Agència Nacional de Ciberseguretat (ANC-AD)

Govern d'Andorra

ANDORRA DIGITAL

ANC-AD

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

2ª Jornada CISO

Visió estratègica per una cadena de subministrament segura i resilient enfront atacs i amenaces

Xavier Gatius Garriga

1 de Març de 2024

La importància de la cadena de subministrament

Captació i retenció de clients

La cadena de subministrament esdevé un factor d'èxit per a les empreses en la millora de la satisfacció dels seus clients, la seva posició de mercat i el valor per als accionistes.

VALOR

NEGOCI

01 **Millora competitiva**
per al creixement i la expansió del negoci i la millora del marge.

Gestió eficaç i organitzada

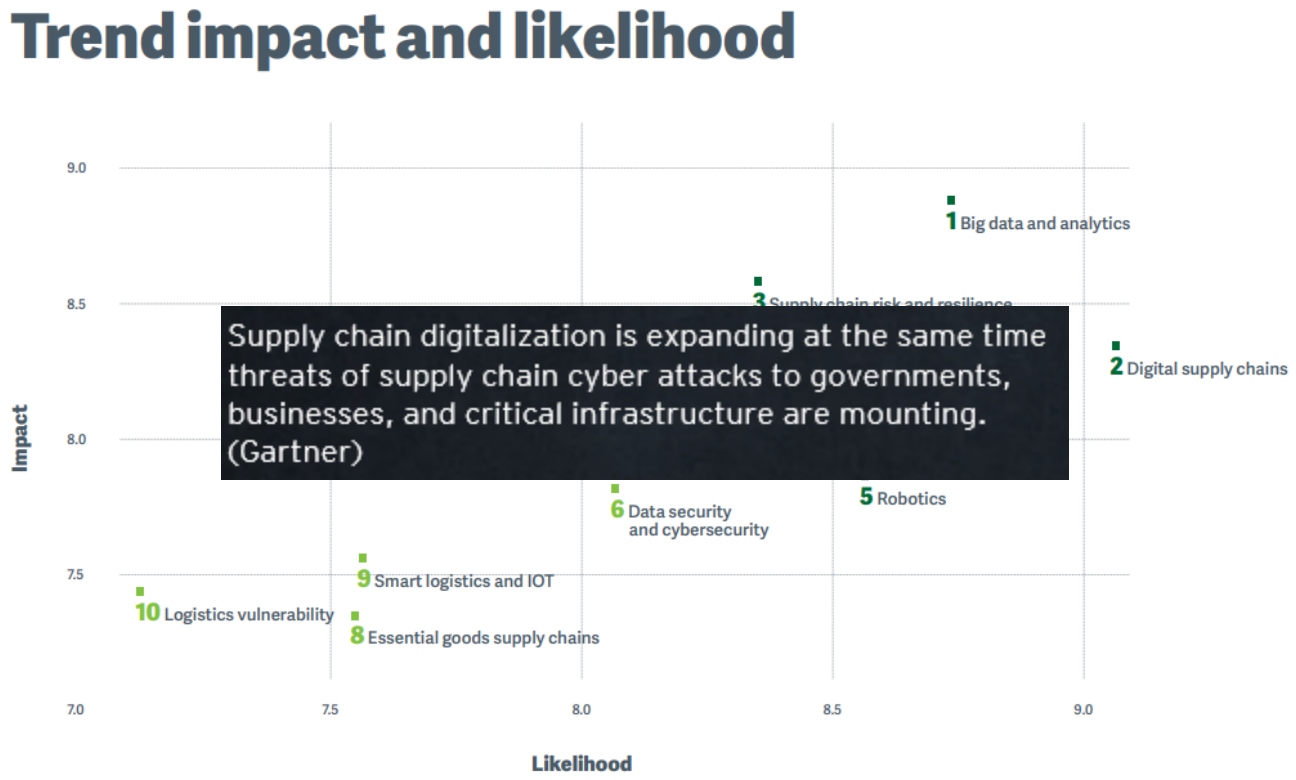
La cadena de subministrament aporta clars beneficis en la gestió proactiva i la mitigació de riscos, el creixement escalable del negoci i la millora de la rendibilitat de les empreses.

02 **Aspecte diferencial**
per a clients, proveïdors i accionistes

Com és preveu la evolució de les cadenes de subministrament?

