PLA DE GESTIÓ DE CIBERINCIDENTS

Localret

Amb la participació de:

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Agraïments

Aquest document és fruit d'un procés col·laboratiu d'anàlisi, reflexió i diàleg, al voltant de la resposta davant d'escenaris de cibercrisi. El grup de treball que ha treballat aquesta iniciativa està vinculat a l'Eix 2: Infraestructures Digitals i Ciberseguretat de l'Agenda Digital dels Municipis de Catalunya, iniciativa que s'emmarca en l'estratègia del municipi digital i que el Consorci Localret du a terme amb la finalitat d'acompanyar els ajuntaments en la seva transformació digital.

El grup de treball Eix 1 – Protocol cibercrisi ha treballat en 2 documents:

- Pla de gestió de ciberincidents
- Protocol breu davant d'un incident de ciberseguretat

El present document ha estat elaborat pel Consorci Localret i ha comptat amb la participació i col·laboració de professionals que formen part de l'Ajuntament de Vilafranca del Penedès, l'Ajuntament de Lleida, l'Ajuntament de Rubí, l'Ajuntament de Terrassa, Ajuntament de Sant Cugat del Vallès, l'Ajuntament de Tarragona, l'Ajuntament de Reus, l'Ajuntament de Calonge i Sant Antoni, l'Ajuntament de Bellpuig i l'Ajuntament de Cornellà de Llobregat.

També hi ha participat amb les seves indicacions i/o recomanacions l'Agència de Ciberseguretat de Catalunya.

Data d'elaboració: Octubre de 2023

agenda digital dels municipis de Catalunya

Índex

1 Introducció

El present document respon a la necessitat de l'Ajuntament de XXXXXX de complir amb els requisits de disposar d'un pla de gestió davant possibles incidents de seguretat de la informació en els sistemes d'informació de la Corporació.

La gestió de la ciberseguretat, com a tasca clau per a la prevenció proactiva, requereix de l'establiment d'un marc de governança, en el que es designin als organismes o unitats responsables d'aquesta gestió i es defineixen clarament les seves competències en aquest àmbit, que haurien de ser conegudes per tota l'organització.

La inversió en ciberseguretat ha de ser una prioritat per a les entitats. Donat l'increment de freqüència dels ciberatacs i el gran impacte que tenen, tant en l'afectació al servei prestat com a salvaguarda de la informació i reputació de la pròpia entitat, no ha d'existir cap dubte a emprendre-la. En aquest context, cal disposar de sistemes que, alhora que protegeixen, facilitin la gestió davant un atac així com una renovació tecnològica constant, a més de promoure una cultura a l'organització conscient i competent en matèria de seguretat de la informació.

En segon lloc, i encara que la component de sistemes és necessària, no és suficient, havent de ser complementada amb la disponibilitat de recursos humans per a la supervisió permanent de l'ecosistema, siguin equips constituïts amb personal propi, extern o una barreja de tots dos.

Tot i això, hi ha ciberincidents que deriven o evolucionen cap al que cal qualificar de crisi pel seu impacte real o potencial, i per això cal preparar-se també amb antelació.

2 Què s'entén per Cibercrisi

Per crisi s'entén qualsevol situació que quan passa genera un gran impacte i els efectes del qual perduren en el temps.

Un ciberincident pot esdevenir una cibercrisi quan el seu impacte a l'organització és prou elevat com per causar un denegació importants dels serveis que presta, afectant-ne a la seva imatge pública i a la ciutadania en general, o a una part d'ella.

Cal donar especial importància a la ciberseguretat per la gran dependència que té l'organització dels sistemes informàtics tant per a les seves tasques i operativa interna com per a la prestació de serveis als ciutadans i a altres administracions públiques.

Cal posar en perspectiva que els sistemes informàtics, tot i les mesures de seguretat, les barreres i salvaguardes que s'hi implementen, sempre estan exposats a possibles ciberincidents que en poden degradar o discontinuar el servei.

En tot cas, cal gestionar les amenaces o circumstàncies abans, durant i després que es produeixin, tenint clar que no cal que hi hagi un problema real per trobar-se en una situació de crisi. Només cal que qualsevol rumor o esdeveniment transcendeixi a l'opinió pública perquè s'acceleri el procés i, fins i tot, i donat el moment actual de les xarxes socials, es propagui sense control, fent estendre el pànic entre els grups d'interès de l'organització. Això farà que la gestió de crisis es dificulti encara més.

La gestió de tota mena de crisis és una disciplina que ha tingut un important desenvolupament en la darrera dècada i des de molt diferents camps, particularment els relacionats amb la Seguretat de la Informació (SGSI) i la Comunicació. En tractar-se de situacions de gravetat especial, que pot arribar a comprometre, no només el funcionament de l'organització, sinó fins i tot el seu funcionament futur, aquesta gestió ha passat a ser cada vegada més una capacitat imprescindible per a un número creixent d'organitzacions. Entre els molts factors que han propiciat el seu desenvolupament cal destacar, entre d'altres, la major exigència quant a la prestació de servei, l'increment de la responsabilitat social i l'impacte potencial de les xarxes socials sobre la reputació i la imatge.

