inetum
Positive digital flow

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

Lot 34-41: Serveis de ciberseguretat

Exp. 2024.01

05/2024

44020231W NURIA PUJOL (R: A28855260)
44020231W NURIA PUJOL (R: A28855260) 2025.05.28 10:04:40 +02'00'

Índex

1 Inetum

Hem entrat en l'era de post-transformació digital. Una era en la qual les necessitats i els usos es reinventen contínuament, i les solucions dels quals encara no existeixen.

En aquest món en constant canvi, el desafiament de les empreses i organitzacions és adaptar-se al permanent flux digital que genera noves oportunitats econòmiques, de gestió i socials. **Creiem que aquest flux digital ha d' estar al servei de les necessitats de les empreses organitzacions i institucions i el seu impacte ha de ser positiu en les dones, els homes i la societat en el seu conjunt.**

És per això, que les nostres persones són aquí per permetre la renovació contínua de les empreses mitjançant el disseny d'estratègies digitals que responguin als seus reptes comercials. A partir de l' experiència pràctica i els usos construeixen solucions concretes i àgils i les integren en l' ecosistema únic de cada client.

Pioners en el negoci, hem crescut mantenint-nos fidels a la cultura empresarial i a l'esperit audaç dels nostres inicis.

La nostra missió és ajudar-los a treure el màxim profit d'aquest flux digital

Estem llestos. Junts, convertirem aquest nou món digital en un món d'èxit i compromís per a la seva empresa.

Grup Global Sòlid i Sostenible

Al Gener de 2021 neix **Inetum,** fruit de la fusió de diferents empreses líders a mercats internacionals. **Inetum** prové de la paraula llatina “incrementum” que significa creixement i que reivindica el nostre esperit emprenedor, ambiciós, proper i innovador.

Inetum és un soci de primer nivell de serveis IT amb valor afegit, solucions i innovació, que ha experimentat, des del seu naixement a França, una trajectòria de creixement única que l'ha convertit en un líder global, present a **19 països**, amb talent de més de **28.000 consultors i 2.500M€** de facturació el 2023.

La nostra Proposta de Valor

Partint d'un model d'entrega global i un model operatiu flexible i col·laboratiu, Inetum ha desenvolupat una **proposta de valor** que ens permet **oferir ràpidament un valor tangible i sostenible als nostres clients**.

Aquesta proposta de valor **s' articula en tres eixos**:

- **Transformació i Disrupció**: innovació i coneixement rellevant per a la indústria per assolir un valor comercial excepcional a partir d' una transformació disruptiva impulsada per la tecnologia.
- **Solucions Digitals**: desplegament de solucions creuades i verticals de classe mundial (IP propi i de tercers) per dinamitzar el rendiment de les empreses.
- **Eficiència TI**: serveis industrialitzats i automatització per impulsar el creixement sostenible i la màxima eficiència en la tecnologia de la informació.

Sota aquestes directrius, presentem un **porfoli de solucions 360º** que ens permet disposar d'una visió i experiència extensa de la transformació digital i ajudar els nostres clients a assolir els seus objectius.

1.1 Elements Diferencials

Tenim com a objectiu ser un partner tecnològic clau per les administracions locals de Catalunya a llarg termini, i més tenint en compte que l'Administració de la Generalitat de Catalunya és un dels principals focus d'activitat de la companyia. Amb el suport de l'estratègia de sector públic a nivell de tot Inetum Internacional, i amb tot l'equip que tenim a Catalunya per a la Generalitat, volem aportar el nostre saber fer i experiència.

Sempre amb un enfocament de proximitat i flexibilitat, acompanyarem a les administracions locals de Catalunya en els seus projectes i iniciatives amb proactivitat i alineament.

Els elements que entenem diferencials de la nostra proposta de valor per aquest servei són:

- **Coneixement extens del model TIC i activitat de la Generalitat:** desenvolupem serveis tecnològics en diferents àmbits de l'activitat de la Generalitat de Catalunya, aportant aquesta experiència al present contracte.
- **Aliances i acords de col·laboració amb proveïdors líders de tecnologia:** cerquem activament associacions i acords de col·laboració amb proveïdors clau de tecnologia per millorar les seves ofertes i proporcionar solucions integrals i capdavanteres.