2023 trend ranking		Change from 2022
1	Big data and analytics	None
2	Digital supply chains	5
3	Supply chain risk and resilience	3
4	Artificial intelligence and machine learning	6
5	Robotics	New in 2023
6	Data security and cybersecurity	2
7	Circular and sustainable supply chains	5
8	Essential goods supply chains	New in 2023
9	Smart logistics and the internet of things	New in 2023
10	Logistics vulnerability	New in 2023

Les cadenes de subministrament s'estan **transformant digitalment** per ser xarxes basades en **data** i incorporar tecnologies emergents que les facin més eficients, competitives i resilients.



Font: Top 10 Supply Chain Trends (Association for Supply Chain Management).

Quina és la percepció dels CISO en relació a les seves estratègies de protecció de la cadena de subministrament?

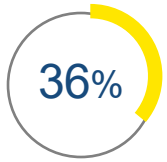
Més de la meitat **(53%)** dels **CISO** i els executius C-Level de les empreses coincideixen que no hi ha un perímetre segur en el ecosistema digital actual.

És a dir, totes les organitzacions estan actualment **vinculades digitalment** a les empreses de la seva cadena de subministrament.

En canvi, pocs **CISOs** i executius estan molt preocupats pels riscos de la cadena de subministrament **(28%)** i riscos relacionats, com ara la protecció de la propietat intel·lectual **(30%)**.

Font: EY 2023 Global Cybersecurity Leadership Insights Study

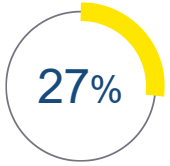
Major impacte dels atacs a la cadena de subministrament



de les organitzacions atribueixen als ciberatacs la sisena causa principal de disrupció.

Font: Business Continuity Institute survey in 2023

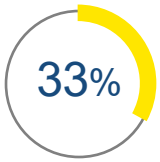
Cal millorar l'operació per mitjà de la automatització i IA



de les empreses minoristes en 2020 han desplegat mesures de seguretat automatitzades i capacitats IA.

Font: IBM

Més necessitat de resiliència en la cadena de subministrament



dels CISO asseguren que tota la cadena de subministrament té capacitats de protecció i recuperació enfront actors i amenaces.

Font: EY Global Information Security Survey 2021

Com afronten els CISO la protecció de la seva cadena de subministrament?

Reptes

Dificultat en **detectar** compromisos de seguretat dels proveïdors en cadenes de subministrament modernes.

Resiliència limitada dels proveïdors en disrupcions de la cadena de subministrament.

Obligacions normatives i legislatives **complexes** amb múltiples canvis en curs.

Amenaces persistents avançades i programari maliciós dirigit a **infraestructures clau** dels proveïdors IT.

Amenaces avançades dirigides a **components** inclosos en productes finals.

Abast addicional en el **creuament** de la cadena de subministrament d'empresa, producte i fabricació.

El **58%** dels atacs a la cadena de subministrament tenien com a objectiu obtenir accés a les dades (dades de clients, personals i IP)

El **62%** dels atacs a clients es van aprofitar de la confiança dels seus proveïdors.

El **47%** de les organitzacions admeten no tenir la capacitat per entendre l'activitat base normal de les seves xarxes.

En el **62%** dels casos, el *malware* va ser la tècnica d'atac utilitzada.

Font: 2022 Report from IBM

Per on podem començar?

Entendre quin és el **grau d'exposició i risc** en la seguretat de la seva cadena de subministrament és fonamental per a dissenyar una estratègia efectiva i resilient enfront atacs i amenaces.

1. Coneixem i entenem les amenaces al voltant de la cadena de subministrament?
2. Coneixem l'abast de l'impacte quan un sistema es veu compromès?
3. Com assegurem que els proveïdors tenen mesures per protegir els seus sistemes i serveis?
4. Com identifiquem ràpidament les ciberamenaces i les vulnerabilitats associades?
5. Quina és la nostre capacitat de resposta enfront incidents de ciberseguretat?