Tota crisi implica una presa de decisions sota pressió, **amb temps i informació limitats i en diversos fronts en paral·lel, i amb molts agents i persones intervenint-hi**.

Amb independència de l'origen que causi la crisi, es fa palesa la component de gestió que la resolució implica. Per això, l'organització afectada necessita haver-se dotat de les capacitats i estructures de gestió adequades que li han de permetre abordar-la amb garanties d'èxit.

3 Aspectes clau en la gestió dels ciberincidents

Les capacitats i estructures de gestió necessàries per fer front a una crisi no s'improvisen quan aquesta apareix, és imprescindible desenvolupar-les amb antelació, per disposar de la preparació necessària

3.1 Lideratge

És important liderar, prendre i mantenir la iniciativa durant la crisi i, si aquesta es perd, cercar les oportunitats que permetin recuperar-la. Prendre mesures raonables és gairebé sempre millor que no fer res; això sí, partint d'una preparació i un Pla prèviament acordat. Serà més fàcil adoptar les mesures oportunes en un breu període de temps (que sol ser habitual en aquestes situacions) si hi ha algun tipus de treball previ que si no n'hi ha.

La presa de decisions ha de partir de la direcció de l'organització que és la única que té la capacitat d'assegurar els recursos materials i humans necessaris i dels diferents nivells de presa de decisions. En el cas dels ciberincidents, és fonamental la funció de **Responsable de Seguretat** de la Informació, que serà el primer en categoritzar el dany i, en funció de la categoria de l'incident, convocar o no el **Comitè de Cibercrisi**, assumint que la ràpida notificació del mateix no només beneficia la pròpia Organització, sinó que redunda en un increment de la seguretat general, de sector i del país, per la qual cosa la seva realització és un compromís ètic davant la societat.

3.2 Plans i protocols estructurats

Les crisis es preparen en temps de normalitat. Tot allò que no es prevegi aleshores és pràcticament impossible improvisar-ho durant l'emergència. Una de les claus per a una gestió efectiva de la crisi és determinada per la capacitat d'anticipació i identificació dels àmbits més vulnerables (gestió de riscos) que poden arribar a transformar-se en situacions crítiques. La identificació d'aquests riscos potencials en el funcionament ordinari de la Organització serà clau per, arribat el cas, saber com respondre i reduir-ne l'impacte el màxim possible.

Des d'aquest punt de vista, les ciberamenaces exigeixen un exercici de prospectiva constant per ser conscients de les debilitats de l'organització i, així, poder preparar-se i anticipar-se.

Per tant, és necessari dotar-se dels diferents processos i protocols tècnics i operatius que permetin mitigar el màxim possible l'impacte d'un ciberincident així com disposar dels mecanismes que permetin dotar de major resiliència els serveis de la Corporació.

3.3 Model d'organització per gestionar els ciberincidents

En la gestió d'un ciberincident poden existir diverses esferes d'actuació. Segons el nivell de gravetat del ciberincident caldrà gestionar-lo des de una o més d'aquestes esferes:

- **Organitzativa i estratègica:** en la mesura en què el seu impacte afecta diferents àmbits de l'organització (servei, operativa, imatge i reputació, relació amb el regulador, grups d'interès, presència a xarxes socials, etc.) i requereix una resposta coordinada a alt nivell, determinant els canals de comunicació amb altres unitats o entitats, pròpies i/o alienes. Recau sobre el Comitè de Crisi.
- **Operativa i de resposta tècnica:** per contenir els efectes immediats de la crisi, donar resposta i resoldre'ls de forma definitiva. Aquesta gestió recau sobre l'Equip de Resposta a Incidents de Ciberseguretat (ERIC-TI).
- **Comunicativa:** per liderar i gestionar de forma coordinada la comunicació interna i externa de l'incident. Recau sobre l'Equip de Comunicació (ECIC).

Tot i que en aquest model es descriuen a continuació moltes figures diferents integrant els diversos equips i el comitè de crisi, cal tenir en compte que en molts ajuntament, especialment en els més petits, molts d'aquests rols poden acumular-se en una única persona o equip, o inclús poden haver-hi rols que no ostenti ningú.

Cada ajuntament haurà d'ajustar les directrius d'aquest document en matèria d'organització a la seva realitat, i recordar que el CATALONIA-CERT pot ajudar a suplir les seves carències a l'hora de gestionar un incident amb el seu personal.

