# Memòria tècnica – Lot 34

## Serveis de ciberseguretat– Àmbit Metropolità de Barcelona

Acord marc de subministrament d'equips informàtics i de serveis associats amb destinació a les entitats locals de Catalunya

## ÍNDEX



# 1. Objectiu

L'objectiu d'aquest document es la de formalitzar la proposta de serveis, que abasten des de l'anàlisi exhaustiva i disseny de l'estratègia per la millora de la resiliència, fins a la capacitació especialitzada per cobrir les necessitats especifiques de les entitats locals de Catalunya, on en el context actual, juguen un paper vertebral en la vida dels ciutadans, gestionant un volum creixent d'informació sensible i proporcionant serveis essencials.

# 2. Servei d'assessoria

Oferim un servei d'Auditoria i Consultoria Inicial. En el que es realitzarà una auditoria exhaustiva de la infraestructura de l'Entitat Locak, per identificar de manera precisa vulnerabilitats i riscos potencials. A més, es durà a terme una revisió detallada dels controls d'accés, sistemes d'encriptació i bones pràctiques de seguretat de dades, amb l'objectiu primordial de reforçar la postura de seguretat global.

A partir d'aquesta anàlisi, es desenvoluparà un Pla de Millora personalitzat, incloent un full de ruta que guiarà estratègicament a les entitats per tal de que avancin en la seva maduresa en Ciberseguretat, convertint-les

en més segures i resilients, incloent recomanacions clares i accionables tant per a la millora de la infraestructura tecnològica com la millora de processos i polítiques. Identificarem solucions efectives per prevenir i mitigar ciberamenaces, entre altres el ransomware i el phishing. Finalment, s'inclourà un pla d'acció específic per assegurar el compliment de l'Esquema Nacional de Seguretat (ENS), la directiva NIS2 i altres normatives que puguin afectar a la seguretat, garantint així la conformitat legal i la confiança dels ciutadans.

## 2.1 El servei i Metodologia

En la realització del servei d' Auditoria, realitzem una avaluació de deu dominis de control que cobreixen per complet la Gestió de la Seguretat de la Informació:

**Polítiques i compliment normatiu:** Aquest apartat té com a objectiu avaluar si l'Entitat Local disposa del suport i gestió adients per a la seguretat de la informació segons tots els requisits normatius.

**L'organització quant a la seguretat de la informació:** La seva finalitat és valorar el marc de referència seguit per a la implantació i control de la seguretat de la informació dins de l'Entitat Local. Aquest domini, inclou un anàlisis tècnic de la infraestructura actual per identificar vulnerabilitats i riscos potencials.

**Gestió d' actius:** El seu objectiu és analitzar informació sobre l'adequada protecció dels actius de l'entitat.

**Seguretat dels recursos humans:** Te com objectiu principal identificar i avaluar les mesures aplicades per controlar la seguretat de la informació, a la que accedeixen els usuaris de l'Entitat Local.

**Seguretat física i de l'entorn:** S'avalua el nivell de protecció física de les instal·lacions de l'entitat.

**Gestió i seguretat de les comunicacions i operacions:** Amb l' objectiu d'identificar els processos i responsabilitats en les comunicacions i operacions, incloent la encriptació, que porta a terme l'Entitat Local.

**Control d' accessos:** S'analitza el control a l'accés a tots els sistemes d'informació i aplicacions de l'entitat.

**Adquisició, desenvolupament i manteniment dels sistemes de la informació:** Amb l' objectiu d'identificar els processos d'adquisició o desenvolupament de programari, avaluant el compliment de requisits per garantir la seva seguretat.