No conèixer de manera adequadament l'exposició de la nostre cadena de subministrament és el pas previ a poder ser compromesos…

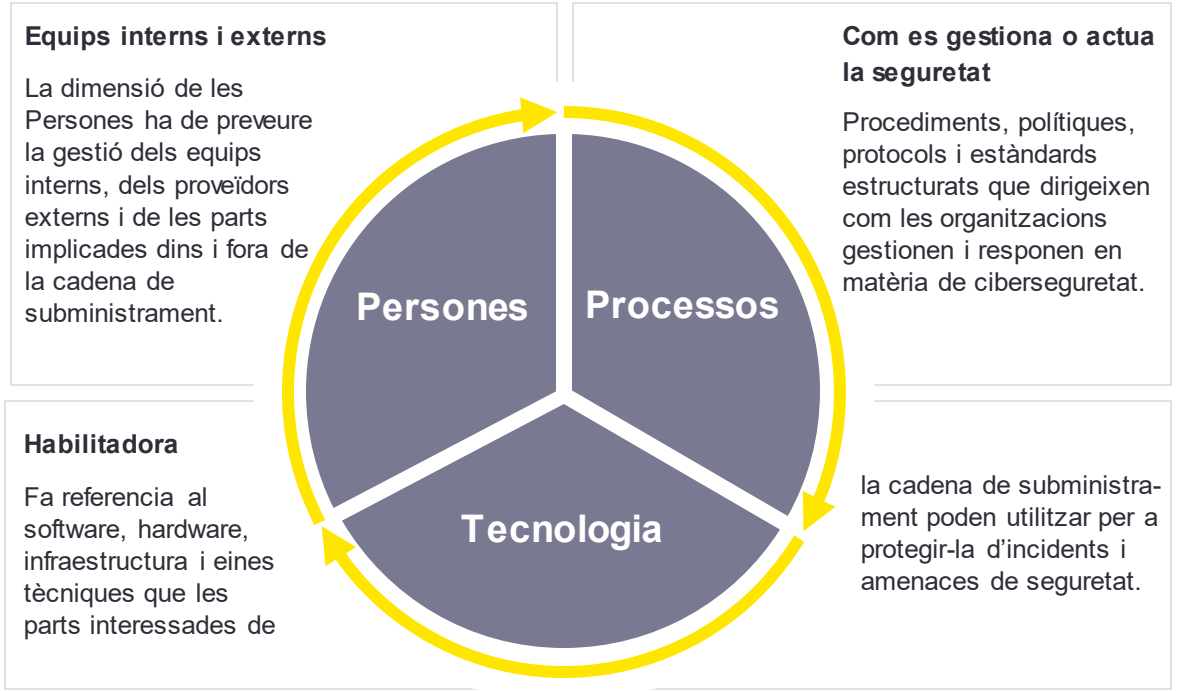
I cal fer-ho de manera continua!

Programa i estratègies de seguretat de la cadena de subministrament

Per implementar estratègies de protecció i resiliència de la cadena de subministrament, cal disposar d'una **visió holística** i establir un programa estructurat que **compti amb la col·laboració** de tota l'organització.

Incorporar exclusivament tecnologia avançada per a la protecció de les operacions no garanteix la seguretat de la **cadena de subministrament funcional**.

El paradigma Persones, Processos i Tecnologia (PPT) permet dissenyar un **programa funcional** de ciberseguretat de la cadena de subministrament i facilita desplegar distintes estratègies de en tota una organització.



Programa funcional de ciberseguretat per a la protecció i resiliència de la cadena de subministrament

En aquesta dimensió la prioritat serà crear un **programa de capacitació**, formar l'equip adequat i crear un **programa de certificació** intern adient.

Programes de formació obligatoris

- Programa de formació en ciberseguretat **específic** per a col·lectius:
  - Personal intern.
  - Proveïdors i parts implicades.
- **Conscienciació** en la protecció de la informació confidencial, la gestió de privilegis, tecnologies IT i OT i enginyeria social.
- Disseny d'**exercicis pràctics** realistes per a facilitar la col·laboració en la resposta a incidents.
- Impulsar una **cultura de la seguretat** a tota la organització.

Certificacions internes

- Programa de **certificació** interna.
- Cal assegurar les **millors pràctiques** de la industria i els estàndards industrials (NIST, ISO, i d'altres).
- Alineat amb els Sistemes de Gestió de Seguretat de la Informació **(SGSI)** de cada organització.

Conclusions clau

- Les persones com l'**actiu més crític** per a qualsevol negoci.
- **Prioritzar** la capacitació i les certificacions adequades per a totes les parts implicades (empleats, proveïdors i socis) en la cadena de subministrament.
- Generar un **ecosistema** de la cadena de subministrament més resilient i segur.

Programa funcional de ciberseguretat per a la protecció i resiliència de la cadena de subministrament

Una definició i execució eficaç dels processos **garanteixen la coherència i el compliment** de les estratègies de protecció i resiliència.

