evolució ràpida de les tecnologies i les tècniques per comprometre-les exigeix mantenir-se constantment un pas per endavant. L'objectiu ha de ser generar productes i solucions que siguin reproduïbles en diferents contextos, i és fonamental que tinguin el suport d'un model de negoci ben definit que contempli la seva comercialització.

Per això, és vital tenir un teixit empresarial potent en ciberseguretat i competitiu internacionalment, que inverteixi en recerca, desenvolupament i innovació, i en solucions i serveis que contribueixin a la protecció de les organitzacions i a la generació de riquesa.

És crucial que les empreses adoptin un enfocament més proactiu cap a la recerca, el desenvolupament i la innovació, no només per millorar la seva mateixa competitivitat, sinó també per enfortir la ciberseguretat a nivell nacional i internacional. En aquest context, la col·laboració entre el sector públic i el privat, com també l'impuls de polítiques que incentivin la inversió en R+D+I, són elements clau per avançar en la creació d'un ecosistema robust i resilient enfront de les amenaces cibernètiques.

Aquest informe té com a objectiu explicar com la recerca, el desenvolupament i la innovació són fonamentals per enfrontar-se a les amenaces emergents a l'entorn digital. L'informe subratlla la necessitat de mantenir-se a l'avantguarda en la creació de solucions avançades per protegir els sistemes d'informació, millorar la detecció i la resposta a ciberatacs, i garantir la seguretat de les dades.

# 3. QUÈ SIGNIFICA R+D+I EN CIBERSEGURETAT?

El concepte d'R+D+I en ciberseguretat fa referència a les activitats i els esforços adreçats a la creació de noves tecnologies, mètodes, processos i solucions innovadores amb l'objectiu de millorar la seguretat digital. Com hem assenyalat, l'R+D+I no es limita només a desenvolupar solucions noves, han de ser replicables i basades en un model de negoci. Si no és així, hi ha el risc de crear productes tècnicament impecables, però destinats al fracàs per no assolir una viabilitat comercial.

Cada component de l'R+D+I té un rol específic.

- **Recerca (R):** consisteix en una anàlisi exhaustiva i un estudi detallat dels problemes actuals o emergents en ciberseguretat, a més de l'exploració de nous coneixements tant teòrics com pràctics. Això abasta des de la recerca sobre vulnerabilitats i amenaces, fins a la identificació de noves tècniques d'atac i la formulació d'estratègies de defensa. Aquest tipus de recerca és crucial per anticipar-se als riscos i desenvolupar les bases sobre les quals es desenvoluparan futures solucions.

- **Desenvolupament (D):** significa dur a la pràctica els resultats obtinguts de la recerca per crear eines, programari, tecnologies o sistemes nous que enforteixin la ciberseguretat. Aquest procés inclou l'elaboració de protocols nous de seguretat, el disseny d'aplicacions més segures, l'automatització de processos per a la detecció d'amenaces i l'optimització d'infraestructures ja existents.

- **Innovació (I):** en analitzar la innovació en l'àmbit de la ciberseguretat, és essencial fer-ho des de dues perspectives. En primer lloc, des de la innovació que hi ha a les tecnologies i estratègies dissenyades per protegir xarxes, sistemes informàtics, dades i sistemes financers a nivell global. Això fa referència a la introducció de solucions noves i eficaces que aborden desafiaments específics de la ciberseguretat. Inclou, per exemple, la incorporació de tecnologies noves, com ara la intel·ligència artificial (IA) o la cadena de blocs, com també la implementació de pràctiques i normatives noves. En segon lloc, és fonamental comprendre que la ciberseguretat permet que les empreses i les organitzacions operin, per la qual cosa té un rol important en la manera com funcionen les empreses.