- **Capacitat com una de les 5 principals companyies de TIC en el panorama d'Espanya:** La nostra posició com una de les 5 principals companyies de TIC a Espanya ens permet oferir una àmplia gamma de serveis i capacitats per a satisfer les necessitats de les administracions locals de Catalunya, aportant un sòlid equip de talent, experiència i recursos.

Per acreditar la qualitat dels nostres serveis, hem optimitzat els nostres processos, assolint una sèrie de **certificacions corporatives** que ens ha permès crear un model d'interacció entre les diferents unitats organitzatives i les parts interessades, identificant el marc d'actuació (processos i procediments) per a la generació de **valor afegit** als nostres clients.

Les nostres ambicions de creixement i la nostra posició com a líder al mercat només es poden materialitzar de manera sostinguda per la confiança dels nostres clients. Per garantir-ne l'assoliment, el Grup Inetum Espanya, compta amb els següents sistemes de gestió:

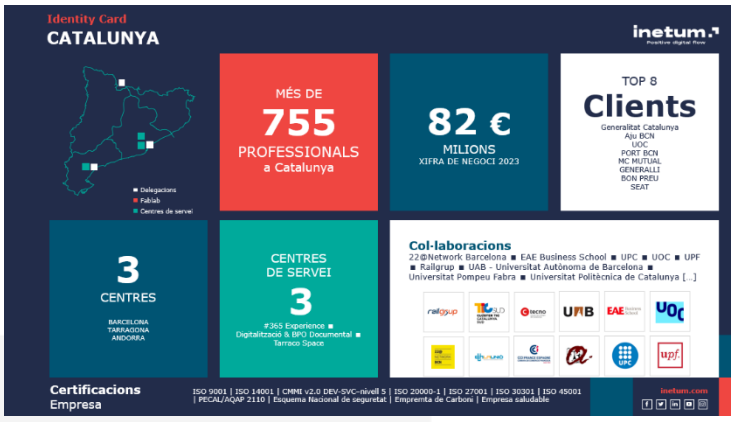
- **UNE-EN ISO 9001** - Sistema de Gestió de la Qualitat.
- **UNE-EN ISO 14001** - Sistema de Gestió Medi Ambiental.
- Empremta de Carboni.
- **ISO 45001**. Sistema de gestió de la seguretat i la salut en el treball per a la millora proactiva de la prevenció de riscos laborals, i el benestar de les persones.
- **UNE-ISO/IEC 20000-1** - Sistema de Gestió dels Serveis.
- **CMMI** Capability Maturity Model Integration
- **PECAL**. Certificació que avala el compliment dels requisits del Ministeri de Defensa d'Espanya (requisits OTAN) per a la gestió de la Qualitat
- **UNE-ISO 30301** - Sistema de Gestió de Documents.
- **UNE-ISO/IEC 27001** - Sistema de Gestió de la Seguretat de la Informació.
- **ENS** - Esquema Nacional de Seguretat.

1.2 Inetum a Catalunya

Inetum és un grup internacional sòlid i sostenible: consultor, integrador i proveïdor de serveis i solucions verticals que donen resposta a l'estratègia dels nostres clients. Un **líder tecnològic europeu** amb una trajectòria de creixement única.

Com hem destacat anteriorment, amb una facturació de 2.500M€ l'any 2023, presència en 19 països, i +**28.000 talents digitals** que formen part de la família **Inetum, portem al nostre ADN la innovació**, com eix de tracció de la nostra societat:

L'èxit d'**Inetum està basat en 3 eixos**:



Som un actor global amb prioritització per la proximitat als seus clients i al territori. Amb un model d'actuació basat en **"pensar en global, actuar en local"**, **Inetum** dins l'àrea de IBERIA&LATAM ha creat 3 societats que consoliden xifres: **Inetum** España, **Inetum** Norte i **Inetum Catalunya**.

Inetum Catalunya, empresa catalana amb NIF propi creada al gener 2021 i arrancant la seva activitat amb un Pla Estratègic territorial molt ambiciós que inclou inversions en infraestructures, talent i centres de referència del grup a nivell global.