3.3.1 Comitè de Crisi

El Comitè de Crisi (també anomenat de Cibercrisi) és el **màxim òrgan decisori** per a la gestió unificada d'una situació de crisi. La seva funció principal serà accelerar el procés de presa de decisions per resoldre incidències, definint les prioritats, establint l'estratègia i la tàctica a seguir. Haurà de fixar els principals escenaris que cal tenir en compte, com actuar i com explicar-ho, dirigint els equips de Resposta a Incidents (ERIC-TI) i de Comunicació (ECIC).

La gestió d'una cibercrisi, encara que l'origen sigui un ciberincident, no és exclusiu de l'equip de seguretat, sinó que **implica tota l'organització**.

3.3.1.1 Funcions

El Comitè de Crisi aporta una visió estratègica i disposa d'una capacitat d'interlocució més gran i de mobilitzar recursos extraordinaris, en cas necessari. Caldrà accelerar el procés de presa de decisions per resoldre incidències, definint les prioritats, establint l'estratègia i la tàctica a seguir. Les seves funcions son:

Funcions del Comitè de Cibercrisi

1. **Assumir l'estat de la situació**
2. **Coordinar i prioritzar les accions de resolució i tornada a la normalitat**
3. **Definir el posicionament comunicatiu de l'Organització**
4. **Coordinar les accions d'anàlisi posterior a l'incident**

1. Comprendre l'estat de situació i fer-ne una previsió d'escenaris.
   - Avaluar tota la informació rebuda sobre l'incident, fer una valoració inicial del seu impacte (real o potencial) i de les conseqüències sobre l'entitat i les parts interessades.
   - Mantenir una previsió de l'impacte potencial i les conseqüències per a l'entitat, considerant els riscos emergents i els escenaris cap a on pot evolucionar per poder fer mesures d'anticipació.
2. Coordinar i prioritzar les accions de resolució i tornada a la normalitat
   - Donar suport als altres equips, sobretot a l'Equip de Resposta a Incidents de Ciberseguretat, que estan sotmesos a molta tensió i pressió.
   - Supervisar les mesures implementades i les decisions preses prèviament pels equips de resposta o altres comitès operatius, assegurant que els procediments posats en marxa per a la resolució són els més eficaços i eficients.
   - Determinar les prioritats per recuperar les activitats i serveis en el menor temps possible.
   - Activar la mobilització de recursos extraordinaris quan calgui.
   - Fer un seguiment dels punts oberts, per exemple, mitjançant un document de "Notes i Acords".
   - Actuar com a centre de referència de informació durant la resposta al incident i la seva posterior recuperació, tant davant dels agents interns com a externs (Administració i altres) involucrats o concernits per l'incident.
   - Assegurar les relacions i la interlocució amb totes les parts interessades.
3. Definir el posicionament comunicatiu de l'entitat.
   - Definir l'estratègia de comunicació interna i externa, en base a la seva missió, el seu propòsit i els seus valors.

- Designar el portaveu i assegurar que es duen a terme les mesures de comunicació prèviament dissenyades, ja sigui en mitjans, xarxes socials, marcs associatius, etc.
- Vetllar per salvaguardar la confiança, la reputació i la imatge.

4. Coordinar les accions d'anàlisi posterior a l'incident.
   - Extreure lliçons apreses i elements de millora.
   - Assegurar que es duu a terme el Pla de Acció resultant.

3.3.1.2 Composició

La composició serà un grup de persones amb diferents perfils, executives i molt resolutives, amb capacitat de reacció davant de situacions d'estrès i agilitat en la direcció dels equips i presa de decisions.

Per assegurar l'èxit de la gestió de l'incident, resulta necessari garantir que entre els membres participants es disposa de la capacitat d'assumir decisions sovint crítiques i amb molta rellevància de cara als propis processos de negoci. No obstant això, la coordinació i conducció del propi comitè normalment la porta a terme el "gestor de la crisi" (o incident handler), en funció de la component tècnica i de la resta de circumstàncies, com ara la disponibilitat dels principals processos de negoci, la estratègia comunicativa, etc.
Amb ells haurien tenir representació cadascuna de les àrees bàsiques de l'organització, perquè la gestió d'una crisi, encara que l'origen sigui un ciberincident, no és exclusiu de l'equip de seguretat, sinó que implica tota l'organització.
La composició d'aquest Comitè pot variar depenent de les característiques de cada crisi, però, en general, estarà composat per les persones següents:

Composició	Funcions
Alcalde/ssa *Suplent :* ***Primer tinent/a d'Alcaldia o Regidor/a en qui delegui***	• Presideix el Comitè de crisi acordat • Designar altres membres al Comitè • Delega responsabilitats • Es manté permanentment informat • Assumir la interlocució al més al nivell i representar a l'Ajuntament. • Mantenir informats als membres de la Junta de Govern i del Ple Municipal • Actua com a portaveu si les circumstàncies ho exigeixen
Cap de Gabinet de l'Alcaldia	• Assisteix a l'Alcalde/sa.
Secretari/a municipal *Suplent :* ***Oficial/a Major***	• Preparar assumptes a ser inclosos en l'ordre del dia de les sessions del Comitè • Assistència i aixecament d'actes de les sessions. • Recollida d'informació i decisions acordades