## 3.1. Per què l'R+D+I a la ciberseguretat?

La probabilitat que es produeixin ciberatacs ha augmentat considerablement. La complexitat creixent de les tecnologies emprades augmenta la superfície d'atac i la innovació constant per part dels ciberdelinqüents incrementa la seva capacitat per amenaçar la seguretat de la informació. Els actors d'amenaça són molt actius i fan servir avenços tecnològics per atacar les organitzacions.

Com ja hem esmentat, l'impacte de ciberatacs és molt més gran per l'augment en l'ús de les tecnologies en els processos de negoci de les organitzacions. La ràpida evolució de les tecnologies i la necessitat per part de les organitzacions per adoptar-les i d'aquesta manera mantenir la seva competitivitat i millorar la seva eficiència porta associada un increment en el nombre de vulnerabilitats a les quals estan exposades aquestes entitats.

Per tant, en un entorn on les amenaces cibernètiques estan en evolució constant, l'R+D+I a la ciberseguretat és essencial per mantenir un avantatge sobre els atacants, garantir la seguretat dels sistemes d'informació i protegir dades delicades. Aquest enfocament permet desenvolupar solucions noves i millorar contínuament les defenses que permet adaptar-se a les diferents tècniques dels ciberdelinqüents. Així, la inversió en recerca, desenvolupament i innovació no només reforça la protecció existent, sinó que també anticipa i mitiga amenaces futures.

En resum, les empreses, els governs i les organitzacions inverteixen en R+D+I per desenvolupar defenses més robustes, garantir la resiliència davant d'atacs i promoure la seguretat en un entorn digital cada vegada més complex.

## 3.2. Tecnologies per a l'R+D+I en ciberseguretat

A través de l'ús de noves tecnologies com ara la intel·ligència artificial (IA), la computació quàntica i la cadena de blocs, es poden crear solucions avançades per protegir els sistemes d'informació, millorar la detecció i resposta als ciberatacs, a més de garantir la seguretat de les dades en un món cada vegada més interconnectat.

### 3.2.1 Intel·ligència artificial (IA)

La intel·ligència artificial (IA) és una tecnologia emergent que està generant una disrupció en tots els sectors professionals. En l'àmbit de la ciberseguretat el seu impacte és significatiu, perquè eleva la protecció a un nivell superior.

La IA juga un paper crucial en l'R+D+I a la ciberseguretat en accelerar-ne els avenços i millorar l'eficàcia de les solucions de protecció. A mesura que continua evolucionant, la IA es posiciona com una eina clau per enfrontar-se als reptes cada vegada més complexos en la protecció digital. La IA aporta la seva contribució, entre d'altres, de les maneres següents:

- **Automatització de la recerca:** la IA pot analitzar grans volums de dades i detectar patrons complexos, i permetre identificar noves amenaces i vulnerabilitats de manera més ràpida i precisa. Això accelera el procés de recerca i descobriment de tècniques noves d'atac.

- **Desenvolupament de solucions intel·ligents:** la IA permet el desenvolupament d'eines que aprenen i s'adapten a atacs nous. Aquestes solucions intel·ligents poden predir comportaments maliciosos que es basen en patrons previs i ajustar les defenses en temps real.

- **Optimització d'algoritmes criptogràfics:** a l'àrea d'innovació, la IA ajuda a dissenyar i optimitzar algoritmes criptogràfics més avançats i resistents enfront d'amenaces emergents, incloses les que podrien provenir de la computació quàntica, de la qual en parlarem més endavant.

- **Detecció d'amenaces i respostes a incidents:** la IA permet desenvolupar sistemes de ciberseguretat capaços de detectar amenaces potencials. Igualment, facilita l'automatització de respostes a incidents, i redueix el temps de reacció i alhora minimitza l'impacte dels atacs.

- **Innovació en ciberdefensa autònoma:** la IA impulsa la creació de sistemes autònoms que no només detecten les amenaces, sinó que també aprenen d'elles, permeten una millora contínua de les defenses i desenvolupen solucions preventives i innovadores.