Actualment **Inetum Catalunya** compta amb prop de 800 professionals i una facturació aproximada de 82M€ al darrer exercici fiscal. Disposem d'oficines a Andorra, Barcelona i **Tarragona i en aquesta darrera seu disposem d'un centre de serveis i de generació de talent** que dona cobertura a projectes de desenvolupament transversals a la corporació.

Des d'**Inetum Catalunya** ens agrada destacar la implicació que tenim al territori formant part activa de les principals associacions que promouen la innovació i l'estratègia digital del país (com per exemple la DCA), a la vegada que mantenim acords i col·laboracions amb les principals universitats catalanes.

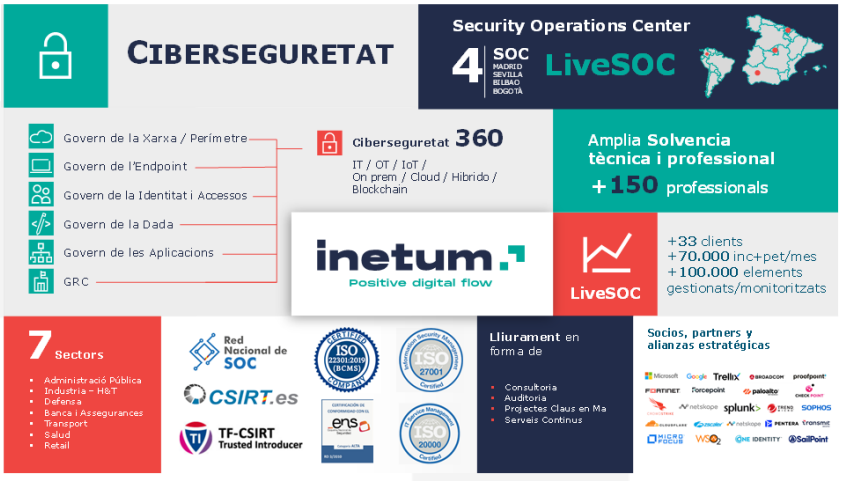
Així mateix, la Generalitat de Catalunya és un client estratègic per l'entitat. Aquesta consideració implica que el Grup Inetum posa focus especial en garantir el millor servei i qualitat per a totes les activitats desenvolupades en el marc de serveis destinats a la seva administració. Així doncs, les administracions locals de Catalunya disposarà d'un elevats estàndards de qualitat i dedicació per part de la companyia.

1.3 Unitat de Negoci de Ciberseguretat

Fent focus en el àrea de Ciberseguretat, **Inetum** compta al territori amb una Unitat de Negoci que alhora ha estat recentment nomenada com a **Divisió Global** per donar **servei a tots els territoris i oficines d'Inetum a nivell mundial**.

La Unitat de Negoci de Ciberseguretat compta amb més de **150 professionals** tocant tots els àmbits dintre del mon de la ciberseguretat: Govern de la Dada, Protecció del lloc de treball, perímetre, cloud, Govern d'aplicacions, Govern, Risc i Compliment; prestant els seu serveis en diferents modalitats: serveis de Consultoria, Auditoria, Projectes tancats o Serveis Continus.

Contemplat dintre d'aquest últim àmbit, els Serveis Continus, **Inetum** disposa d'un **SOC amb 4 ubicacions geogràfiques** des d'on es presten molts serveis com prestats per les administracions locals catalanes i sobre els que es prestaran les serveis objecte d'aquest expedient. En aquest sentit, **Inetum** brinda les seves capacitats i coneixements en aquest àmbit, **coneixements adquirits amb la seva pròpia experiència**, per tal de oferir els millors serveis possibles a les administracions locals de Catalunya.



La solvència del SOC d'**Inetum** ve avalada per les principals certificacions en l'àmbit de la qualitat en la Prestació de Serveis (**ISO 20000**), en serveis de Seguretat de la Informació (**ISO 27001**), Continuïtat de Negoci (**ISO 22301**) i la recentment obtinguda per a l'entorn del SOC com es l'**ENS** (Esquema Nacional de Seguridad) de **nivell Alt**.

