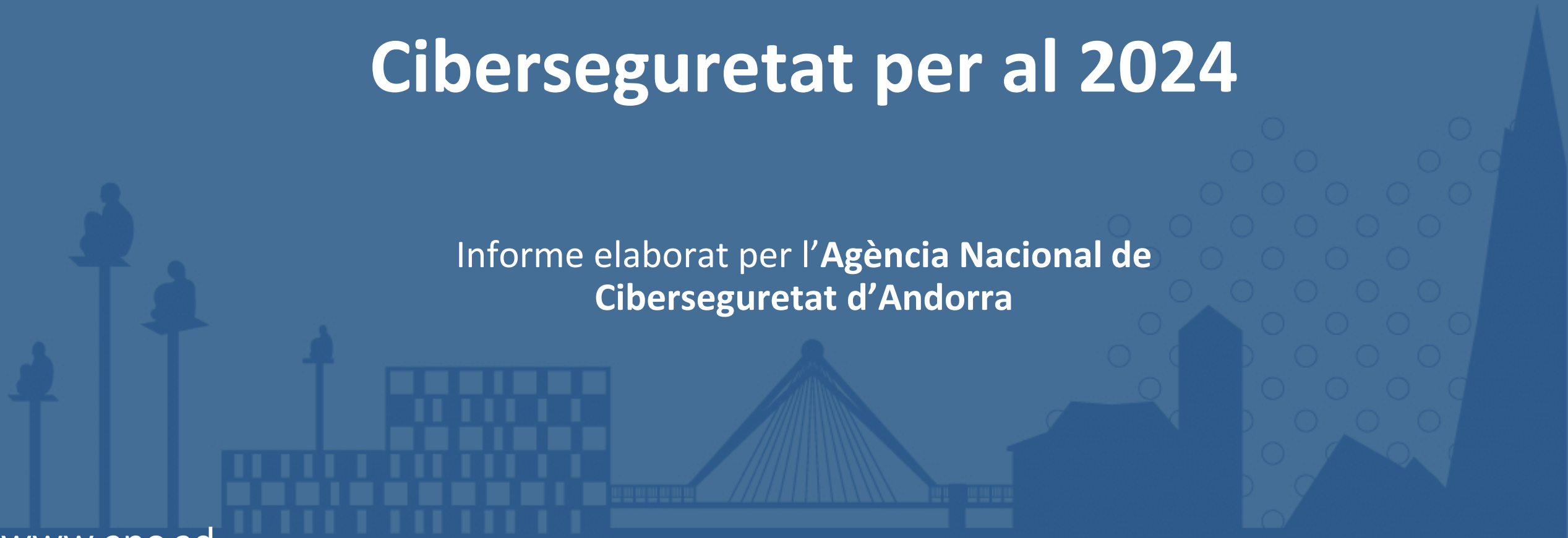
ANDORRA DIGITAL

Agència Nacional de Ciberseguretat d'Andorra

Prediccions i tendències clau Ciberseguretat per al 2024

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



www.anc.ad

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

El 2023 ha sigut un any marcat pels nombrosos desastres digitals en forma de ciberatacs que han tingut lloc arreu del món. A mesura que les empreses emmagatzemin més dades al núvol i que segueixi creixent el nombre de dispositius connectats a internet, la ciberseguretat serà cada vegada més una «assignatura troncal» per a totes les organitzacions.

A mesura que ens acostem al 2024, es fa més palès que en l'àmbit de la ciberseguretat es produiran canvis transformadors. Les amenaces cibernètiques no només són cada vegada més freqüents, sinó que s'estan tornant més sofisticades i desafiants per als paradigmes de seguretat tradicionals. Tenint en compte que el panorama digital evoluciona tan de pressa, comprendre les pròximes tendències és una qüestió de previsió i una necessitat de preparació.