En resum, la IA impulsa l'R+D+I a la ciberseguretat en accelerar la recerca, facilitar el desenvolupament de solucions avançades i fomentar la innovació per abordar les amenaces cada vegada més complexes de l'entorn digital.

Els algoritmes de la IA permeten l'aprenentatge automàtic, que es coneix com a Machine Learning (ML), el qual ajuda el sistema a aprendre patrons, i adaptar-se per simplificar la resposta als riscs d'incidents.

**Machine Learning (ML)**

Actualment, gran part de les recerques i els avenços més significatius en el sector de la ciberseguretat provenen de la subdisciplina de la IA coneguda com a Machine Learning (ML), la qual s'enfoca en l'ús d'algoritmes aplicats a grans volums de dades.

El ML és una branca de la IA basada en la idea que els sistemes poden aprendre de les dades, identificar patrons i prendre decisions amb una intervenció humana mínima. El ML està transformant la detecció d'intrusions, i està permetent que els sistemes aprenguin dels patrons de dades i reconèixer activitats sospitoses o anòmales pràcticament en temps real. Aquests sistemes basats en ML es poden adaptar i evolucionar amb les tàctiques noves dels atacants, cosa que significa que poden detectar amenaces emergents més ràpidament i amb una precisió més gran.

Ras i curt, el ML permet que les màquines aprenguin a fer tasques determinades sense estar programades explícitament per fer-ho i, d'aquesta manera, evitar possibles atacs.

### 3.2.2 Computació quàntica

La computació quàntica representa un paradigma nou que fusiona elements de la computació tradicional, la física i les matemàtiques per abordar problemes complexos i resoldre algoritmes, i fa servir capacitats de processament sense precedents.

La computació quàntica té el potencial de transformar l'R+D+I a la ciberseguretat en oferir ordinadors quàntics amb capacitats de processament i resolució de problemes molt més ràpids i eficients que els ordinadors tradicionals. En resum, aquests ordinadors permeten processar grans volums d'informació en una fracció del temps que trigarien a fer-ho els ordinadors convencionals.

Algunes de les seves contribucions clau inclouen:

- **Optimització de sistemes de detecció d'amenaces**: la capacitat de la computació quàntica per processar grans volums de dades de la manera més eficient pot millorar els sistemes d'IA que es fan servir a la ciberseguretat. Això permetria detectar amenaces més ràpidament i amb una precisió més gran, i analitzar patrons complexos de dades que els ordinadors tradicionals no poden gestionar amb la mateixa eficàcia.

- **Modelatge avançat de ciberatacs**: pel que fa a la recerca, la computació quàntica permet dur a terme simulacions més detallades i precises de possibles ciberatacs, i ajuda els experts a predir com podrien evolucionar les amenaces en el futur i a desenvolupar defenses més sòlides.

- **Millorar en l'optimització de xarxes de seguretat**: la computació quàntica també pot contribuir a optimitzar el disseny i la gestió de xarxes de seguretat complexes. La seva capacitat per resoldre problemes d'optimització permet que les organitzacions trobin solucions més eficients per protegir grans infraestructures tecnològiques.

- **Xifratge:** La computació quàntica pot ajudar a millorar la seguretat de la informació en permetre la creació d'algoritmes de xifratge més avançats dels que hi ha en l'actualitat, de manera que es poden fer servir a l'hora de generar contrasenyes i certificats, com també pel que fa al xifratge de les connexions, arxius o dades. No obstant això, encara que sembli paradoxal, aquest paradigma nou suposa un desafiament en termes de ciberseguretat, perquè suposa una amenaça sobre els mecanismes de xifratge convencionals.