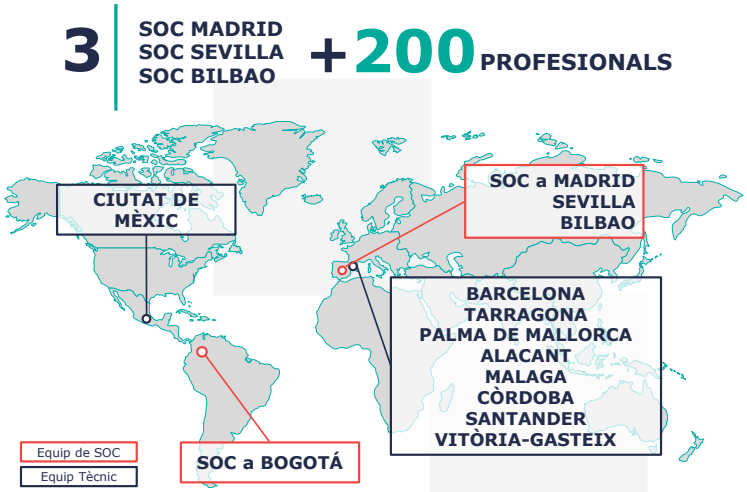
Addicionalment, dintre de l'ecosistema dels Centres d'Operacions de Seguretat, el SOC d'**Inetum** es membre de la **Red Nacional de SOC**, **CSIRT.es, TF-CSIRT** i **FIRST**.

2 Serveis de Ciberseguretat

La unitat de negoci de Ciberseguretat d'Inetum es una unitat amb cobertura global que dona suport a la totalitat de territoris i oficines a nivell mundial. La unitat de Ciberseguretat compta amb més de 200 professionals especialitzats en tots els àmbits dintre del mon de la ciberseguretat. Partint d'aquestes capacitats, per tal de donar cobertura a la heterogeneïtat de les possibles necessitats de les administracions locals dintre del servei, es posa a disposició del servei una piràmide de recursos segons les necessitats en cada moment. Aquesta piràmide serà coordinada pel **Service Manager**.

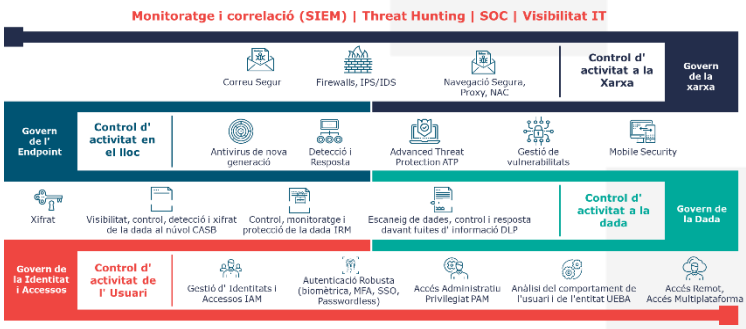
La metodologia d'Inetum, centrada en la millora contínua, permet no solament el **monitoratge i anàlisi detallada del servei prestat**, sinó també la identificació i implementació de **punts de millora** que contribueixen a l'evolució i optimització del servei. Això es tradueix en una **capacitat per afrontar augments de demanda o la incorporació de coneixements específics** que inicialment no estaven contemplats, gràcies a la **gestió dinàmica de recursos** i a la disposició d'oficines tècniques que assignen aquests recursos de manera flexible i adaptada a les necessitats del moment.

L'equip de Ciberseguretat d'Inetum consta actualment de **10 localitzacions en territori nacional**, compost per més de **200 professionals** distribuïts entre les diferents pràctiques i serveis, volum que permet assumir aquests augments de la demana, incorporació de coneixements en tecnologies específiques.



Inetum disposa dintre de la unitat de negoci de Ciberseguretat de coneixement i ampli *expertise* en l'entrega de serveis de ciberseguretat en tots els seus àmbit. Una visió global de la tipologia de serveis que Inetum presta des d'aquesta línia de serveis es la que es detalla a la següent imatge.

Disposem de referències en projectes i serveis en aquests àmbits en entorns equivalents com son **AENA, JUNTA DE ANDALUCIA, GOBIERNO DE ARAGÓN, BANCO DE ESPAÑA, MINISTERIO DE ECONOMIA Y EMPRESA o SAREB** i serveis en el entorn de la **GENERALITAT DE CATALUNYA** com es el Servei de Qualitat en la Provisió de Serveis a l'Usuari (Lloc de Treball), on la unitat de Ciberseguretat gestiona els serveis de seguretats associats a l'àmbit.