L'objectiu d'aquest document és desentranyar les deu principals tendències i prediccions de ciberseguretat per al proper any, i oferir informació sobre com les tecnologies s'estan alineant amb aquests canvis per enfortir les nostres defenses digitals. Des de l'augment de la IA en la ciberseguretat fins a la creixent importància de la seguretat mòbil, ens endinsarem en les previsions de futur per a aquest camp crític.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

1

Prediccions i tendències clau
Ciberseguretat 2024

L'auge de la computació quàntica i el seu impacte en la ciberseguretat

ANDORRA DIGITAL

ANC-AD

1

L’auge de la computació quàntica i el seu impacte en la ciberseguretat

La computació quàntica, un camp que evoluciona ràpidament, està revolucionant la manera com pensem sobre el processament de dades i la resolució de problemes. A diferència de la computació clàssica, que utilitza bits representats amb zeros i uns, la computació quàntica fa servir qbits. Els qbits poden existir en diversos estats simultàniament, gràcies a la superposició quàntica. Això permet als ordinadors quàntics processar grans quantitats de dades a una velocitat sense precedents, de manera que poden resoldre problemes complexos molt més de pressa que els ordinadors tradicionals.

L’auge de la computació quàntica presenta tant oportunitats com desafiaments per a la ciberseguretat. D’una banda, el seu immens poder de processament ofereix el potencial per enfortir les mesures de ciberseguretat: la computació quàntica pot millorar els mètodes de xifratge, desenvolupar algoritmes més sofisticats per detectar amenaces cibernètiques i gestionar de manera eficient les operacions de dades segures a gran escala.

D’altra banda, la computació quàntica representa amenaces significatives per als protocols de ciberseguretat actuals. La seva capacitat per trencar ràpidament els mètodes de xifratge tradicionals, com RSA i ECC, pot fer que molts sistemes de seguretat existents esdevinguin vulnerables. Aquesta vulnerabilitat posa en relleu la necessitat urgent de desenvolupar tècniques de xifratge resistents als quàntics, un camp conegut com a criptografia postquàntica.

A mesura que avança el 2024, el panorama de la ciberseguretat haurà d’evolucionar ràpidament per aprofitar els beneficis i mitigar els riscos que comporta la computació quàntica. Això inclou l’actualització dels mètodes de xifratge actuals i la preparació dels sistemes per tal que siguin resistents a les capacitats avançades de les tecnologies quàntiques.

ANDORRA DIGITAL

Agència Nacional de Ciberseguretat d'Andorra

2

Prediccions i tendències clau
Ciberseguretat 2024

La IA i l'aprenentatge automàtic en la ciberseguretat

ANDORRA DIGITAL

ANC-AD

2

La IA i l'aprenentatge automàtic en la ciberseguretat

El 2024 la IA i l'aprenentatge automàtic (ML) tindran un paper més crític en la ciberseguretat. Les capacitats avançades d'anàlisi de dades de la IA s'utilitzen cada vegada més per identificar i predir les amenaces cibernètiques, cosa que millora els sistemes de detecció precoç. Els algorismes d'aprenentatge automàtic estan evolucionant per reconèixer i respondre millor a les noves amenaces, fet que amb el temps millora les mesures defensives. El 2024 esperem veure algorismes d'IA que proporcionin anàlisis d'amenaces en temps real, la qual cosa permetrà respostes més ràpides i precises als incidents cibernètics. És probable que l'aprenentatge automàtic evolucioni per adaptar i actualitzar els protocols de ciberseguretat de forma autònoma, i es redueixi així la dependència de les actualitzacions manuals.

També podem ser testimonis de l'aparició de bots de seguretat impulsats per la IA programats per identificar i neutralitzar de manera independent les amenaces cibernètiques, cosa que faria que la seguretat de la xarxa fos més proactiva i menys reactiva. Tot això significa un canvi cap a sistemes de ciberseguretat més intel·ligents i autònoms, impulsats pels avenços en IA i ML.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

3

Prediccions i tendències clau
Ciberseguretat 2024

Atacs de pesca «vitaminats» amb la IA generativa

ANDORRA DIGITAL

3

Atacs de pesca «vitaminats» amb la IA generativa

www.anc.ad

ANC-AD

Els atacs d'enginyeria social adreçats a enganyar els usuaris perquè donin accés als atacants als seus sistemes també seran cada vegada més sofisticats. Les eines d'IA generativa (com ChatGPT) permeten fer atacs de manera més intel·ligent i personalitzada, i els hipertrucatges (atacs *deepfake*) seran com més va més freqüents.

