MEMÒRIA RELATIVA AL CRITERIS SUBJECTES A UN JUDICI DE VALOR.

SERVEIS DE CIBERSEGURETAT . EXP 2024.01

David Garriga
Administrador Solidari

2025.05.29 12:04:55 +02'00'

ÍNDEX

Resum executiu

SISTEMES INTEGRALS DE XARXES I TELECOMUNICACIONS, S.L., d'ara endavant SIRT, és una enginyeria i empresa tecnològica amb una alta capacitat per identificar i oferir solucions innovadores perquè els nostres clients puguin assolir els seus objectius i metes. Portem des de 1998, més de 25 anys, donant **servei en Tecnologies de la Informació, Comunicacions i Seguretat de la Informació** en una àmplia diversitat d'empreses i organismes oficials.

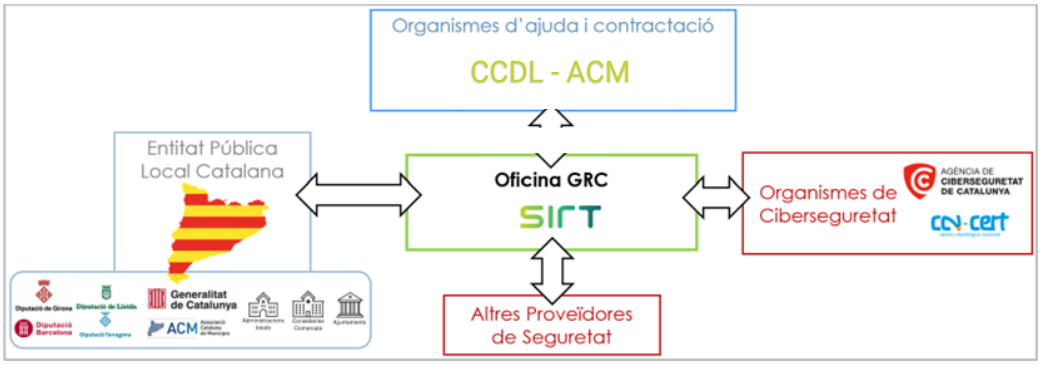
L'experiència que hem adquirit ens han posicionat dins del mercat, com una de les millors empreses de serveis a l'hora de buscar **solucions tecnològiques,** i molt especialment per acompanyar als nostres clients en la **millora de la seva postura de ciberseguretat**. Especialment experiència en l'entorn de l'administració pública catalana, i especialment en els ens locals, gràcies a un dels projecte emblemàtics de SIRT, com es el Catalunya SOC.

La nostra metodologia pròpia es basa en una evolució del framework *GRC Capability Model 3.0* de l'*OECG*, particularitzada amb *Learn – Align – Perform – Review,* que a través de la nostra experiència i evolució ens permet absorbir gran volum de serveis, alhora que es mantenen nivells de qualitat i adaptabilitat, per les diferents entitats associades aquest Acord marc.

Un altre aspecte que garanteix, la nostra expertesa es el grau de certificació, a nivell tècnic i empresa:

1. Model de relació

L'exercici dels serveis proposats, requerirà de **coordinació i participació** per part de SIRT, i varis departaments, tan de l'Ens (IT, RRHH, Legal, ...) com potencialment de tercers actors com pot ser la CCDL, l'ACM, l'Agència de Ciberseguretat, proveïdors externs de l'ens o agents reguladors.



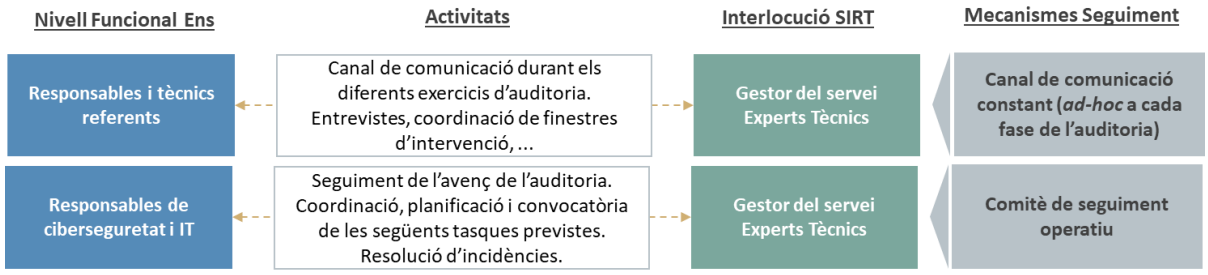
El model de relació proposat, es basa amb l'establiment de l'oficina GRC (govern, risc, i compliment), que establirà els mecanismes i canals formals de comunicació entre les parts, així com els processos necessaris per assegurar un alineament entre les expectatives del ens, i la proposta de serveis de SIRT.

Tot i que el tipus de tarificació del servei, pugui semblar que es tendeix a una servei de poc valor, (preu/hora), el fet de incorporar l'oficina GRC, reforça el valor afegit i l'aposta de SIRT.