Aquesta experiència multidisciplinar tant en l'àmbit de serveis de govern com en àmbits tecnològics diversos dintre de la ciberseguretat ha dotat a l'equip d'Inetum de coneixement en la prestació d'aquests tipus de serveis en format d'experiència, *best practices*, lliçons apreses, etc. **que proporcionarà a les administracions catalanes una amplia experiència i cobertura de capacitats** en els serveis proporcionats per Inetum.

Per altre banda, tal i com es descriu mes endavant en el punt 2.3, Inetum compta amb mecanismes per accelerar la incorporació de nous recursos quan això esdevé necessari. Això inclou la **pre-formació i capacitació contínua en l'entorn de les administracions locals**, l'**emmirallament de perfils clau** per garantir la cobertura del servei davant eventualitats, i una gestió proactiva de la rotació de l'equip. Aquest enfocament es complementa amb la **Factory Cyber de Tarragona**, una iniciativa que actua com a incubadora d'innovació i talent en ciberseguretat, proporcionant un entorn ric en recursos i coneixement on els professionals poden desenvolupar les seves habilitats.

2.1 Serveis d'Implantació, Assessoria Tècnica i Formació

En aquest apartat es descriuen les característiques generals i particulars que reuneixen els materials, solucions i serveis inclosos en les diferents unitats d'obra que integren el present projecte, així com les condicions que s'aplicaran per a la seva implantació, configuració i posada en funcionament.

Davant les necessitats plantejades per l'Ens Públic o Administració destinatària del present document, la proposta contempla un **model de col·laboració integral** que abasta des de l'assessoria prèvia i el disseny d'arquitectura fins a la implantació, formació i suport postvenda. Les tasques incloses són les següents:

- **Serveis d'Assessoria Tècnica especialitzada**, per a l'anàlisi de la situació actual, definició de requeriments, selecció de tecnologies i acompanyament expert en la presa de decisions estratègiques.
- **Definició de la topologia i redisseny de l'arquitectura**, considerant els requisits funcionals, normatius i de seguretat específics de l'entorn.
- **Desenvolupament de la configuració detallada, instal.lació i proves de validació** en entorn productiu, alineades amb els criteris establerts per la Direcció Tècnica del Projecte.
- **Formació operativa a peu de màquina**, adreçada al personal tècnic de l'organisme client, amb l'objectiu de garantir l'autonomia en l'operació i gestió de les solucions desplegades.
- **Prestació d'un servei de suport i manteniment tècnic**, per assegurar l'acompanyament durant el primer any del servei, incloent resolució d'incidències, actualitzacions i suport tècnic funcional.

Previ a l'execució del projecte, es durà a terme un **replanteig in-situ** entre Inetum i el personal tècnic del client, amb l'objectiu de concretar detalls tècnics, logístics i organitzatius.

2.1.1 Abast dels Treballs d'Execució

Els treballs d'execució compresos en aquest projecte es desenvoluparan en les instal.lacions designades per l'Ens Públic, i inclouran:

- El subministrament dels materials necessaris i la prestació de la mà d'obra tècnica especialitzada, per a l'execució completa dels treballs.
- Reunions inicials amb els responsables tècnics del client per definir el calendari del projecte

i revisar els aspectes tècnics clau.

- Implantació, configuració i validació funcional dels equips i eines, assegurant la seva plena operativitat.
- Execució de proves de posada en marxa, conforme a l'establert i supervisades conjuntament.
- Reparació o substitució d'elements que presentin fallades durant la fase de proves.
- Assumpció, per part d'Inetum, de les despeses logístics i operatives associades a l'execució del projecte: transport, lloguer de maquinària, mitjans auxiliars, etc.

2.2 Coordinació amb l'Entitat Local

Durant tota la vigència de la prestació dels serveis de ciberseguretat, es garantirà una coordinació fluïda, estructurada i permanent amb l'entitat local, amb l'objectiu d'assegurar una resposta àgil i efectiva davant qualsevol incidència que pugui afectar la seguretat de la informació i els sistemes gestionats.