Atacs més sofisticats:

- La capacitat de generar llenguatge natural d'eines com ChatGPT podria ser explotada per crear missatges més convincents i personalitzats en els atacs de pesca (*phishing*).
- Els atacants podrien utilitzar informació recopilada en línia per personalitzar els atacs, i fer que els missatges d'enginyeria social siguin encara més creïbles i difícils de detectar.

Hipertrucatges:

- Els hipertrucatges no es limiten només a l'àmbit de l'enginyeria social verbal. La manipulació de contingut multimèdia, com vídeos i àudios, també es pot fer servir per enganyar les persones i comprometre la seguretat.
- La detecció d'hipertrucatges esdevé un desafiament creixent. Per això, les solucions basades en intel·ligència artificial, com algorismes d'aprenentatge profund, també s'estan desenvolupant per contrarestar aquesta amenaça.

Respostes i solucions:

- La conscienciació i l'educació són essencials. Els usuaris han de ser conscients dels riscos i aprendre a identificar possibles intents d'enginyeria social.
- La implementació de polítiques de seguretat robustes i la capacitació contínua poden ajudar a enfortir les defenses contra aquests atacs.
- La incorporació de tecnologies basades en intel·ligència artificial, com sistemes de detecció d'anomalies i anàlisis de comportament, pot ser fonamental per identificar patrons inusuals que podrien indicar un atac.
- L'adopció de models de «confiança zero» implica que la confiança no s'assumeix, fins i tot dins de la xarxa d'una organització, i que cal verificar constantment les identitats i els accessos.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

4

Prediccions i tendències clau
Ciberseguretat 2024

Seguretat de confiança zero *ZERO TRUST*

ANDORRA DIGITAL

ANC-AD

4

Seguretat de confiança zero
ZERO TRUST

El concepte de «confiança zero» *(zero trust)* va agafar embranzida el 2023, i ha evolucionat d'un enfocament de nínxol a un aspecte fonamental de l'estratègia de ciberseguretat. Essencialment, la seguretat de confiança zero es basa en el principi de «mai confiar, sempre verificar». A diferència dels models de seguretat tradicionals, que se centren a assegurar el perímetre, el de confiança zero assumeix que les amenaces poden existir tant fora com dins de la xarxa.

En un modelo de confiança zero, cada sol·licitud d'accés, independentment de l'origen o de la xarxa en què es troba, es tracta com una amenaça potencial. Això requereix una rigorosa verificació d'identitat, estrictes controls d'accés i supervisió contínua de les activitats de la xarxa. La implementació de la seguretat de confiança zero implica un enfocament integral que abraça diversos aspectes de la ciberseguretat, inclosa l'autenticació de l'usuari, la seguretat dels punts finals i l'accés amb menys privilegis.

Un dels beneficis clau de la confiança zero és la seva eficàcia per mitigar els riscos que plantegen les amenaces internes i el moviment lateral dels atacants dins d'una xarxa. Les organitzacions utilitzen cada vegada més serveis al núvol i models de treball remot i, per tant, augmenta la rellevància de la seguretat de confiança zero, ja que ofereix una arquitectura flexible i adaptable per assegurar entorns de TI diversos i distribuïts.

La transició a un marc de confiança zero aquest 2024 representa un canvi de paradigma en relació amb la ciberseguretat, ja que se centra en la verificació contínua i els drets d'accés mínims per reduir les vulnerabilitats i millorar la seguretat general de la xarxa.

ANDORRA DIGITAL

Agència Nacional de Ciberseguretat d'Andorra

5

Prediccions i tendències clau
Ciberseguretat 2024

Estratègia de proveïdor de seguretat consolidada

www.anc.ad

ANDORRA DIGITAL

5

Estratègia de proveïdor de seguretat consolidada

www.anc.ad

ANC-AD

La ciberseguretat s'està tornant més complexa dia a dia. Amb el creixement continu de la superfície d'atac, l'expansió dels proveïdors planteja desafiaments com ara més complexitat en la gestió, problemes d'integració i possibles escletxes en la cobertura de seguretat per a les organitzacions.

El gran volum i la varietat de les amenaces en l'ecosistema digital d'una organització han fet que sigui poc pràctic abordar cada amenaça que s'identifica individualment. Com a resposta estratègica, es recomana que les empreses facin la transició a un sistema de gestió contínua de les amenaces. Aquest canvi implica ampliar l'abast de les avaluacions d'amenaces per incloure-hi les cadenes de subministrament integrades, atès que les operacions comercials modernes estan interconnectades.