Governança i compliment

- Donar **compliment** i adaptar-se a les polítiques i estàndards específics de la industria i al marc legislatiu vigent.
- Palanca de **millorar la postura** general de la seguretat de la cadena de subministrament.
- Es recomanable disposar de polítiques implementades a punt per a ser utilitzades **en previsió** de riscos o problemàtiques que puguin materialitzar-se.

Resposta a incidents

- Desenvolupar un ***Runbook*** de resposta a incidents per a gestionar eficaçment incidents de ciberseguretat amb l'ajuda de totes les parts implicades.
- Assegurar **estableixi** els RPO i RTO, així com els procediments per a la intervenció de les autoritats.

Gestió del cicle de vida dels actius cyber

- **Avaluació** dels actius prèvia a la posada en marxa, durant el seu servei i en el decomissat.
- Disposar d'una visió clara del **cicle de vida** dels actius ajuda a detectar les seves vulnerabilitats i a protegir-los de manera adequada.

Protecció a amenaces per entorns de fabricació

- Aspecte **fonamental** de la cadena de subministrament.
- Desenvolupar un programa per a avaluar i dur a terme la monitorització de **l'ús de les practiques** de ciberseguretat establertes per als entorns de fabricació interns de les organitzacions.

Programa funcional de ciberseguretat per a la protecció i resiliència de la cadena de subministrament

Les cadenes de subministrament involucren nombroses organitzacions, proveïdors, fabricants, distribuïdors i proveïdors de logística. La gestió eficaç de tercers és clau per garantir que totes les parts involucrades de la cadena de subministrament responguin ràpidament als reptes dels tercers i a incidents de ciberseguretat o disrupcions de servei.

Gestió del Third-Party

Perfils de risc i avaluació continua

- **Bases de dades** de riscos dels tercers, incorporant informació en relació a resposta a incidents i continuïtat de negoci.
- **Avaluació del risc** en proveïdors, *vendors*, i prestadors de serveis cloud.

Protecció d'amenaces en tercers

- Programes per **avaluar l'ús** de les mesures de ciberseguretat i la seva higiene en tercers.
- **Monitoritzar l'eficàcia** de les mesures per a prevenir incidents i protegir la cadena de subministrament.
- Gestió primerenca d'incidents en tercers com a estratègia d'**anticipació** en parts que encara son s'han vist afectades.
- Establir **canals de comunicació** entre totes les parts implicades per a mitigar l'impacte i la millora de la resiliència.

Gestió de vulnerabilitats

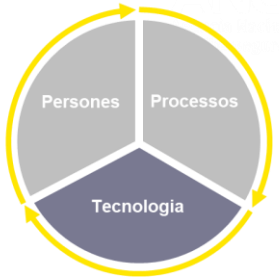
- La gestió de vulnerabilitats permet **identificar**, **avaluar** i **mitigar** riscos de ciberseguretat dins de la cadena de subministrament.
- **Avaluar la seguretat** del software i dels sistemes
- Analitzar proactivament la obsolescència del sistema en coherència a la **postura del risc** i verificar la seguretat de les infraestructures aportades i el software instal·lat pels *vendors*.

Conclusions clau

- Els ciberatacs aprofiten la **manca de gestió** dels actius TI, i una gestió deficient de les seves vulnerabilitats.
- Una gestió adequada dels tercers, contribueixen a **mitigar riscos i a evitar incidents**.
- Les cadenes de subministrament **depenen** en grau mesura de procediments y processos ben definits per a les seves operacions, el que fa la dimensió del Procés tant important com les Persones i la Tecnologia.

Programa funcional de ciberseguretat per a la protecció i resiliència de la cadena de subministrament

La Tecnologia en l'àmbit de la ciberseguretat de la cadena de subministrament es refereix al software, hardware, infraestructura i eines tècniques que els integrants poden utilitzar per a protegir-la enfront amenaces, atacs i incidents de ciberseguretat.



Torre de control segura

- Torre de Control de la cadena de subministrament per obtenir, en temps real, **indicadors i mètriques clau** per a identificar infraccions i incidents.
- Segons *Gartner*, la Torre de Control és un concepte que resulta de **combinar** Persones, Processos, Dades, Organització i Tecnologia.

Redisseny eficaç de l'arquitectura de seguretat

- **Columna vertebral** de la cadena de subministrament.
- Imprescindible **reexaminar** i **redissenyar** l'organització de solucions, infraestructures i dades.
- **Adopció** adequada del concepte *Security By Design*.
- Contribueix a **reduir el cost** operatiu en la implementació de mesures de seguretat poc efectives.