A més, es designarà un **Responsable de Servei assignat** que actuarà com a interlocutor tècnic i operatiu de referència per a l'entitat local, encarregat de coordinar les activitats de seguiment, informar de l'estat de les incidències i vetllar pel compliment dels terminis de resolució establerts en els acords de nivell de servei (SLA).

Aquest esquema de comunicació quedarà recollit en un **Pla de Comunicació Operativa**, que s'acordarà amb cada entitat local en l'inici de la prestació, i que detallarà els punts de contacte, canals disponibles, procediments de notificació i protocols d'escalat.

La coordinació del projecte/servei serà responsabilitat del **Responsable del Servei d'Inetum**, qui actuarà com a únic interlocutor davant la Direcció Tècnica del client.

Entre les seves responsabilitats s'inclouen:

- **Interlocució tècnica i operativa**
  - Exercir de punt de contacte únic entre l'entitat local i l'equip de prestació del servei.
  - Canalitzar les consultes, sol·licituds i incidències que afectin el servei de ciberseguretat.
  - Participar en les reunions de seguiment periòdiques amb l'entitat local.
- **Gestió i seguiment d'incidències**
  - Supervisar i fer el seguiment de totes les incidències registrades, vetllant pel seu correcte tractament segons els protocols establerts.
  - Coordinar els recursos tècnics necessaris per a la resolució d'incidències, especialment en cas de situacions crítiques.
  - Informar l'entitat local sobre l'estat i l'evolució de les incidències obertes.
- **Gestió de canvis i peticions de servei**
  - Recollir i valorar les peticions de canvis o ampliacions de servei proposades per l'entitat local.
  - Coordinar l'anàlisi de viabilitat i la planificació d'implementació d'aquests canvis.
  - Comunicar formalment les decisions i calendaris associats.
- **Supervisió del compliment dels acords de nivell de servei (SLA)**
  - Controlar els indicadors de servei i vetllar pel compliment dels nivells de servei establerts en el contracte.
  - Proposar accions correctores o de millora en cas de desviacions detectades.

- **Gestió documental i informes**
  - Elaborar i remetre els informes periòdics de servei, incloent-hi estadístiques d'incidències, temps de resposta i resolució, i altres indicadors rellevants.
  - Actualitzar la documentació operativa associada al servei: protocols, inventari de sistemes, i procediments de gestió d'incidències.
- **Coordinació d'activitats preventives i de manteniment**
  - Planificar i comunicar a l'entitat local les tasques de manteniment preventiu o evolutiu que puguin tenir impacte sobre el servei.
  - Coordinar les activitats tècniques amb l'equip de servei i l'entitat local per minimitzar riscos i afectacions.
- **Escalat d'incidències i situacions crítiques**
  - Actuar com a responsable d'escalat en situacions d'incidència crítica o d'emergència, assegurant la comunicació immediata amb els responsables de seguretat de l'entitat local i amb els equips d'intervenció corresponents.
- **Assessorament i proposta de millores**
  - Proposar millores en la prestació del servei, tant a nivell de processos com de solucions tecnològiques.
  - Assessorar l'entitat local en matèria de bones pràctiques en ciberseguretat, en relació amb els serveis contractats.

Durant el projecte, els responsables d'Inetum estaran localitzables a través dels següents canals:

- Telèfon fix i mòbil.
- Correu electrònic amb resposta garantida.

2.3 Procediment d'Actuació Davant de Desastres

Model d'Activació

Durant la fase de Recepció del Servei, es definirà conjuntament amb l'AALL el model d'activació de l'equip de Resposta a Incidents Crítics. Aquest model assegura una resposta ràpida i eficaç davant incidents d'alt impacte, com atacs massius o la indisponibilitat de serveis crítics, mitjançant un procés d'escalat que mobilitza eficientment els recursos necessaris.

L'activació de l'equip de resposta depèn de la severitat de l'incident i el seu impacte en els serveis o actius crítics de l'AALL. S'establiran criteris per classificar els incidents i determinar la necessitat d'activació del servei, que seran revisats i ajustats conjuntament per adaptar-se a les necessitats específiques de l'AALL.