Si bé la reducció de costos no hauria de ser el principal impulsor d'una estratègia de ciberseguretat consolidada, porta a un creixement general en la postura de ciberseguretat de l'organització.

- Estratègia de seguretat unificada
- Gestió simplificada
- Visibilitat millorada
- Reducció de la complexitat
- Comunicació optimitzada
- Aplicació coherent de polítiques
- Resposta a incidents millorada
- Economies d'escala

.

ANDORRA DIGITAL

Agència Nacional de Ciberseguretat d'Andorra

6

Prediccions i tendències clau
Ciberseguretat 2024

Més importància de la seguretat d'IdC

ANDORRA DIGITAL

6

Més importància de la seguretat d'IdC

www.anc.ad

ANC-AD

A mesura que el 2024 vagi avançant, l'internet de les coses (IdC) continuarà creixent exponencialment, i cada vegada hi haurà un nombre més gran de dispositius interconnectats. No obstant això, aquesta expansió porta associada una sèrie de desafiaments de seguretat. La diversitat i la ubiqüitat dels dispositius IdC fan que siguin objectius atractius per als ciberatacs, i la seva naturalesa interconnectada pot portar a vulnerabilitats generalitzades.

Aquest 2024, un objectiu clau serà millorar la seguretat de l'IdC en diversos àmbits. Cal avançar significativament cap al desenvolupament de protocols de seguretat més robustos i estandarditzats per a dispositius IdC. Això podria incloure estàndards de xifratge universal i certificacions de seguretat obligatòries per als nous dispositius. Un altre àmbit de millora podria ser la integració d'algorismes d'IA i aprenentatge automàtic en els sistemes d'IdC. Aquestes tecnologies poden monitorar patrons inusuals indicatius d'una escletxa, la qual cosa permet respondre de manera més ràpida en cas d'amenaça.

A més a més, és probable que en l'educació dels usuaris es faci més èmfasi en la seguretat de l'IdC. Per tant, a mesura que els usuaris siguin més conscients dels possibles riscos i de les millors pràctiques, la postura general de seguretat de les xarxes d'IdC millorarà. Finalment, podria haver-hi un augment de l'ús de la tecnologia de cadena de blocs (*blockchain*) per descentralitzar i protegir les xarxes d'IdC, cosa que les faria menys vulnerables als atacs dirigits als sistemes centralitzats. En conjunt, aquests avenços suggereixen que el 2024 l'ecosistema de l'IdC serà més segur i resistent.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

7

Prediccions i tendències clau
Ciberseguretat 2024

Bretxa notable en les habilitats de ciberseguretat i educació

ANDORRA DIGITAL

ANC-AD

7

Bretxa notable en les habilitats de ciberseguretat i educació

El 2024, el sector de la ciberseguretat continua lluitant contra un repte significatiu: la bretxa d'habilitats. A mesura que les amenaces cibernètiques es tornen més sofisticades, augmenta la demanda de professionals de ciberseguretat qualificats. No obstant això, hi ha una manca notable de persones amb les habilitats i els coneixements necessaris per combatre eficaçment aquestes amenaces en evolució.

Aquesta bretxa representa un risc no només per a les organitzacions individuals, sinó també per a la infraestructura cibernètica global.

Per abordar aquesta bretxa, és essencial invertir en programes educatius actualitzats, fomentar la formació contínua i promoure la consciència sobre la importància de la ciberseguretat en tots els nivells de la societat. A més, cal que les organitzacions treballin activament per reclutar i retenir talent en ciberseguretat, així com per implementar mesures de seguretat robustes.