- **Desenvolupament de criptografia postquàntica**: encara que la computació quàntica no representa una amenaça avui dia, atès que el seu ús està limitat a un petit nombre d'ordinadors a nivell mundial, ben aviat es desenvoluparà més i se'n democratitzarà l'accés. Quan passi això, el camp de la ciberseguretat s'haurà d'adaptar, i implementar nous algoritmes criptogràfics que puguin resistir la potència de processament d'un ordinador quàntic i evitar que aquestes màquines superin les barreres actuals de protecció. Anticipar-se a aquest canvi serà crucial per salvaguardar la integritat de la informació en un futur on la computació quàntica serà una realitat comuna. Amb la computació quàntica s'impulsa la recerca i el desenvolupament d'algoritmes criptogràfics nous i resistents als atacs quàntics. Això és crucial perquè les tècniques de xifratge actuals podrien ser vulnerables a futurs ordinadors quàntics. L'R+D+I en aquesta àrea se centrarà a crear sistemes criptogràfics que mantinguin la confidencialitat i la seguretat de les dades fins i tot en un entorn dominat per la computació quàntica.

### 3.2.3 Cadena de blocs

La cadena de blocs (*blockchain*) és una tecnologia que va sorgir el 2008 per facilitar les transaccions bancàries segures mitjançant l'ús de la criptografia. Aquesta tecnologia contribueix significativament a l'R+D+I a la ciberseguretat en oferir solucions noves per protegir dades, millorar-ne l'autenticació, assegurar les transaccions i crear sistemes més resilients i auditables. És una font clau d'innovació per desenvolupar estratègies noves que enforteixin la seguretat digital en un món cada vegada més connectat. Algunes de les formes principals de contribució de la cadena de blocs a l'R+D+I són:

- **Millora de la seguretat de les dades:** aquesta tecnologia introdueix una capa addicional de seguretat en oferir una estructura descentralitzada i immutable. Això significa que les dades emmagatzemades en una cadena de blocs no poden ser alterades sense el consens de la xarxa, la qual cosa dificulta els intents de manipulació o els ciberatacs. Aquest enfocament està impulsant la innovació en noves maneres de protegir la integritat de la informació i prevenir bretxes de seguretat.

- **Desenvolupament de mètodes nous d'autenticació:** la tecnologia de cadena de blocs està impulsant la recerca i el desenvolupament de sistemes avançats d'autenticació, com ara la identificació descentralitzada. Aquests sistemes permeten verificar la identitat dels usuaris sense necessitat d'intermediaris, i reduir l'exposició a atacs de pesca, frau d'identitat i altres amenaces cibernètiques.

- **Seguretat a les transaccions**: aquesta tecnologia permet fer transaccions segures i verificables sense necessitat d'intermediaris. Això està impulsant la creació de solucions innovadores per protegir transaccions financeres, contractes intel·ligents i altres processos que requereixen nivells alts de seguretat i confiança.

- **Resiliència operativa**: la naturalesa descentralitzada de la cadena de blocs proporciona una resiliència més gran contra els atacs distribuïts, com ara els atacs DDoS, que poden paralitzar sistemes centralitzats. En l'àmbit de l'R+D+I això fomenta la creació de xarxes més segures i resistents, capaces de continuar operant fins i tot enfront d'intents de sabotatge.

- **Traçabilitat i auditoria**: una de les contribucions més significatives de la cadena de blocs és la capacitat de garantir la integritat de la informació i la seva traçabilitat, perquè facilita la traçabilitat de la informació i la transparència en els processos. Això ha permès innovar en sistemes d'auditoria que garanteixen que tots els moviments dintre de la xarxa es poden verificar i auditar en temps real, i proporcionen una confiança i fiabilitat més grans en la gestió de les dades i els processos.

  La naturalesa de la cadena de blocs reforça les defenses cibernètiques, assegura les plataformes i preveu activitats il·legals a través de mecanismes consensuats entre un gran nombre d'actors, cosa que dificulta considerablement les activitats malicioses i/o facilita la seva detecció. Això és gràcies a les seves característiques d'immutabilitat, transparència, auditabilitat, encriptació i resiliència operativa.