- **Incident massiu**: Un incident es considera massiu quan afecta múltiples sistemes, usuaris, o aplicacions de manera simultània i compromet significativament la integritat, confidencialitat o disponibilitat dels actius de l'organització. Els incidents d'aquest tipus solen ser atacs coordinats, com ara un atac de ransomware que xifra dades crítiques i paralitza operacions, atacs DDoS que interrompen múltiples serveis simultàniament, o una filtració massiva de dades que comprometi informació sensible, afectant la reputació i el compliment normatiu de l'organització.
- **Indisponiblitat greu d'un servei crític:** Els serveis crítics són aquells que són essencials per a la continuïtat del negoci i l'operació diària. La indisponiblitat d'un d'aquests serveis pot tenir conseqüències greus, afectant la productivitat i, en alguns casos, la viabilitat operativa de l'organització. Els serveis crítics solen incloure plataformes de negoci essencials com sistemes

ERP, CRM i administració electrònica, infraestructura de xarxa com sistemes de connectivitat i servidors centrals, o sistemes de seguretat com firewalls, eines de protecció de llocs de treball i sistemes d'autenticació, deixant vulnerable l'organització.

Procés d'Activació

El procés d'activació es divideix en diverses etapes, assegurant que la resposta a l'incident sigui ràpida, precisa i ben coordinada. La primera etapa es centra en la detecció de l'incident, seguida per la confirmació de la seva criticitat i la activació formal de l'equip de resposta i del Comitè de Crisi.

- **Detecció Inicial:** L'incident és detectat a través de diversos mecanismes. Normalment des del SOC amb el servei de monitorització, però també pot provenir d'informes externs, com notificacions de proveïdors de serveis d'intel·ligència d'amenaces, socis comercials, o reguladors, així com dels mateixos usuaris que experimenten problemes amb els sistemes afectats.
- **Validació i Escalat:** Un cop detectada l'alerta, l'equip d'analistes del SOC (generalment de nivell 2 o superior) s'encarrega de validar la seva legitimitat i determinar si realment constitueix un incident de seguretat crític. En aquesta fase, s'analitza la naturalesa de l'atac, el seu abast i el seu potencial impacte sobre els serveis i actius crítics de l'organització. Si els resultats d'aquesta validació confirmen que l'incident compleix amb els criteris de severitat, es procedeix a l'activació del servei de Resposta a Incidents Crítics i el Comitè de Crisi.
- **Activació del servei de Resposta a Incidents Crítics**: El **Responsable de Servei** d'Inetum és notificat immediatament una vegada que s'ha confirmat que l'incident és crític. En aquest punt, l'equip de resposta a incidents s'activa formalment. Això implica mobilitzar tots els membres clau de l'equip, involucrant perfils tant d'Inetum com de l'AALL, que inclou responsables dels serveis afectats, perfils tècnics multidisciplinars com analistes del SOC, especialistes en xarxes i sistemes, experts en intel·ligència d'amenaces i forenses digitals, per iniciar la resposta coordinada a l'incident.
- **Generació del Comitè de Crisi:** Simultàniament, el Comitè de Crisi es convoca per coordinar les decisions estratègiques a nivell tàctic. Aquest comitè inclou interlocutors tant de l'AALL, d'Inetum (no només del servei continu sinó aquells addicionals que puguin assessorar i guiar les decisions i mesures preses en el comitè) i, segons el cas, tercers que puguin aportar en la resolució del incident. El comitè com a objectiu supervisar i autoritzar les accions més crítiques, com l'aïllament de sistemes, la comunicació a reguladors i la priorització de la restauració de serveis. En el punt 2, Gestió i Governança del Servei, de la present proposta es desenvolupa en mes detall aquest comitè.

Pla de Comunicació i Seguiment

El pla de comunicació i seguiment és essencial per a la gestió efectiva d'un incident crític, assegurant que totes les parts involucrades estiguin informades en temps real sobre el progrés, les accions en curs, les decisions estratègiques i els propers passos. Inetum disposa d'un pla estructurat que es pot adaptar a les necessitats específiques de l'AALL, garantint flexibilitat i adequació a les seves polítiques internes. Els objectius principals són mantenir informats tots els actors clau, facilitar la presa de decisions, coordinar accions eficientment, garantir la transparència i assegurar l'adaptabilitat del pla.