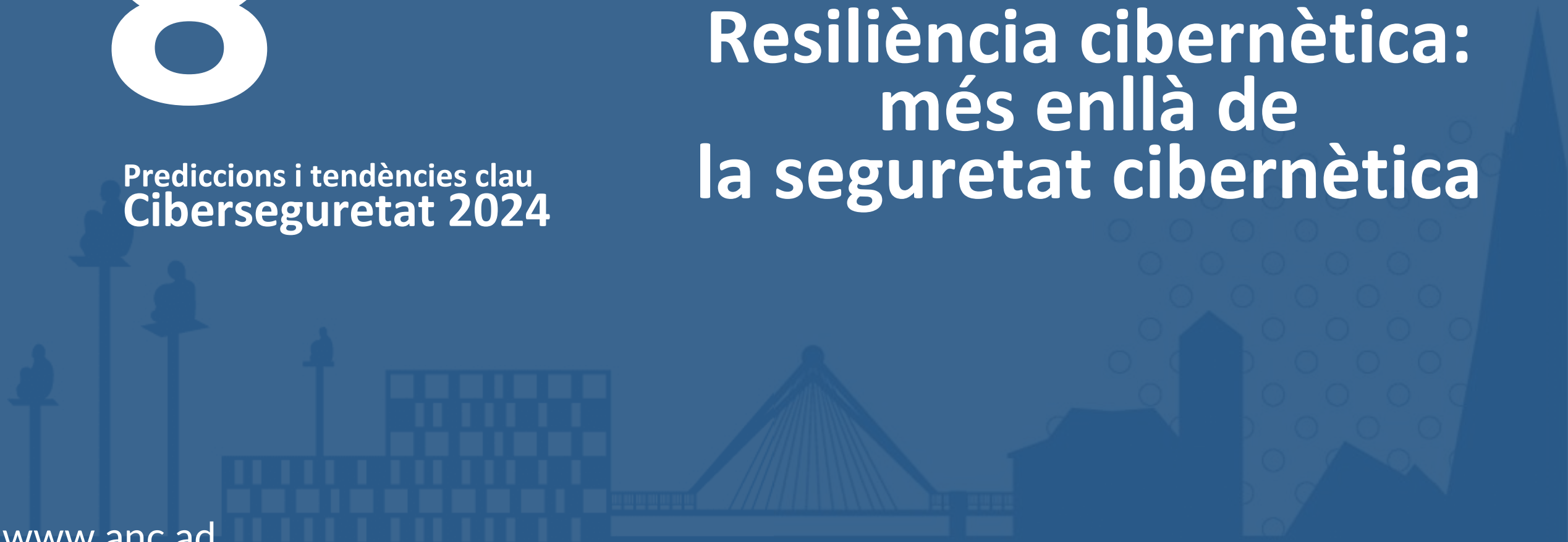
ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

8

Prediccions i tendències clau
Ciberseguretat 2024

Resiliència cibernètica: més enllà de la seguretat cibernètica



www.anc.ad

ANDORRA DIGITAL

8

Resiliència cibernètica: més enllà de la seguretat cibernètica

www.anc.ad

ANC-AD

La resiliència cibernètica es refereix a la capacitat d'una organització per resistir davant d'esdeveniments cibernètics adversos, adaptar-s'hi i recuperar-se'n. En un entorn en constant evolució, en què les amenaces cibernètiques són com més va més sofisticades i persistents, la resiliència cibernètica és fonamental per garantir la continuïtat del negoci i la protecció de la informació delicada. Alguns aspectes clau de la resiliència cibernètica són:

Planificació i preparació:

- Desenvolupament de plans de resposta a incidents: és essencial disposar d'un pla detallat per abordar incidents cibernètics. Això inclou procediments clars, rols i responsabilitats definits, i línies de comunicació establertes.
- Exercicis i simulacres: fer exercicis regulars i simulacres d'incidents ajuda a millorar la preparació de l'equip de seguretat i permet identificar àrees de millora en els processos.

Seguretat proactiva:

- Avaluació de riscos: identificar i avaluar constantment els riscos cibernètics permet a les organitzacions anticipar-se a possibles amenaces i prendre mesures preventives.
- Implementació de mesures de seguretat: adoptar una postura proactiva en relació amb la seguretat implementant mesures com tallafocs, sistemes de detecció d'intrusions, xifratge i autenticació de dos factors.

Detecció i resposta ràpida:

- Monitoratge continuat: implementar sistemes de monitoratge i detecció d'amenaces en temps real per identificar activitats sospitoses i respondre-hi ràpidament.
- Resposta coordinada: disposar d'un equip de resposta a incidents ben entrenat i tenir processos definits per prendre mesures ràpides i coordinades en cas que es produeixi un incident.