# 4. QUI IMPULSA L'R+D+I A EUROPA?

A Europa, l'R+D+I a la ciberseguretat està impulsada per una combinació d'actors públics i privats, com ara institucions governamentals, organitzacions internacionals, empreses tecnològiques, universitats i centres de recerca.

L'R+D+I a la ciberseguretat a nivell europeu ha experimentat avenços significatius en els darrers anys, impulsats per la preocupació creixent per la seguretat digital i la necessitat de protegir els ciutadans, les infraestructures crítiques i les empreses enfront de les amenaces cibernètiques. La Unió Europea (UE) ha estat desenvolupant diverses iniciatives i projectes per fomentar la recerca, el desenvolupament i la innovació en aquest àmbit. Igualment, està invertint en tecnologies emergents com ara la IA aplicada a la ciberseguretat, la cadena de blocs per garantir la integritat de les dades, i la criptografia avançada per protegir la informació en un entorn d'amenaces creixents.

Tot seguit, es destaquen alguns dels avenços i enfocaments principals.

## 4.1. Programes europeus

Els programes europeus com ara Digital Europe, el Fons Europeu de Defensa i Horizon Europe estan centrats en el finançament de projectes i programes relacionats amb la ciberseguretat.

### Horizon Europe

Horizon Europe és el principal programa de recerca i innovació de la Comissió Europea. Aquest programa finança projectes que cerquen desenvolupar tecnologies i solucions de seguretat noves, com també millorar la resiliència de les infraestructures digitals.

### Digital Europe Programme (DEP)

Aquest programa, complementari a Horizon Europe, se centra en la construcció de capacitats digitals, inclosa la ciberseguretat, la IA, la supercomputació (forma de computació d'alt rendiment) i l'educació digital.

## 4.2. Actors europeus

### Comissió Europea

Tal com hem esmentat, la Comissió Europea impulsa l'R+D+I a través de programes de finançament com ara Horizon Europe, que ofereix fons per a projectes de recerca i innovació en àrees clau com ara la ciberseguretat, la intel·ligència artificial i les tecnologies avançades.

### Centre Europeu de Competència en Ciberseguretat

L'any 2021, la UE va establir el Centre Europeu de Competència en Ciberseguretat a Bucarest, Romania. Aquest centre coordina la inversió en recerca i desenvolupament de ciberseguretat a

nivell europeu, i impulsa la col·laboració entre els estats membres, el sector i el món acadèmic. El seu objectiu és enfortir la capacitat de ciberseguretat de la UE i fomentar la innovació, amb el suport a les petites i les mitjanes empreses (PIME) i als centres de recerca en el desenvolupament de noves tecnologies de ciberseguretat.

### Institut Europeu d'Innovació i Tecnologia (EIT)

A través de les seves comunitats de coneixement i innovació, l'EIT finança projectes col·laboratius d'R+D+I en àrees diferents, com ara la ciberseguretat, i promou associacions entre empreses, universitats i centres de recerca.

### Xarxa de Centres de Competència en Ciberseguretat

Juntament amb el Centre Europeu de Competència en Ciberseguretat, la UE ha promogut la creació d'una xarxa de Centres de Competència en Ciberseguretat en tots els estats membres. Aquests centres col·laboren en projectes d'R+D+I, on es comparteixen coneixements i tecnologies per millorar la ciberseguretat arreu d'Europa.

La xarxa facilita la transferència de tecnologia i la cooperació transnacional, cosa que permet que les innovacions en ciberseguretat desenvolupades en un país siguin adoptades i adaptades per altres.

### Agència de la Unió Europea per a la Ciberseguretat (ENISA)

L'ENISA juga un paper crucial en la coordinació dels esforços en R+D+I a nivell europeu. Aquesta entitat treballa en estreta col·laboració amb estats membres i el sector privat per identificar necessitats emergents, fomentar l'estandardització i promoure l'adopció de les millors pràctiques en ciberseguretat.