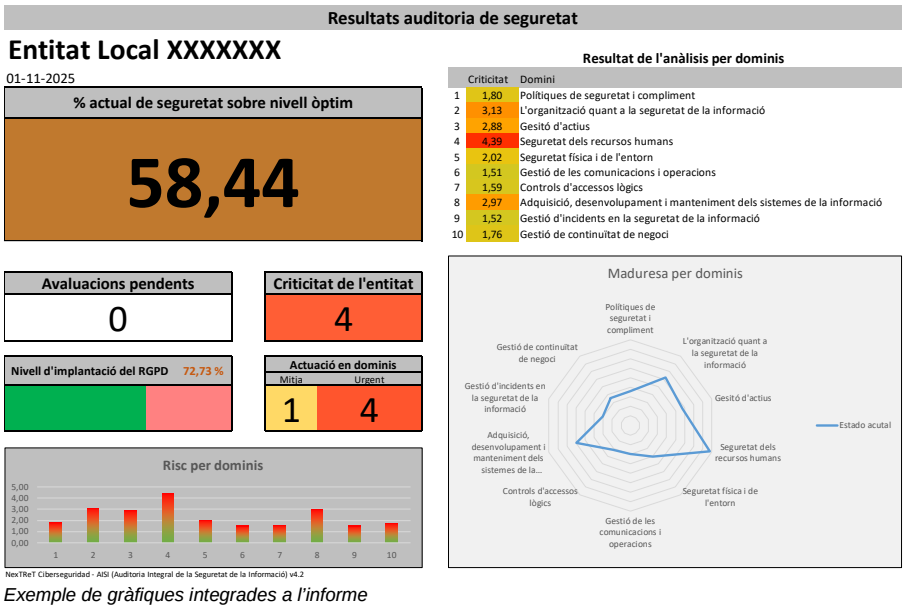
**Gestió d'incidents en la seguretat de la informació:** En aquest punt, s' avalua la gestió d' incidents de seguretat de la informació, incloent tractament, anàlisis i comunicació a parts interessades.

**Gestió de continuïtat de negoci:** L'objectiu és identificar i avaluar les mesures implementades per assegurar la continuïtat operativa dels serveis i sistemes d'informació de l'Entitat Local.

Aquesta auditoria es portarà a terme mitjançant reunions online, formularis tipus enquesta, sessions presencials i accions tècniques d'auditoria sobre la infraestructura, segons les necessitats de cada Entitat.

## 2.2 Resultats

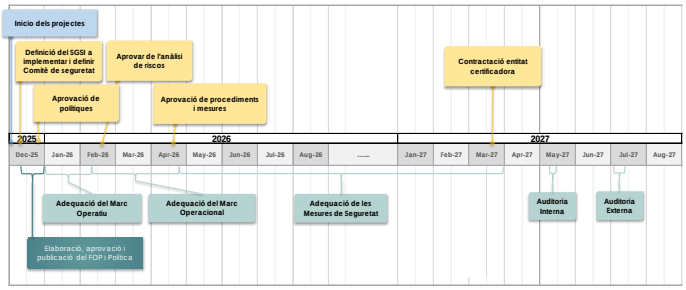
Després de l'avaluació d'aquests dominis, els nostres auditors realitzaran l'anàlisi dels resultats i presentaran un complet i profund informe, que constarà d'una secció amb el resum executiu que inclourà una valoració quantitativa de l'estat general de la seguretat i compliment normatiu de l'Entitat Local; una secció que mostrarà l'estat actual de la seguretat de l'organització i nivell de compliment específic per a cadascun dels dominis de control, amb l'avaluació qualitativa, punts forts i punts de millora; una secció amb una proposta d'accions i fulls de ruta per evolucionar cap a una infraestructura més segura, amb recomanacions tant pel que es refereix a la gestió de la

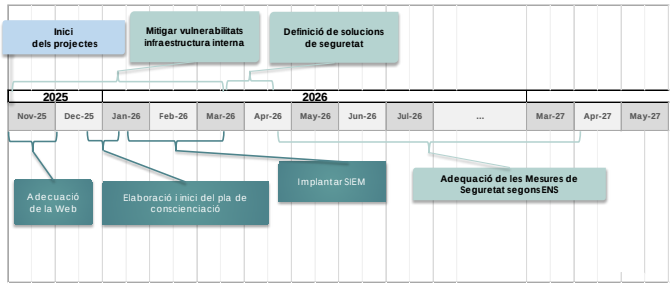



*Exemple de gràfiques integrades a l'informe*

seguretat, el compliment normatiu, millores de maquinari, millores en el programari, solucions especifiques per pervenir els Ciberatacs, en generar i especialment el ransomware i phishing; i per tancar l'informe, una secció amb annexos tècnics que mostraran els resultats i evidències de les proves realitzades.

La secció de l'informe que inclou la proposta d'accions mostrarà dos fulls de ruta un a nivell organitzatiu que mostrarà una proposta d'accions organitzatives a nivell d'Entitat Local, que van enfocades aconseguir un òptim compliment normatiu (RGOD, ENS, NIS2,...) i un altra full de ruta a nivell tècnic, que aborda les tasques tècniques que es recomanen. A continuació es mostren exemples dels gràfics amb la planificació proposada, que acompanyen com a referencia visual, al detall de cadascuna de les accions y projectes recomanats:

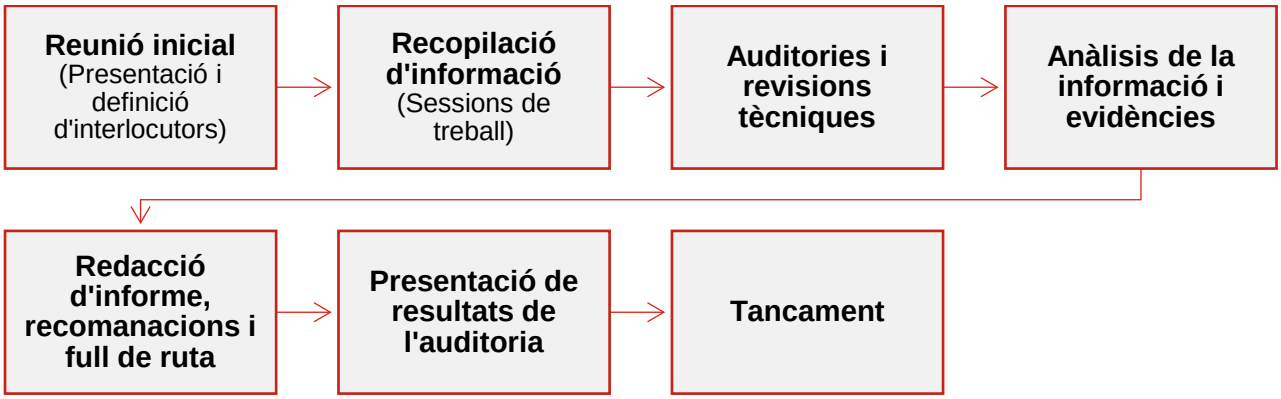



Les Entitats receptores dels plans redactats, podran realitzar consultes relatives a ells, fins a un any després de la contractació del servei.

## 2.3 Planificació

Per tal de portar a terme el servei, la planificació s'estableix seguint les següents fases que comprenen un període d'entre 3 i 4 setmanes, vinculades a la disponibilitat del personal de la pròpia l'Entitat Local:




# 3. Servei de formació en ciberseguretat

Oferim un servei de Formació General en Ciberseguretat: Amb continguts específicament orientats a la identificació i prevenció de riscos digitals, com el phishing, el malware i altres amenaces habituals per al conjunt del personal de les entitats locals. Aquesta formació inclourà aspectes com les bones pràctiques per a la gestió segura de contrasenyes, l'ús responsable d'eines digitals i la protecció de dades, il·lustrat amb explicacions de casos reals per a una major comprensió i conscienciació. Dins d'aquest servei, també oferirem formació especialitzada per a Responsables TIC: Dissenyada per al personal tècnic, aquests cursos específics aprofundeixen en la gestió d'infraestructures segures, la resposta eficaç davant incidents de seguretat i la implementació de mesures de seguretat avançades, i una actualització constant sobre les normatives aplicables, com la LOPD, l'ENS, la NIS2 i altres estàndards rellevants com la ISO 27001.

## 3.1 Metodologia

La metodologia del servei es basa en un enfocament pràctic, interactiu i adaptat a les necessitats específiques de cada Entitat Local. Per la definició de les activitats de formació, es tindrà en compte a nivell general:

- Adaptabilitat: La formació s'adaptarà al nivell tècnic i a les necessitats específiques de cada grup de participants.
- Interactivitat: Es fomentarà la participació activa dels assistents a través de preguntes, debats i exercicis.
- Claredat i Senzillesa: Els conceptes tècnics es presentaran de manera clara i accessible per a tots els nivells. Tenint en compte usuaris amb un nivell bàsic, fins a tècnics IT amb un nivell elevat.
- Aplicabilitat Pràctica: Es posarà èmfasi en la rellevància dels continguts per al treball diari dels empleats municipals.
- Actualització Constant: Els continguts es revisaran i actualitzaran periòdicament per a reflectir les últimes amenaces i normatives.

### 3.1.1 Servei de Formació General en Ciberseguretat

De forma especifica per portar a terme una formació ajustada a les necessitats a un col·lectiu generalista, es posarà focus en realitzar:

- Sessions Interactives: Es prioritzaran sessions dinàmiques amb exemples pràctics, preguntes i respostes, i debats per a fomentar la participació i la comprensió.
- Ús de Casos Reals i Simulacions: Es presentaran casos reals d'atacs i es podran realitzar simulacions senzilles (per exemple, identificació de correus de phishing) per a posar en pràctica els coneixements.
- Material Didàctic Clar i Concís: Es proporcionarà material de suport fàcil de comprendre i consultar posteriorment (infografies, guies ràpides, etc.).
- Avaluació del Coneixement (Opcional segons Entitatl Local): Es podrà incloure una avaluació senzilla (qüestionari, test, ...) per a verificar la comprensió dels conceptes bàsics.