1.1. Model de seguiment

Mitjançant l'oficina GRC, es proposa un model de relació flexible i escalable, alineat amb el model de govern del ens local, així com amb la resta d'entitats que puguin intervenir. **Destaquem:**

- **Supervisió i seguiment continuo** per part del coordinador assignat de l'oficina CRG, punt únic de contacte, vetlla per el compliment de tasques, estableix prioritats, interlocució a tercers.
- **Comitès de Seguiment tècnics**. Establerts com a base de seguiment, fòrums de validació, donant pro activitat per anticipar-se a necessitats i establint propostes de millora.
- C**omitè de Seguiment operatiu**, planificat de forma recurrent (preferiblement setmanal), que permeti fer seguiment del grau d'avanç, l'orientació a objectius estratègics i planificació de següents tasques, identificant-ne els actors rellevants a participar per totes les parts.



Des de l'oficina GRC, s'establiran **Eines de comunicació** directa i permanent, sistema de ticketing per augmentar la traçabilitat dels serveis, SLA adequats a ENS en categoria alta amb temps de resposta en funció de l'esdeveniment i personal amb àmplia experiència en diversos sectors. D'aquesta manera ens **assegurem mantenir la qualitat i garantir** un bon mecanisme de coordinació i monitorització de les activitats relaciones amb el servei de auditoria i formació en ciberseguretat.

En el context de la governança del servei, el seguiment de l'auditoria de Seguretat es mantindrà un enfoc pràctic. Al marge de que de forma natural existirà una **dinàmica de comunicació constant** tant en els anàlisi basats en controls (en els que les dinàmiques basades en entrevistes i reunions ja estabiran un marc de comunicació), com també l'anàlisi de camp (*pentest*), on s'establiran **canals segurs de comunicació constant**, de forma que es puguin planificar finestres d'intervenció, rebre feedback i resoldre dubtes.

1.2. Gestió de la demanada

SIRT incorpora dintre de **l'oficina CRG**, un model madur de gestió de la demanda. Aquest model basat en metodologia ITIL, i alineat amb els estàndards ISO20000 e ISO27000, permet tenir una planificació i dedicació constant dels recursos assignat, així com les capacitacions dels mateixos, en els diferents serveis proposats

- Identificació de la demanada. Planificar possibles necessitats futures o emergents, i preparar els requisits tècnics necessaris per cobrir-les
- Gestió dinàmica de la demanada. Establir mecanismes de priorització en cas d'assoliment de noves tasques o evolutius, no previstos. Sempre alineats amb l'ens contractant.
- Desbordament. En cas necessari, SIRT posa a disposició del servei una estructura de **personal tècnic, multidisciplinari** (suport multi client, Arquitectes N3), especialistes en altres línies d'especialització de SIRT (xarxes i comunicacions, sistemes, entorn cloud)

Referent a la capacitació, disposem de mecanismes per desenvolupar-los i enfortir-los:

- Elaboració d'una **matriu de capacitats**, on s'identifica el coneixement clau que ha de tenir cada persona involucrada en el servei, així com les seves fortaleses i mancances. Aquesta matriu s'ha d'anar actualitzant amb els reptes que plantegi el servei.
- Traspàs de coneixement i documentació actualitzada, per el bon funcionament futur del servei, amb el fi de no condemnar el servei al personal inscrit.
- Formació. Actualització continua dels plans de formació i reforç, per tal d'aconseguir una eficiència i evolució continua del servei.

1.3. Equip de treball

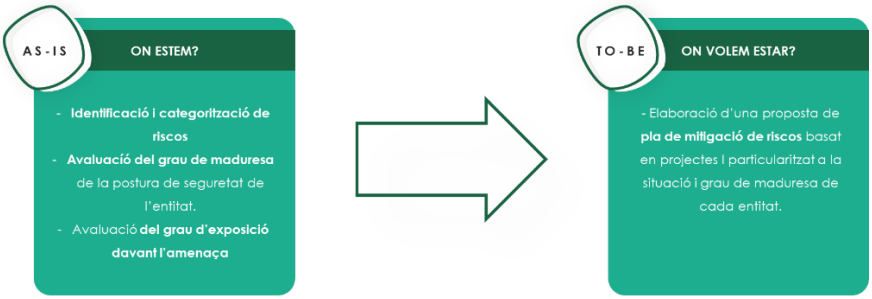
SIRT compta amb recursos humans i assignarà i dimensionarà el servei de cada una de les prestacions, en funció dels objectius i àmbit, amb l'objectiu de reduir els temps de resposta i aportar valor afegit a l'ens contractant. Una mostra de capacitació de l'equip tècnic

Addicionalment, SIRT posa a disposició **perfils específics del departament de *CiberGRC*** com a certificats en DPD o Lead Auditors 27001 així com perfils tècnics **especialistes en Solucions i Serveis de Ciberseguretat del SOC de SIRT** per a una adaptació i ràpida reacció en cas de necessitat. Aquests recursos s' activaran d' acord amb l' ens contractant a mode de desbordament.