Recuperació i continuïtat del negoci:

- Còpies de seguretat i restauració: fer còpies de seguretat periòdiques de les dades crítiques i tenir procediments clars per a la restauració ràpida en cas de pèrdua de dades.
- Plans de continuïtat del negoci: desenvolupar plans detallats per garantir la continuïtat de les operacions en cas d'incident, incloent-hi la capacitat de canviar a sistemes de suport.

Col·laboració i conscienciació:

- Col·laboració amb la comunitat: participar en la comunitat de ciberseguretat, compartir informació sobre amenaces i millors pràctiques, i aprendre de les experiències d'altres organitzacions.
- Conscienciació del personal: educar i conscienciar el personal sobre les pràctiques de seguretat cibernètica, fomentar una cultura de seguretat en tota l'organització.

ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

9

Prediccions i tendències clau
Ciberseguretat 2024

L'auge de les assegurances de ciberriscos

www.anc.ad

ANDORRA DIGITAL

9

L’auge de les assegurances de ciberriscos

www.anc.ad

El 2024 l’assegurança de ciberseguretat esdevindrà un component fonamental de les estratègies de gestió de riscos empresarials. A mesura que les amenaces cibernètiques creixen en complexitat i freqüència, les organitzacions recorren cada vegada més a les assegurances de ciberseguretat per mitigar els riscos financers associats a les violacions de dades i als ciberatacs. No obstant això, el cost d’aquesta assegurança pot variar significativament en funció de la postura de l’organització quant a la ciberseguretat.

L’ús de solucions de ciberseguretat pot tenir un impacte directe en la reducció dels costos de l’assegurança. Les entitats asseguradores sovint avaluen el nivell de risc d’una organització en funció de les mesures de seguretat de què disposa; per tant, tenir bones defenses, pot ajudar a aconseguir primes d’assegurança més favorables.

A més a més, la integració de solucions de ciberseguretat demostra a les asseguradores que una organització és proactiva pel que fa a la seva protecció. Aquesta actitud proactiva sovint és vista de manera positiva per part dels proveïdors d’assegurances, atès que suggereix un perfil de risc més baix. En essència, les organitzacions que inverteixen en solucions de ciberseguretat confiables no només milloren la seva seguretat, sinó que també es posicionen perquè els costos de l’assegurança de ciberseguretat siguin potencialment més baixos, cosa que demostra el seu compromís amb pràctiques sòlides de gestió de riscos.

ANDORRA DIGITAL

Agència Nacional de Ciberseguretat d'Andorra

10

Ciberseguretat al núvol

Prediccions i tendències clau
Ciberseguretat 2024

www.anc.ad

ANDORRA DIGITAL

10

Ciberseguretat al cloud

La seguretat en el núvol és un aspecte crític en el panorama actual de la tecnologia. A més a més, el servei de seguretat en el núvol és cada vegada més important a causa de l'augment de les tendències de mobilitat, el treball remot i la subcontractació. Les empreses cada vegada migren més dades al núvol, per això és molt important disposar d'una estratègia integral de ciberseguretat.

Riscos de la seguretat en el núvol:

- Accés no autoritzat: la gestió d'accessos i l'autenticació dèbil poden donar lloc a accessos no autoritzats.
- Pèrdua de dades: la transferència de dades a través de xarxes no segures o l'emmagatzematge inadequat poden tenir com a resultat que es perdin o es comprometin dades.
- Amenaces internes i externes: tant actors interns com externs poden representar riscos, des de treballadors malintencionats fins a ciberdelinqüents.

Importància del servei de seguretat en el núvol:

- Protecció en capes: les solucions de seguretat en el núvol ofereixen protecció en capes, des de la infraestructura fins a les aplicacions i les dades.
- Monitoratge continuat: el monitoratge constant d'activitats en el núvol és fonamental per identificar possibles amenaces i respondre-hi ràpidament.

Estratègia integral de ciberseguretat:

- Enfocament proactiu: la seguretat en el núvol requereix un enfocament proactiu, incloent-hi l'educació del personal, la implementació de mesures de seguretat des del disseny i l'actualització constant de polítiques.
- Compliment normatiu: cal que les empreses s'assegurin de complir amb les regulacions específiques de la indústria i la regió a l'hora de migrar dades al núvol.

ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Avís Legal