Per aconseguir aquests objectius, es defineixen un conjunt de reunions i sessions de seguiment:

- **Reunions inicials d'avaluació:** Just després de l'activació de l'equip de resposta a incidents crítics, es realitzen reunions per entendre l'abast de l'incident i prioritzar les accions a prendre, compartint una anàlisi preliminar.
- **Sessions regulars de seguiment:** Durant la gestió de l'incident, s'estableixen reunions periòdiques per revisar les accions preses, discutir els resultats obtinguts i ajustar el pla de resposta segons sigui necessari, coordinant recursos addicionals si cal.

- **Comitè de Crisi:** Aquest comitè es reuneix segons l'evolució de l'incident per prendre decisions estratègiques, presentant informes d'estat per part del CSIRT i els analistes forenses, juntament amb recomanacions sobre accions futures.
- **Revisió final post-incident:** En finalitzar la fase crítica de l'incident, es realitza una reunió d'avaluació final per revisar els resultats obtinguts, l'efectivitat de les mesures implementades i les lliçons apreses, discutint possibles millores en les polítiques i procediments de seguretat.

Aquest pla de comunicació inclourà la comunicació a organismes pertinents com el **Centre Nacional per a la Protecció d'Infraestructures Crítiques i Ciberseguretat (CNPIC)**, l'**Agència de Ciberseguretat de Catalunya** o el **Centre Criptològic Nacional (CCN-CERT)**, i altres autoritats reguladores i de seguretat, garantint la transparència i la coordinació necessària per gestionar incidents crítics de manera eficaç. A més, es consideraran les notificacions a entitats com l'**Autoritat Catalana de Protecció de Dades (APDCAT)** i l'**Agencia Española de Protección de Datos (AEPD)** en cas de bretxes que afectin dades personals.

Informes de Progrés

Al llarg del cicle de vida de l'incident, es generaran diferents tipus d'informes, amb diferents nivells de detall i audiència:

- **Informes d'estat tècnic:** Emesos regularment pel CSIRT, detallen les accions realitzades, els indicadors de compromís (IoCs) identificats, i el progrés en la mitigació o resolució de l'incident. Aquests informes són dirigits a l'equip tècnic de l'AALL i els interlocutors clau.
- **Informes executius:** Resum les decisions clau, l'impacte de l'incident, i les properes accions per a l'alta direcció de l'AALL. Aquests informes es generen amb menor freqüència però amb un enfocament en l'impacte estratègic i operatiu.

Activitats Post-Incident i Definició d'un Pla de Millora Contínua

Un cop gestionat un incident crític i restaurats els sistemes afectats, és essencial realitzar un anàlisi detallat de l'incident i de les accions preses per identificar causes, efectes i establir millores per prevenir futurs incidents. A Inetum, aquest procés inclou activitats post-incident i la definició d'un pla de millora contínua.

- **Anàlisi Forense Complet:** Després de contenir l'incident i restaurar la funcionalitat dels sistemes, es realitza una anàlisi forense detallada per comprendre l'abast i la causa de l'incident. Aquesta anàlisi inclou identificar la causa arrel, avaluar l'impacte, capturar evidència digital i documentar els Indicadors de Compromís (IoCs).
- **Informe d'Incident i Lliçons Apreses:** Un cop finalitzada l'anàlisi forense, s'elabora un informe detallat de l'incident que resumeix les troballes clau, les accions de contenció, l'impacte en els serveis crítics, l'efectivitat de les mesures de resposta i el temps total de resposta i restauració. Posteriorment, es realitza una sessió de lliçons apreses amb els equips involucrats per identificar punts de millora i àrees on les defenses van funcionar adequadament.
- **Notificació a Parts Interessades:** Depenent de l'incident, pot ser necessari notificar a parts externes com reguladors, clients, proveïdors o el públic, assegurant una comunicació transparent i controlada per evitar danys addicionals a la reputació o conseqüències legals.
- **Definició d'un Pla de Millora Contínua:** Un cop finalitzades les activitats post-incident, es passa a la fase de millora contínua basada en els resultats de l'anàlisi post-incident, alineada amb les millors pràctiques de la indústria com el marc de ciberseguretat del NIST, per enfortir les capacitats de seguretat i reduir la probabilitat i l'impacte de futurs incidents.