L'experiència de SIRT, tant en serveis gestionats de SOC on posseïm **certificat OR de la RNS del CCN-CERT** i som membres del **First**, com en matèria de ciberseguretat, milloren els processos i adeqüen la tecnologia en base als objectius de les auditories.

2. Servei d'assessoria

La postura de ciberseguretat de qualsevol organització, és un procés continu i dinàmic, esdevé necessari partir d'un anàlisi de situació (**As-Is**), prèviament a la definició d'un estat desitjat (**To-Be**). Aquest plantejament permetrà avaluar el **grau d'exposició l'amenaces** de l'entitat, així com **identificar els principals riscos i àrees de millora,** i arribar als estats desitjats de forma més eficient. Establint-se com a fonament d'una modelització i exercici de Govern de ciberseguretat òptim.

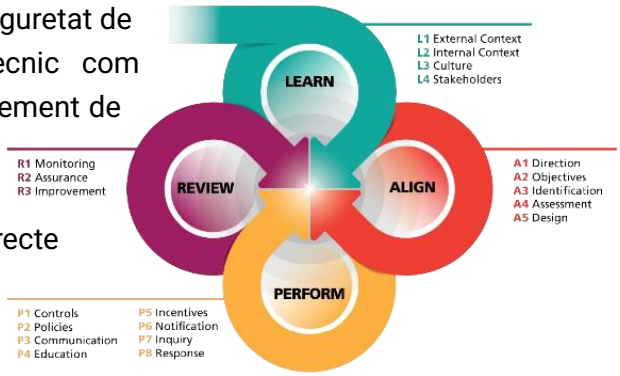


Tenint en compte que tots els potencials destinataris de l'assessoria són organismes adherits al Consorci Català pel Desenvolupament Local (CCDL), pertanyents a l'administració local, l'avaluació del grau d'exposició es realitzarà envers a les principals amenaces identificades des de fonts de ciberintel·ligència i principals incidències al vertical d'administració i govern local.

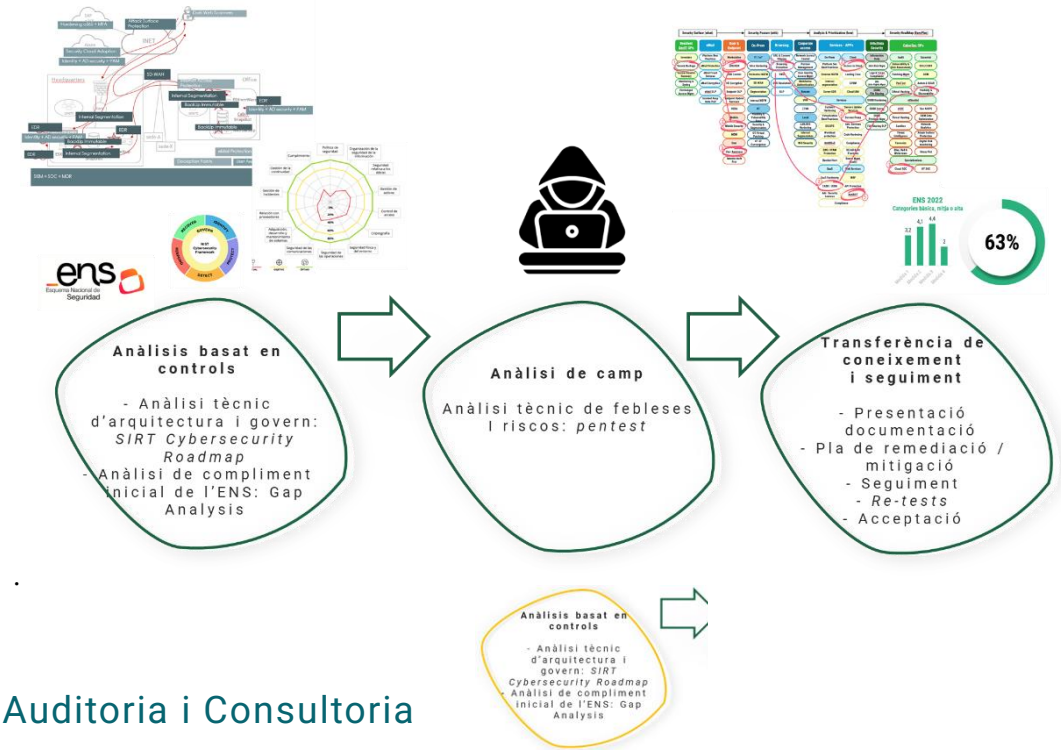
D'aquesta forma, s'obté una **metodologia escalable, sistemàtica i particularitzada** que permet absorbir gran volum de serveis alhora que es mantenen nivells de qualitat i comparabilitat entre els ens, i ens generar coneixement agregat.