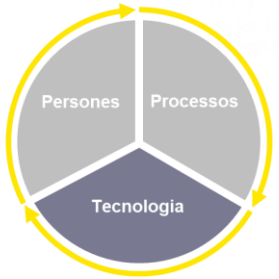
DevSecOps a la cadena de subministrament

- Enfoc **avançat** que combina el desenvolupament, les operacions i la seguretat del software de la cadena de subministrament.
- Pràctica segura **per disseny**.
- Garanteix una **major seguretat** i **eficiència** en tota la cadena de subministrament.

Protecció de les dades operatives

- Les dades són un dels **actius digitals** més importants en una cadena de subministrament.
- Cal implementar tecnologies per a la **protecció** de dades operatives confidencials.
- La governança de les dades, el seu xifrat y la prevenció de la seva pèrdua són **clau**.
- Disposar d'una protecció eficaç de les dades pot evitar possibles **fuites** i divulgació no autoritzada.

Programa funcional de ciberseguretat per a la protecció i resiliència de la cadena de subministrament



Proves de seguretat i seguretat a la xarxa

- Molts dispositius OT i IoT tenen **sistemes integrats** i cal garantir que aquests sistemes siguin segurs.
- És **necessari** la revisió de codi, proves de seguretat estàtica i dinàmica de les aplicacions, proves de sistemes i **garantir** la inexistència de backdoors i vulnerabilitats crítiques.
- **Vetllar** per la seguretat de la xarxa per a un intercanvi segur de les dades entre tots els dispositius i disposar de tecnologia avançada per tenir **visibilitat** en temps real.

Gestió de la identitat i l'accés a recursos (IAM)

- **Garantir** l'accés als recursos autoritzats en cada moment i **evitar** els no autoritzat per part d'usuaris malintencionats o negligents.
- Disminueix les possibilitats de **danys per amenaces** internes i és clau per assolir una major integració de la seguretat contra amenaces internes.
- Implementar **solucions** de gestió d'accés i identitats basades **en rols**, combinat amb l'inici de sessió únic (SSO) i l'autenticació multifactor (MFA).

Serveis Cloud

- Els servei basats en Cloud poden ajudar a **millorar la postura** de la ciberseguretat de la cadena de subministrament.
- Els serveis al núvol ofereixen la capacitat d'**escalar** fàcilment els recursos disponibles, ajuden a reduir costos operatius i errors de configuració que **eviten** el risc d'incidents de seguretat.
- El implicats a la cadena de subministrament també hauran de **garantir les mesures** de seguretat quan s'utilitzin serveis Cloud.

Conclusions clau

- La implementació de tecnologies eficaces poden ajudar a **reduir riscos** de ciberseguretat amb un gran impacte en la cadena de subministrament.
- Cal realitzar de manera diligent **avaluacions** de les tecnologies implementades per tal de determinar el **compliment** dels estàndards i requeriments de seguretat de les organitzacions de la cadena de subministrament.

Un marc normatiu i legislatiu orientat a aquest propòsit...

El Govern d'Andorra ha impulsat i aprovat diverses mesures normatives i legislatives orientades a la protecció adequada de la informació i els serveis prestat per entitats essencials i aquelles que estiguin integrades a les seves respectives cadenes de subministrament.

La cadena de subministrament és un dels criteris a tenir en compte per a valorar la proporcionalitat dels esforços en la gestió dels riscos.

La llei inclou els aspectes de seguretat de la cadena de subministrament relatius a la relacions entre cada organització i els seus proveïdors o prestadors de serveis.

Decret 417/2022, del 12-10-2022, pel qual s'aprova el Reglament de l'Esquema nacional de seguretat del Principat d'Andorra

Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació.

Cal no oblidar també altres normes internacionals, com ara DORA en el cas del Sector Financer

Conclusions i reflexions

1. La protecció i resiliència com a valor competitiu.
2. La transformació digital de la Supply Chain.
3. Entendre i conèixer l'exposició i els riscos.
4. Canvi de paradigma en l'estratègia de seguretat.
5. Generar ecosistemes resilients i segurs.
6. Disposar d'una estratègia amb visió holística.
7. Avaluació continua de la implementació tecnològica.
8. Existència d'un marc legislatiu i normatiu favorable.

MOLTES GRÀCIES

ANDORRA DIGITAL

ANC-AD

@anc_ad

@anc-ad

csirt.anc@govern.ad