### 3.1.2 Formació Especialitzada per a Responsables TIC

Tenint en compte els coneixements tècnics i requeriments específics dels destinataris de la formació, es posarà focus en realitzar:

- Cursos Teòric i Pràctics: Es combinaran explicacions teòriques amb exercicis pràctics, configuracions en entorns de laboratori (si és possible) i anàlisi de casos tècnics.
- Debats i Intercanvi d'Experiències: Es fomentarà la discussió i l'intercanvi de coneixements entre els participants i el formador.
- Actualització Contínua: Es farà èmfasi en la importància de la formació contínua i es proporcionaran recursos per a mantenir-se actualitzat en un entorn de ciberseguretat en constant evolució.
- Documentació i Recursos Específics: Es lliurarà documentació tècnica detallada i accés a recursos especialitzats.

### 3.1.3 Seguiment i Avaluació del Servei

Segons les necessitats i requisits de l'Entitat Local es podran dur a terme entre altres:

- Recollida de Feedback: Es realitzaran enquestes de satisfacció i es recolliran opinions del personal participant per a avaluar la qualitat de la formació, la claredat dels continguts i la seva aplicabilitat al seu treball diari.
- Avaluació de l'Impacte: A mitjà termini, es podrà avaluar l'impacte de la formació en la reducció d'incidents de seguretat o en la millora de les pràctiques de ciberseguretat a l'Ajuntament (a través d'indicadors preestablerts).
- Informe Final i Recomanacions: Es presentarà un informe final a l'Ajuntament amb els resultats de la formació, el feedback rebut i recomanacions per a futures accions en matèria de ciberseguretat i formació contínua.

### 3.1.4 Material didàctic

Dins de la metodologia prevista per la execució de les formacions es disposarà de:

- Presentacions (Diapositives): Amb llenguatge clar i senzill, incloent resums, icones i esquemes.
- Guies ràpides: Llistes i esquemes concisos, de "què fer" i "què no fer".
- Qüestionaris: Per verificar la compressió de conceptes claus i poder donar feedback als alumes.
- Exemples de correus electrònics: amb simulacions d'atacs de phishing i ransomware.

- Enllaços a recursos externs: A manuals, articles tècnics, guies i infografies de l'Agència Catalana de Ciberseguretat, Centro Criptológico Nacional, INCIBE i altres.
- Documentació sobre normatives: (LOPDGDD, RGPD, ENS, NIS2)

### 3.1.5 Exemples d'Activitats Formatives

#### 3.1.5.1 Activitats per a la Formació General en Ciberseguretat

- **Sessió Introductòria: "Introducció a la Ciberseguretat en el mon Local" (3-4 hores per grup)**
  - **Objectiu:** Sensibilitzar sobre la importància de la ciberseguretat i introduir els conceptes bàsics.
  - **Activitats:**
    - Presentació interactiva amb exemples quotidians i impactants d'atacs.
    - Dinàmica de grup per a identificar els principals riscos en l'entorn laboral.
    - Explicació bàsica de termes clau: phishing, malware, ransomware, enginyeria social.
    - Test ràpid de coneixements inicials (opcional).
- **Taller Pràctic: "Identifica a el Phishing" (2-3 hores per grup)**
  - **Objectiu:** Proporcionar eines pràctiques per a reconèixer correus electrònics, missatges i trucades fraudulentes.
  - **Activitats:**
    - Anàlisi de casos reals de correus de phishing (identificació de senyals d'alerta).
    - Simulació interactiva d'un intent de phishing (per exemple, un correu sospitós).
    - Discussió sobre bones pràctiques per a verificar la legitimitat de les comunicacions.
- **Xerrada: "Protecció de Dades en el Teletreball" (2-3 hores per grup)**
  - **Objectiu:** Conscienciar sobre la importància de la protecció de dades personals i proporcionar pautes per a un tractament segur, tant en entorns presencials com remots.
  - **Activitats:**
    - Explicació dels principis bàsics de la LOPD i el RGPD aplicables als empleats públics.
    - Discussió sobre escenaris comuns de risc en el tractament de dades.
    - Consells pràctics per a protegir la informació sensible (documents, dispositius, etc.).