2.1. Metodologia

SIRT disposa d'una metodologia (basada en el framework *GRC Capability Model 3.0* de l'*OECG,* particularitzant la metodologia proposada de ***Learn – Align – Perform - Review***), que permet obtenir una visió del grau de maduresa de la postura de ciberseguretat de l'organització 360º, fruit d'un anàlisi intern, tan tècnic com organitzacional/negoci; com extern, amb un fort coneixement de context de les tendències en ciberseguretat, per cadascun del sectors a avaluar (en particular l'Administració local Catalana). Això garanteix el correcte funcionament del servei d'assessoria, així com l'alineament amb els objectius estratègics de cada ens.



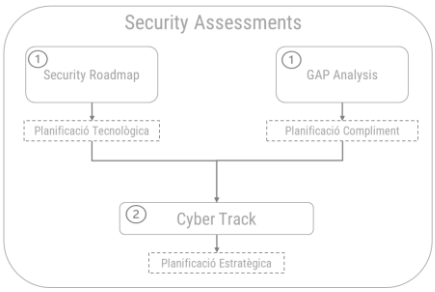
Seguint l'enfoc i visió metodològica expressada, s'estableixen les següents **fases** que agrupen els diferents procediments d'anàlisi emprats per a l'execució de l'auditoria. I en la última fase, s'estableix, entre altre coses, el pla de projectes que ha de permetre mitigar el riscos detectats, així com un pla de remediació, on es defineixen procediment d'actuació davant de desastres.



2.2. Auditoria i Consultoria

L'objectiu es recopilació de la màxima informació i evidències possibles de l'ens. *SIRT Security Assessment* ho materialitza, avaluem dos pilars clau: **Tecnologia** i **Regulació/Compliment** sobre seguretat de la informació mitjançant un **Roadmap** tecnològic i el **Gap Analysis**; per finalitzar es consolida la informació, amb la creació del **CiberTrack**

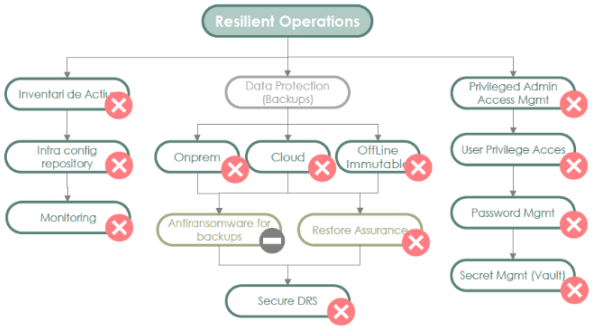
Pilar 1: Security Roadmap Tecnològic



L'objectiu és avaluar el **grau de maduresa tecnològica en ciberseguretat** de l'ens, prioritzant millores alineades amb els seus riscos i necessitats, en format de **full de ruta** d'adopció tecnològica. L'auditoria tecnològica inclouria:

- Revisió (si existeix) del **Pla de Seguretat**.
- **Entrevistes amb responsables**: Reunions amb els equips de TI, seguretat i negoci del client per entendre la seva infraestructura, processos i prioritats operatives.
- **Verificacions i evidències**: llistat estructurat de troballes en base als controls establerts.
- Classificació dels actius seguint els principis de confidencialitat, integritat i disponibilitat.
- Recopilació de documentació tècnica existent.
- **Estudi i definició d'estratègia**: Anàlisi des del punt de vista de vectors d'atac i què protegim (serveis, usuaris, infraestructura...) i avaluació de maduresa davant d'un estàndard mínim de seguretat global adaptat a l'ens.
- **Recomanacions amb prioritzacions, dependències i sinèrgies**.
    a. **Curt termini** – per exemple: pegats urgents, controls bàsics.
    b. **Mig termini** – per exemple: SIEM, Zero Trust, serveis d'operació i resposta...

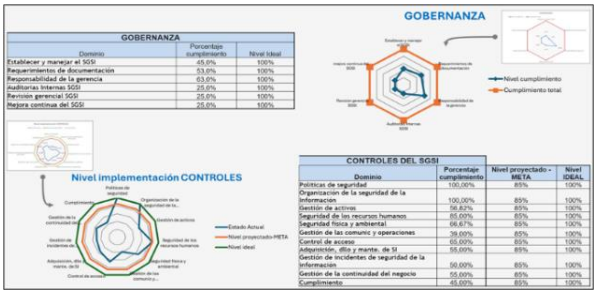
c. **Llarg termini**: Automatitzacions, solucions avançades.