L'ENISA també organitza exercicis de ciberseguretat a gran escala, com ara Cyber Europe, on se simulen incidents de ciberseguretat per contribuir a millorar la preparació i la resposta en tota la UE.

## 4.3. Projectes europeus emblemàtics i avenços tecnològics

Projectes com ara CyberSec4Europe, SPARTA, CONCORDIA i ECHO són exemples de xarxes i consorcis finançats per la UE que agrupen investigadors, universitats, empreses i altres entitats per treballar en solucions avançades de ciberseguretat. Aquests projectes aborden desafiaments específics, com ara la protecció d'infraestructures crítiques, la privacitat de les dades i la lluita contra la ciberdelinqüència.

## 5. CONCLUSIONS

Tal com s'ha explicat a l'informe, l'R+D+I a la ciberseguretat és un dels pilars essencials per abordar els desafiaments actuals i futurs, i alhora assegura que les tecnologies i els sistemes romanguin segurs i protegits contra les amenaces cada vegada més avançades.

Atès l'avanç ràpid de la tecnologia i el nombre creixent de ciberamenaces, l'R+D+I a la ciberseguretat cerca innovar i desenvolupar solucions noves que puguin preveure, detectar, mitigar i respondre a aquests riscos de manera eficaç.

Tot seguit, ressaltem alguns punts que considerem rellevants sobre l'R+D+I:

- **Ha de ser una prioritat per a la ciberseguretat:** la inversió en recerca, innovació i desenvolupament a la ciberseguretat hauria de ser una prioritat tant per als actors públics com privats, de cara a millorar la resiliència del sector. La capacitat d'anticipar-se a les amenaces constants i desenvolupar solucions efectives depèn en gran manera d'una inversió constant i estratègica en R+D+I.

- **És un motor de protecció avançada:** les tecnologies emergents, com ara la intel·ligència artificial, la computació quàntica i la cadena de blocs, estan revolucionant la ciberseguretat en oferir noves maneres de protegir les dades, els sistemes i les xarxes. L'adopció d'aquestes tecnologies està permetent la creació d'algoritmes de xifratge més robustos, sistemes de detecció d'amenaces més precisos i xarxes més segures i resilients.

- **La col·laboració publicoprivada és un dels factors d'èxit:** l'èxit de l'R+D+I a la ciberseguretat a Europa depèn en gran manera de la col·laboració entre actors públics i privats. Institucions governamentals, universitats, centres de recerca i empreses tecnològiques poden crear (i ho estan fent) un ecosistema col·laboratiu que fomenta el desenvolupament de noves solucions innovadores i protegeix les infraestructures crítiques enfront dels ciberatacs.

- **Necessitats de preparar-se per al futur:** a mesura que les tecnologies disruptives com ara la computació quàntica es van estenent, sorgeix la necessitat urgent de desenvolupar mecanismes nous de protecció adaptats a les capacitats d'aquestes tecnologies. Per tant, la inversió en R+D+I no només s'ha d'enfocar envers el present, sinó anticipar desafiaments del futur, i assegurar que les solucions de ciberseguretat evolucionin al ritme de les amenaces tecnològiques.

- **Impacte econòmic i social:** La ciberseguretat ja no és un component aïllat de la infraestructura digital; és un element clau per a la competitivitat econòmica i la confiança en els sistemes digitals. Les iniciatives en R+D+I no només protegeixen les dades i la privacitat dels usuaris, sinó que també impulsen el creixement econòmic en crear noves oportunitats de negoci i ocupació en el sector de la ciberseguretat.

Tot i que l'R+D+I a la ciberseguretat ha permès grans avenços, encara hi ha reptes significatius, com ara la complexitat creixent dels ciberatacs i l'escassedat de talent especialitzat en ciberseguretat. Tanmateix, aquests reptes també representen oportunitats per continuar invertint en formació, innovació i desenvolupament de noves capacitats.

## 6. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. 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 de l'Agència Nacional de Ciberseguretat d'Andorra.