#### 3.1.5.2 Activitats per a la Formació Especialitzada per a Responsables TIC

- **Taller Avançat: "Resposta a Incidents de Ciberseguretat" (6 hores)**
  - **Objectiu:** Desenvolupar habilitats per a la detecció, anàlisi, contenció, eradicació i recuperació davant incidents de seguretats segons el Esquema Nacional de Seguretat (ENS).
  - **Activitats:**
    - Introducció al ENS i requeriments en la gestió d'incidents
    - Procediments de resposta a incidents i guies CCN-STIC.
    - Simulació d'un incident de seguretat (per exemple, un atac de ransomware) amb assignació de rols.
    - Discussió sobre la comunicació i la gestió post-incident.
- **Seminari: "Implementació i Gestió de Sistemes d'Autenticació Avançada" (4 hores)**
  - **Objectiu:** Aprofundir en les tècniques d'autenticació multifactor, biometria i altres sistemes per a reforçar la seguretat d'accés.
  - **Activitats:**
    - Explicació de les diferents tecnologies d'autenticació.
    - Anàlisi de casos d'implementació en entorns públics.
    - Debat sobre els avantatges i desavantatges de cada sistema.
- **Curs Online: "Normativa de Ciberseguretat per a Entitats Públiques (LOPD, ENS, NIS2)" (8 hores)**
  - **Objectiu:** Proporcionar un coneixement exhaustiu de les normatives de ciberseguretat aplicables als Ajuntaments.
  - **Activitats:**
    - Mòduls dedicats a cada normativa amb explicacions detallades, exemples i casos pràctics.
    - Fòrums de discussió per a resoldre dubtes i compartir interpretacions.
    - Qüestionaris d'avaluació per a cada mòdul.
    - Recursos addicionals (enllaços a la legislació, guies, etc.).

# 4. Model de relació, coordinació i seguiment del projecte

Aquest model es basa en la comunicació oberta, la coordinació integral, una col·laboració proactiva i la definició clara de responsabilitats per garantir l'èxit dels serveis oferts, facilitant la màxima col·laboració entre ambdues parts, permetent que el control del projecte i serveis per part de l'entitat local, convisqui amb la responsabilitat de NexTReT Ciberseguretat per a la consecució dels objectius.

## 4.1 Comitè de seguiment

Aquest comitè és el màxim òrgan de seguiment i supervisió del projecte i servei. Donat el seu caràcter estratègic estarà format per representants de la Direcció del projecte de l'Ajuntament de Sitges i el Responsable del projecte de NexTReT Ciberseguretat. Aquest comitè ha de definir les línies estratègiques del servei, vetllar pel seu compliment així com per la seva qualitat.

| | |
|---|---|
| **Comitè de seguiment** | •Responsables o representants de l'Entitat Local<br>•Responsable del projecte de NexTReT Ciberseguretat<br>•De forma puntual, altres persones que es puguin considerar necessaries segons l'evolució del projecte |

Per part de l'Entitat Local: Es designarà un Responsable del Projecte que serà el punt de contacte principal per a totes les qüestions relatives al servei. Aquesta persona tindrà la capacitat de prendre decisions i facilitar la coordinació interna dins de l'entitat.

Per part del Proveïdor del Servei de Formació: Es designarà un Gestor del Servei que serà el responsable de la planificació, execució i seguiment del servei, així com el principal interlocutor amb el Responsable del Projecte de l'entitat local.

Les funcions definides per aquest comitè són:

- Gestionar i coordinació del projecte.
- Elaboració i validació de les propostes estratègiques que afectin el projecte i el servei.
- Definir i revisar estratègies d'execució, fites, calendari, els canals de comunicació i metodologia de monitorització del servei.
- Supervisió del compliment dels Acords de nivells de serveis establerts, assegurant el compliment d' objectius i obligacions.
- Aprovació i revisió dels programes de treball i procediments d' actuació.
- Realitzar reunions periòdiques per revisar el progrés i evolució, abordar dubtes o problemes, i planificar les següents etapes

### 4.1.1 Reunions de Coordinació del Comitè de Seguiment

**Reunió inicial (Kick-off):** Abans de l'inici del servei, es realitzarà una reunió per establir els objectius detallats, el cronograma, els canals de comunicació, les responsabilitats de cada part i el procediment de gestió d'incidències.

**Reunions de seguiment periòdiques**: Es realitzaran reunions periòdiques del Comitè de Seguiment (a definir, segons la durada i intensitat del servei) per revisar el progrés, abordar possibles dubtes o problemes, i planificar les següents etapes.

**Reunió de tancament**: Un cop finalitzat el servei, es realitzarà una reunió de tancament formal, per avaluar els resultats, recollir feedback, identificar possibles àrees de millora i realitzar el traspàs d'informació i coneixement que sigui necessari.