Pilar 2: Regulació i compliment – *Gap Analysis*

Aquest es basa en el compliment normatiu, i es tracta de detectar les escletxes entre la situació actual de l'ens i els requisits de certificacions referents a la seguretat de la informació (***PCE RES de l'ENS*** per defecte), preparant el terreny per al seu compliment. Analitzem el nivell de maduresa de compliment normatiu respecte a la seguretat de la informació fent fort èmfasi als **circuits de governança, organitzatius i de cadena de subministrament** en matèria de seguretat de la informació. Presentació de resultats en format full de ruta d'adequació. El Cap Analysis inclouria:

- Revisió (si existeix) del **Pla de Seguretat**.
- **Entrevistes amb responsables**: Sessions amb els equips de compliment, RRHH, seguretat i direcció de l'ens per tal de mapejar processos i documentació existent.
- **Verificacions i recopilació d'evidències**:
- Revisió de polítiques, plans de continuïtat i registres d'incidents.
- Comprovació de compliment amb requisits específics (ENS, NIS2, ISO, ...).
- Recopilació de documents normatius actuals.
- **Estudi i definició d'estratègia**: Comparativa entre l'estat de l'ens envers els requisits del perfil de compliment desitjat
- **Priorització en fases**: Ordenació de tasques segons urgència (terminis legals), impacte en la certificació, alineació amb l'operativa de l'ens i cost d'implantació/manteniment.
- **Reunió de presentació de resultats**: Sessió amb l'ens per revisar conclusions del Gap Anàlisis (nivell de compliment, bretxes, ...) i recomanacions, ajustant prioritats segons retroalimentació



Pilar de Integració: Creació del CiberTrack

Consolidar la informació i coneixement generats entre el *Security Roadmap* i el *Gap Analysis* en un format **únic de fulla de ruta personalitzada**. Identificar Quick Wins contextualitzats en l'estat de situació i context estratègic de l'ens. Activitats:

- **Creuament de prioritats:** Comparativa entre les accions del Roadmap i el Gap Analysis per identificar sinergies i dependències. Per exemple: el **Pla de continuïtat** (del *Gap Analysis*) requereix primer controls bàsics (del *Roadmap*).
- **Ajust estratègic:** Modificació, si cal, de les prioritzacions inicials per optimitzar esforços

De forma general tots els riscos identificats amb anterioritat s'avaluaran obtenint-ne una valoració dels mateixos en base a un anàlisi qualitatiu i quantitatiu segons els següents criteris:

- **Impacte en l'organització**. Impacte operacional, financer i reputacional
- **Probabilitat d'explotació**. avalua la dificultat amb la que una vulnerabilitat identificada pot ser explotada per un atacant, incloent la disponibilitat d'eines, existència d'exploits, etc.
- **Classificació dels actius:** en base a la seva importància per a l'organització com dades sensibles, serveis al ciutadà, etc. Així com les seves dependències entre ells.
- **Esforç de remediació/gestió del canvi.** Avalua la mitigació segons criteris de temps, recursos, coneixement. Considera l'impacte en la remediació, i en l'operativa
- **Compliment normatiu:** avalua si el risc o vulnerabilitat, afecta al grau de compliment desitjat.

2.3. Anàlisis tècnics basats en pentests

Aquesta fase, plantejada com a anàlisi de camp, planteja una altra òptica i metodologia d'auditoria **totalment complementària** a la plantejada per l'enfoc basat en controls. L'auditoria duran a terme proves automàtiques i manuals, incloent l'escaneig de vulnerabilitats (es categoritzaran en base al criteri ***CVSS v3.1***), i l'explotació controlada de vulnerabilitats. Tots els descobriments es documentaran amb evidències i una anàlisi d'impacte.

De forma general, es mantindrà un canal de comunicació constant amb l'ens durant l'execució dels pentest per tal de poder demanar finestres d'actuació, executar consultes o rebre *feedback*, fent un informe mínim diari durant el temps d'execució.

Durant el procés de pentesting poden anar sorgint diferents oportunitats i adversitats que poden fer variar la planificació, abast i bateria de proves, tot i que de forma general s'identifiquen els següents abasts: pentest intern, pentest extern, pentest web, i pentest cloud,

2.4. Pla de millora: Transferència de coneixement i seguiment

Un cop finalitzades les proves i anàlisi, s'arriba a la fase de presentació de resultats i **Pla de Millora.**

2.4.1. Presentació de resultats

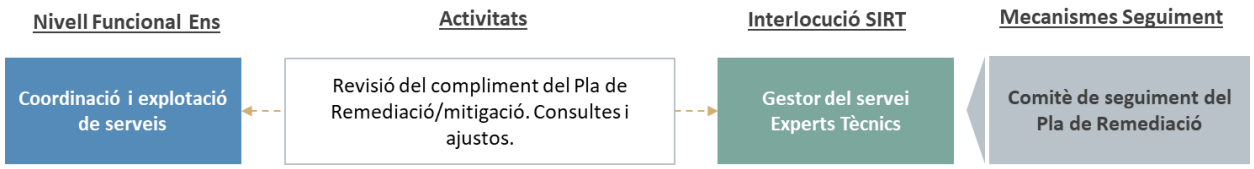
A la finalització de l'elaboració de la documentació, es convocarà una reunió de presentació de resultats que compti amb l'equip d'auditoria i els principals interessats de l'ens:

Reunió	Assistents	Agenda
Presentació de resultats	Ens: - CIO / Responsable IT. - CISO / Responsable de seguretat. - Representant de Direcció.	Presentació de la planificació i abast de la fase de Transferència de Coneixement i seguiment. Presentació informe executiu Comentar principals riscos i febleses. Comentar conclusions.

2.4.2. Pla de Remediació i Actuacions front desastres

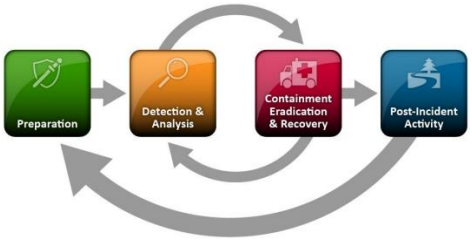
S'estableix un comitè de seguretat que inclogui a l'equip de projecte i els experts tècnics necessaris per part de SIRT, així com interlocutors tècnics i de direcció IT/Seguretat per part de l'Ens per tal de mantenir una comunicació eficient i una execució del **Pla d'Actuació front desastres**.

El Comitè de Seguiment mantindrà reunions periòdiques abans del tancament del projecte a fi de mantenir el control i interlocució envers el Pla de Remediació amb la següent estructura:



2.4.2.1. Metodologia i contingut del Pla de Remediació

La metodologia utilitzada per tractar l'incident cas d'ús es basarà en la proposada del marc normatiu NIST. I la descripció dels incidents, es en la catalogació de tàctiques i tècniques que proposa el framework proposat per Mitre ATT&CK



1. Preparació

Te com objectiu que l'entitat disposi de una preparació adequada per afrontar un incident de seguretat amb les màximes garanties. Contar amb les eines o suport de resposta incidents, tenir actualitzar el pla de contingència, definit la comunicació directa amb la gerència, realització de simulacres, tenir establerts els rols, funcions. Revisió continua (persones, tecnologia i processos).

2. Detecció i Anàlisis

Monitoratge amb SIEM, IPS, EDRs,XDRs, NDRs, etc. La detecció precoç és clau per reduir l'impacte.

Confirmació de l'incident: validar si és real o un fals positiu. En cas de confirmació, obtenir una descripció complerta sobre els fets que estan constituint l'incident de seguretat. En aquest punt; la identificació i catalogació del vector d'atac, així com el registre i la comunicació seran els punts fonamentals d'aquesta fase. El vector d'atac te relació amb l'origen del nostre incident de seguretat.

3. Contenció, erradicació i recuperació del servei

Aïllament dels sistemes compromesos, bloqueig dels accessos, i desactivació dels serveis vulnerables. L'equip assignat a l'incident proposarà una estratègia, agrupant les mitigacions prèviament executades, sota la premissa d'evitar robatoris de dades, danys potencials, i preservació de les evidencies.

L'estratègia d'erradicació i recuperació, vetllarà per la **perpetuïtat** de la **solució** i garantit la **no repetició** del **incident** de seguretat amb el mateix vector d'entrada. S'activarà una oficina de desbordament, Sirt posarà a disposició de la entitat afectada un **equip multidisciplinar d'experts** amb disponibilitat 24x7 per mitigar qualsevol carència de coneixement i dotar dels perfils necessaris per tal de garantir que aquesta fase s'executa amb totes les garanties.

4. Activitats post incident

Un cop recuperat el servei de l'Ens afectat, es convocarà una última sessió, que tindrà dos objectius; treballar les lliçons apreses i realitzar la entrega formal de la documentació. Les lliçons apreses, consisteix en recapitular la descripció dels fets, i valorar conjuntament que es podria haver fet millor. Per últim, caldrà notificar l'incident:

- Notificar a l'Agència de Ciberseguretat de Catalunya si l'incident afecta entitats públiques o privades amb seu a Catalunya. En cas que l'Ens també fos un servei digital, s'ha de notificar a INCIBE-CERT segons la normativa (RD-Llei 12/2018).
- En cas de fuita de dades personals, també s'ha de comunicar a l'AEPD segons el RGPD.

5. Servei de Formació en Ciberseguretat.

Avaluar el **grau d'exposició a amenaces**, es el principal objectiu de l'auditoria, i es important definir una sèrie de Vectors d'Atac Principals que esdevinguin un marc de referència per a tots els controls i proves tècniques de la auditoria.

SIRT ha identificat aquests vectors d'atac en base a les principals amenaces en el vertical Administració / Govern Local a Catalunya, a partir de fonts obertes d'intel·ligència (OSINT), incidents recurrents i butlletins com els publicats per l'Agència de Ciberseguretat.

Principals Vectors d'Atac

	Atacs a través de **ransomware** que puguin bloquejar l'accés per part de l'usuari a actius mitjançant tècniques com el xifrat.
	**Enginyeria social i phishing** a usuaris per tal de que revelin informació confidencial o credencials d'accés. Contemplant particularitats com la suplantació d'identitats.
	**Intrusions** a sistemes crítics tant mitjançant elements de codi maliciós com obtenció de credencials, atacs de força bruta, ...