## 4.2 Equip tècnic

L'equip tècnic que prestarà el serveis associats a aquests projectes està format per:

- Consultors en Ciberseguretat: Amb amplia experiència en serveis de Ciberseguretat i formació o certificacions d'alt valor (Màster en Ciberseguretat, CISSP, ISO 27001 Lead Auditor o similars)
- Consultors en compliment normatiu: Amb amplia experiència en implantació i realització de formacions en normatives relacionades amb la Ciberseguretat (RGPD, ISO 27001, ENS, GxP, DORA, etc..)
- Tècnics especialistes: Amb amplia experiència en serveis d'auditories de seguretat i formació o certificacions d'alt valor (OSCP, CEH, Altres)

## 4.3 Canals de Comunicació Generals:

L'Entitat Local definirà els interlocutors autoritzats per realitzar consultes a NexTReT. Aquests interlocutors disposaran d'accés a les següents eines per a la tramitació de consultes, assessorament i incidències:

- **Telèfon**: 932 541 530 (Ciberseguretat extensió 5005)
- **Correu**: Correu electrònic del responsable del projecte, consultors o tècnics.
- **Ticketing**: Url assignada al client (si escau)

## 4.4 Canals de Comunicació Específics per a la Gestió d'Incidències:

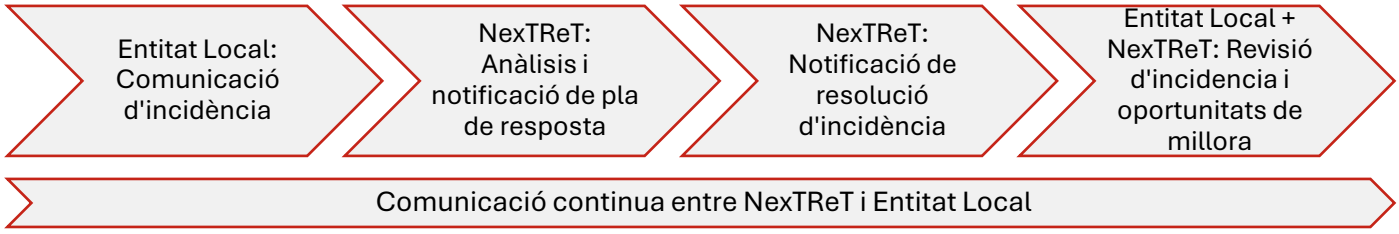
Independentment dels canals de comunicació generals que s'han establert i la monitorització contínua que el servei pugui incloure per detectar problemes tècnics, es defineixen els següents canals específics per a la comunicació d'incidències que puguin sorgir durant la prestació del servei:

- **Adreça de correu electrònic dedicada**: Es crearà una adreça de correu electrònic específica per a la comunicació d'incidències. Aquesta adreça serà monitoritzada de forma prioritària pel Gestor del Servei i/o l'equip de suport designat.
- **Telèfon de contacte directe**: Es posarà a disposició de l'Entitat Local un número de telèfon de contacte directe amb el responsable del projecte o responsable del servei, per tal de poder comunicar de forma immediata qualsevol incidència que pugui succeir.

## 4.5 Procediment de Comunicació d'Incidències

L'entitat local, a través del seu Responsable del Projecte o personal designat, comunicarà la incidència a un dels canals de comunicació específics establerts, proporcionant la màxima informació possible:

- Assumpte concís: Descrivint la naturalesa de la incidència.
- Descripció detallada de la incidència: Explicant què ha passat, quan, on i com afecta al servei.
- Identificació de les persones o grups afectats (si escau).
- Nivell d'urgència percebut (alt, mitjà, baix).
- Qualsevol documentació adjunta rellevant (captures de pantalla, missatges d'error, etc.).




NexTReT mantindrà un registre de totes les incidències comunicades, les accions preses per a la seva resolució i els temps de resposta. Aquesta informació podrà ser compartida amb l'entitat local periòdicament o sota demanda.