	**Exploits de vulnerabilitats** tant àmpliament coneguts com *ZeroDay* de forma que puguin comprometre elements que formin part dels actius a protegir: llibreries de codi, aplicacions, sistemes operatius, dispositius/hardware.
	Atacs volumètrics i distribuïts de denegació de servei (DDoS) que impedeixin la operació i funcionament de serveis publicats.

Respecte els principals vectors d'atacs més prolífers per els Ens Local, destaques els 3 primers, amb un protagonista comú: **l'usuari**. Aquest és l'eslavó més dèbil de la cadena. És per això, que cal tenir definida una política de **formació i conscienciació activa,** que formarà de per vida, del pla de millora.

5.1. Formació especialitzada a responsables TIC.

El nostre servei de formació s'estructura per cobrir les necessitats específiques de sensibilització i capacitació de les entitats públiques de Catalunya. L'objectiu és reduir la superfície d'atac mitjançant la formació del personal, tant general com tècnic, combinant teoria i pràctica amb eines reals, recursos gratuïts i casos adaptats al sector públic.

En l'àmbit del sector públic, aquest component pren una importància crítica per l'exposició creixent a atacs digitals i la necessitat de complir amb normatives com l'ENS o la NIS2. La nostra proposta de formació en ciberseguretat per a ens locals i autonòmics de Catalunya respon a aquesta necessitat amb una oferta estructurada, pràctica i alineada amb el marc normatiu i tècnic actual.

El servei es divideix en **dues grans línies**: una orientada a tot el personal de l'organització per promoure una cultura de ciberseguretat bàsica, i una altra pensada específicament per a responsables TIC, amb continguts tècnics i enfocats a la gestió de riscos, infraestructura i compliment legal. Totes les formacions inclouen exemples reals, exercicis pràctics i accés a recursos reutilitzables perquè l'ens pugui continuar el procés formatiu amb autonomia.

Modalitats disponibles:

- Formació presencial, en línia en directe o asíncrona.
- Sessions úniques, itineraris per rols, o campanyes recurrents.
- Acompanyament i suport post-formació per a reforçar l'aprenentatge.

El nostre servei de formació en ciberseguretat no només busca complir amb els requisits formals, sinó generar un canvi real en la cultura de seguretat digital.

5.1.1. Servei de Formació General en Ciberseguretat

El personal no tècnic sovint és la porta d'entrada per a molts ciberatacs, ja sigui per desconeixement, falta de protocols clars o per manca de sensibilització. Aquesta formació està dissenyada per reduir aquest risc educant a tot el personal sobre les amenaces més habituals, promovent bons hàbits

digitals i oferint eines per actuar amb seguretat en el dia a dia. Els **continguts** s'expliquen amb un llenguatge proper i comprensible, utilitzant **exemples extrets de situacions reals** ocorregudes al sector públic i facilitant materials visuals i pràctics que reforcen l'aprenentatge:

- **Riscos digitals habituals:**
  - Identificació de correus electrònics fraudulents (phishing).
  - Amenaces a través de missatgeria (SMS, WhatsApp).
  - Exercici pràctic: visualització i identificació de 10 exemples reals de correus fraudulents.
  - Simulació opcional de phishing amb resultats agregats i recomanacions.
- **Malware i seguretat bàsica:**
  - Com s'infiltra el malware: adjunts, webs compromeses, USBs.
  - Protecció mitjançant actualitzacions, antivirus i hàbits segurs.
  - Exercici pràctic: revisió guiada del propi equip i navegador per detectar punts febles.
- **Contrasenyes i autenticació segura:**
  - Criteris per a crear contrasenyes segures.
  - Ús de gestors de contrasenyes i activació de MFA.
  - Exercici pràctic: taller de creació i prova d'un gestor de contrasenyes.
- **Protecció de dades i eines digitals:**
  - Bones pràctiques amb correu, emmagatzematge i compartició.
  - Introducció a la protecció de dades i responsabilitats com a usuari.
  - Exercici pràctic: revisió de documents amb dades sensibles mal protegits.

A més, oferim recursos com infografies, vídeos, recordatoris periòdics i un qüestionari final que serveix com a avaluació i obtenció del certificat d'aprofitament.

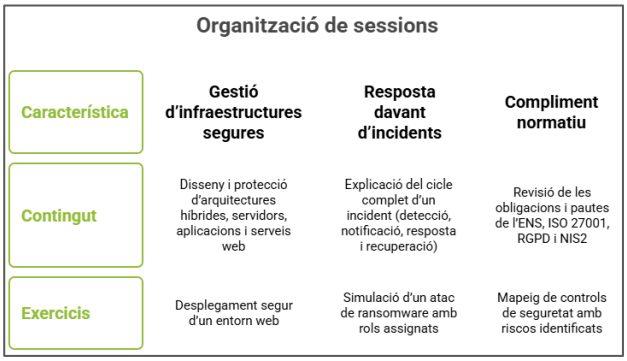
5.1.2. Formació Especialitzada per a Responsables TIC

Aquesta formació està pensada per proporcionar coneixements actualitzats, eines pràctiques i una visió estratègica per fer front a les amenaces actuals i futures, així com per a la correcta implementació de marcs legals i normatius.

Les sessions s'organitzen en **mòduls temàtics** i inclouen **exercicis** en entorns controlats, simulacions i documents útils per a la gestió tècnica del dia a dia:

- **Gestió d'infraestructures segures**: es treballa el disseny i protecció d'arquitectures híbrides, servidors, aplicacions i serveis web. Inclou una pràctic de desplegament segur d'un entorn web.

- **Resposta davant d'incidents**: s'explica el cicle complet d'un incident (detecció, notificació, resposta i recuperació) i com aplicar procediments d'actuació ràpida. Inclou una simulació d'un atac de ransomware amb rols assignats i resposta coordinada.



- **Compliment normatiu**: es revisen les obligacions i pautes de l'ENS, ISO 27001, el RGPD i la directiva NIS2, posant l'accent en accions concretes i auditories de compliment. Inclou un exercici de mapeig de controls de seguretat amb els riscos reals identificats a l'organització.

Els participants disposen també de guies pràctiques, plantilles de polítiques i informes, així com accés a eines gratuïtes per a l'avaluació de vulnerabilitats i gestió d'actius.

5.1.3. Personalització, llengua i continuïtat

Conscients de la diversitat dels ens públics catalans, el nostre servei és modular i adaptable. Oferim versions personalitzades per a sectors específics (educació, salut, serveis socials, etc.) i ajustem el nivell tècnic a cada col·lectiu.

Les formacions es poden impartir en **català** o **castellà**, i els materials es lliuren sempre en la llengua escollida. També oferim opcions presencials, remotes o híbrides, així com formació asíncrona a través d'una plataforma pròpia o de l'ens. Garantim la continuïtat i efectivitat de la formació, oferim:

- Microcàpsules trimestrals de reforç.
- Avaluacions post-formació.
- Suport i assessorament per a l'establiment de plans de formació interns i mecanismes d'autoavaluació.

5.1.4. Equip docent i compromís amb la qualitat

El nostre equip està integrat per professionals amb àmplia experiència en ciberseguretat aplicada al sector públic. Comptem amb perfils tècnics i docents amb certificacions reconegudes com **DPD, CISM**, **CISSP**, **ISO 27001 Lead Auditor** i una trajectòria contrastada en formació i consultoria per a administracions públiques. Treballem amb un model de qualitat basat en indicadors objectius com:

- Ràtios d'assistència i participació activa.
- Satisfacció dels participants.
- Millora dels indicadors de seguretat (reducció de clics en campanyes de phishing, millora en l'ús d'eines segures, etc.).

També incorporem l'avaluació contínua i el feedback dels participants per actualitzar els continguts i adaptar-los a les noves amenaces i canvis normatius.

Al marge dels vectors d'atac generals ja descrits, es desenvolupa una llista més exhaustiva de potencials vectors o particularitzacions de simulacions ja descrites, que poden esdevenir objecte de referencia per a basats en funció de les casuístiques de cada ens:

Servei/Acció	Descripció	Eines Suggerides
Identificació de Vulnerabilitats	Escaneig i avaluació de vulnerabilitats en sistemes, xarxes, aplicacions, usuaris i servidors.	*Nessus, Nmap, Burp Suite, OpenVAS...*
Avaluació d'AD On-Premise i Microsoft Entra	Anàlisi específic de la seguretat del Active Directory local i al núvol (Microsoft Entra).	*PingCastle, AzureAD PowerShell, BloodHound...*
Pentest d'Infraestructura Extern	Avaluació de seguretat dels sistemes exposats a internet, incloent-hi servidors, VPNs i dispositius perimetrals.	*Nmap, Nessus, OpenVAS, Hydra, Metasploit...*
Proves de Denegació de Servei (DoS)	Simulació d'atacs DoS per avaluar la resiliència de serveis crítics davant interrupcions.	*Hping3, Slowloris, etc.*
Simulacre de Portàtil Robat	Prova per avaluar la seguretat de les dades en cas de robatori d'un dispositiu corporatiu, incloent-hi xifrat de disc, credencials emmagatzemades i accés a xarxes internes.	*BitLocker Bypass, Mimikatz, Responder, EDR Evasion Tools...*
Campanya de phishing	Atacs d'Enginyeria Social (phishing, vishing) per comprometre usuaris i obtenir credencials o accés inicial.	*Phishing Frameworks, Spearphishing Tools...*
Red Team Físic	Simulació d'entrada no autoritzada a un edifici per verificar procediments físics.	Dispositius de hacking: *Rubber Ducky, Key Croc, etc.*
Compromís de Dispositius IoT o OT	Avaluació de seguretat de dispositius IoT o sistemes operatius industrials, si aplica.	*Shodan, Binwalk, Custom Exploits...*