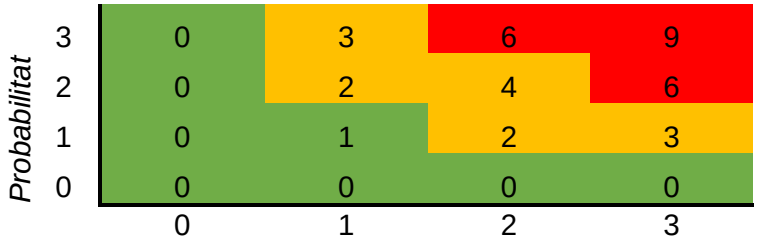
### 4.6 Anàlisi de riscos del projecte

El propi desenvolupament d' un projecte pot experimentar canvis, créixer en complexitat a mesura que s' afegeixen nous requisits, patir incidències i esdeveniments que poden causar efectes negatius sobre els seus objectius. Per tal de garantir la disponibilitat i seguretat dels serveis a prestar, es realitza la següent valoració de riscos i es defineixen les mesures correctores o mitigadores a aplicar.

**Taula de valoració de riscos**

Per a l' anàlisi de riscos s' ha establert la següent taula de valoració de la severitat tenint en compte la probabilitat i impacte.

**Càlcul de la Severitat**




*Impacte:*

| | | |
|---|---|---|
| | Sense impacte rellevant | Requereix tenir prevista la mitigació |
| | Impacte mitjà | Requereix tenir prevista la detecció i mitigació |
| | Impacte alt | Requereix tenir prevista la detecció i mitigació urgents |

**Prob:** Probabilitat que s' esdevingui l' incident
**Imp:** Gravetat de l' impacte
**Sev:** Severitat del risc (Prob x Imp)
**Propiet:** Propietari del risc

### 4.6.1 Valoració dels riscos

Com a primer punt del projecte i després d' establir l'abast, les necessitats tècniques, arquitectura i integració, s'han identificat els riscos intrínsecs al projecte, s'han valorat i han quedat definits en la taula següent:

| Risc | Descripció | Prob | Imp | Sev | Propiet | Disparador |
|---|---|---|---|---|---|---|
| De disseny | Que el disseny del projecte no s'ajusti amb l'entorn real existent | 1 | 2 | 2 | Entitat Local | Quan l' entorn real no correspongui amb el previst |
| De comunicació | Que no existeixi una comunicació fluida entre les parts | 1 | 2 | 2 | Entitat Local i NexTReT | Quan una part detecti una falta o deteriorament de la comunicació |
| Sobre l' abast | Que l'abast del projecte s'hagi d'alterar per la modificació dels requeriments | 1 | 1 | 1 | Entitat Local | Quan el client requereixi una modificació de l'abast o una part detecti la necessitat |
| Recursos | Que el projecte o terminis d'execució puguin veure's compromesos per incidències en els recursos (malaltia, baixes, ...) | 2 | 2 | 4 | NexTReT | Quan un recurs estratègic no estigui disponible per un període destacable |
| | Que una pandèmia, manifestació o situació especial afecti la mobilitat dels recursos | 1 | 1 | 1 | Entitat Local i NexTReT | Quan s' estableixin limitacions a la lliure circulació |
| De planificació | Que una de les fases del projecte no compleixi la planificació establerta | 2 | 2 | 4 | NexTReT | Quan una fase supera en un 10% el temps establert |
| | Que la planificació entri en col·lisió temporal amb intervencions extraordinàries o excessos de treballa del departament IT de l'Entitat Local | 2 | 1 | 2 | Entitat Local | Quan l'Entitat Local de forma extraordinària i temporal tingui un impediment per l'evolució del projecte |

| Risc | Descripció | Prob | Imp | Sev | Propiet | Disparador |
|---|---|---|---|---|---|---|
| | Que no sigui possible realitzar una reunió de seguiment | 3 | 1 | 3 | Entitat Local i NexTReT | Quan alguna de les parts no pugui ser present a la reunió |
| Seguretat | Quan es detecti una deficiència tècnica o humana que pugui afectar la seguretat | 2 | 1 | 2 | Entitat Local i NexTReT | Quan s'identifiqui la deficiència |
| | Quan s'esdevingui un possible incident de seguretat | 1 | 3 | 3 | Entitat Local i NexTReT | Quan es detecti l'incident |
| | Quan s'esdevingués una possible infracció del RGPD | 1 | 3 | 3 | Entitat Local i NexTReT | Quan es detecti el possible incompliment |
| Tècnics | Quan una de les solucions o la infraestructura existent ofereixi problemes de compatibilitat | 2 | 1 | 2 | Entitat Local | Quan es detecti una incompatibilitat |
| | Que es produeixin esdeveniments que afectin de forma important la disponibilitat de la infraestructura o actius | 1 | 3 | 3 | Entitat Local | Quan es detecti la falta de disponibilitat |

### 4.6.2 Mitigació de riscos

| Risc | Descripció | Sev | Mitigació | Acció |
|---|---|---|---|---|
| De disseny | Que el disseny del projecte no s'ajusti amb l'entorn real existent | 2 | Reunions inicials i de seguiment amb l'objectiu de definir els requeriments i encaix amb l'entorn actual | Comunicar-ho a l'equip perquè sigui analitzat en la següent reunió de seguiment |
| De comunicació | Que no existeixi una comunicació fluida entre les parts | 2 | S' estableixen fils de comunicació comuns i reunions periòdiques de seguiment i coordinació. | Comunicar-ho en la següent reunió de seguiment per avaluar els canals i millorar aquesta comunicació |
| Sobre l' abast | Que l'abast del projecte s'hagi d'alterar per la modificació dels requeriments | 1 | Es realitzarà una reunió extraordinària per identificar els requeriments, així com l'impacte sobre el projecte. | La que es determini en la reunió extraordinària. |
| Recursos | Que el projecte o terminis d'execució puguin veure's compromesos per incidències en els recursos (malaltia, baixes, ...) | 4 | La majoria dels recursos estratègics del projecte es troben duplicats, fins i tot alguns d'ells poden cobrir diferents rols dins del projecte, de manera que sempre hi ha un Backup per a cada perfil. | Comunicar-ho en la següent reunió de seguiment i indicar qui és la persona que substitueix el recurs indisponible. |
| | Que una pandèmia, manifestació o situació especial afecti la mobilitat dels recursos | 1 | S'avaluarà la possibilitat de fer accions 100% en remot o l'aplicació d'altres mesures per mitigar el possible impacte. | Es comunicarà a totes les parts la limitació existent i es comunicaran les mesures acordades. |

| Risc | Descripció | Sev | Mitigació | Acció |
|---|---|---|---|---|
| De planificació | Que una de les fases del projecte no compleixi la planificació establerta | 4 | Es dissenyen les fases de forma que puguin executar-se de forma solapada amb fins a un 15% de marge. | Iniciar de forma paral·lela la següent fase o establir accions compensatòries, per realinear el projecte. |
| | Que la planificació entri en col·lisió temporal amb intervencions extraordinàries o excessos de treballa del departament IT de l'Entitat Local | 2 | Establir tasques alternatives que no requereixin l'equip IT de l'Entitat Local o modificar la planificació per tal d'adaptar-la a la seva disponibilitat. | Comunicar les accions a realitzar als equips de treball. |
| | Que no sigui possible realitzar una reunió de seguiment | 3 | Es necessari que en totes les reunions de seguiment hi siguin presents totes les parts | S'establirà una nova data de reunió en el menor període possible |
| Seguretat | Quan es detecti una deficiència tècnica o humana que pugui afectar la seguretat | 2 | Adequació prèvia de NexTReT i Certificació en l'Esquema Nacional de Seguretat en la seva Categoria Alta | Comunicació immediata al responsable de seguretat de NexTReT per procedir a aplicar mesures mitigadores. |
| | Quan s'esdevingui un possible incident de seguretat | 3 | Adequació prèvia de NexTReT i Certificació en l'Esquema Nacional de Seguretat en la seva Categoria Alta | Comunicació immediata a NexTReT i a l'Entitat Local. Activar procediments establerts en l'ENS |
| | Quan s'esdevingués una possible infracció del RGPD | 3 | Adequació prèvia de NexTReT i Certificació en l'Esquema Nacional de Seguretat en la seva Categoria Alta | Comunicació immediata a NexTReT i a l'Entitat Local. Activar procediments establerts en l'ENS |
| Tècnics | Quan una de les solucions o la infraestructura existent ofereixi problemes de compatibilitat | 2 | S'analitzarà l'afectació i possibles solucions. | Comunicar-ho en la següent reunió de seguiment per definir la solució. |
| | Que es produeixin esdeveniments que afectin de forma important la disponibilitat de la infraestructura o actius | 3 | Cercar solució a la no disponibilitat | Comunicar-ho de forma immediata a l'Entitat Local |

78076751P ALBERT DOMINGO (R: B88090816)

Firmado digitalmente por 78076751P ALBERT DOMINGO (R: B88090816)
Nombre de reconocimiento (DN): 2.5.4.13=Ref:AEAT/AEAT0438/PUESTO 1/40750/08072024111622, serialNumber=IDCES-78076751P, givenName=ALBERT, sn=DOMINGO MELGOSA, cn=78076751P ALBERT DOMINGO (R: B88090816), 2.5.4.97=VATES-B88090816, o=NEXTRET CIBERSEGURIDAD SL, c=ES
Fecha: 2025.05.29 11:05:59 +02'00'