	• Donar seguiment a les accions a seguir de acord a les lleis que apliquin. • Actuar com a fedatari en la formalització de contractes, convenis i documents en els que intervingui l'Ajuntament, com aquells subscrits amb tercers proveïdors -públics o privats- de serveis dirigits a garantir la resolució de l'incident. • Disposar que es publiquin, quan sigui preceptiu i en la mesura que sigui possible, els actes i acords, en els mitjans oficials de publicitat. • Dirigir el registre i arxiu de la Corporació. • Conèixer dades afectades des del punt de vista de servei • Notifica a les autoritats pertinents
Gerència Municipal (Coordinador/a general o caps d'Àrea/Servei que correspongui)	• Acompanyen i donen suport, en l'àmbit respectiu de les seves responsabilitats al Comitè de Cibercrisi.
Responsable de Serveis Jurídics	• Analitzar la responsabilitat legal provocada per l'incident i orienta sobre els assumptes legals. • Preparació informes jurídics vers companyies asseguradores
Cap de Servei TIC *Suplent :* ***Cap de gestió infraestructures, sistemes i operacions TIC***	• **Actua com a coordinador del Comitè** • Coordinar l'equip **intern** de resposta a l'incident • Nomenament responsable operatiu o gestor del ciberincident. • Enllaç entre el comitè de crisi i l'equip tècnic i equip de resposta a l'incident • Assegura la disponibilitat de les còpies de seguretat segons la política de còpies. • Contractarà de forma ràpida servidors virtuals si fos necessari. • Preparar i canalitzar la informació sobre l'estat de situació i pla d'acció en curs i previst.
Responsable de Seguretat de la Informació	• És el primer coneixedor de l'incident i determina si cal traslladar-lo o no al Comitè de Crisi. • **Activar i desactivar el comitè de cibercrisi** • **Inicia la gestió de crisi** • Notifica de forma immediata al CERT de referència.
Inspector/a en cap de la Policia Local	• Suport en la comunicació i coordinació dels cossos de seguretat supramunicipals, en la denúncia i investigació i resolució del ciberincident
Cap de Comunicació Corporativa **Cap de Premsa** *Suplent :* **Tècnic de Comunicació Designat**	• Definir el pla de comunicació externa i interna i amb grups d'interès, **conjuntament** amb el Servei de Comunicació de l'Agència de Ciberseguretat de Catalunya • Gestionar relació amb els mitjans, els canals, xarxes socials, etc • Definir quins són els missatges clau, el format i el canal més adequat, en funció dels grups d'interès. • Seguiment i repercussió de la crisi als diferents mitjans de comunicació i xarxes socials. • Ajuda a la preparació del portaveu. • Vetllar per la proactivitat en relació a les parts interessades. • Assegurar que el que es comunica al personal de la Corporació està perfectament alineat amb els missatges i explicacions cap a l'exterior.
Delegat/da de Protecció de Dades	• Assessora al Comitè de Crisi en l'àmbit de la seva competència, amb veu sense vot

	• Si afecta a dades personals, inici d'expedient de l'incident a APDCat dins les 72 h d'inici de l'incident, i responsabilitzar-se del mateix fins la finalització. • Supervisar l'acompliment de lo disposat en la normativa vigent. • Cooperar amb les autoritats de control (APDCat) • Actuar com a punt de contacte de l'autoritat de control.
Secretari de Telecomunicacions i Transformació Digital de la Generalitat de Catalunya **Director/a General de l'Agència de Ciberseguretat de Catalunya** **Director/a del CATALONIA-CERT** **Responsable del CATALONIA-CERT** **Responsable de Comunicació de l'Agència de Ciberseguretat de Catalunya**	• Determinaran l'estratègia i les accions a prendre en l'àmbit de la Ciberseguretat, per a una resolució eficaç i efectiva del ciberincident • Lidera les reunions de seguiment tàctica i estratègica del Ciberincident • Conjuntament amb els equips interns, donarà suport a la realització de les tasques tècniques associades a la investigació • Acompanyen i es coordina l'actuació, comunicació i suport institucional al Comitè de crisi.
(segons impacte en àmbits de negoci)	• Acompanyen i donen suport, en l'àmbit respectiu de les seves responsabilitats, al Comitè de Cibercrisi.
Cap de gestió infraestructures, sistemes i operacions TIC *Suplent :* ***Enginyer Sistemes***	• Garanteix la continuïtat del servei utilitzant, arribat el cas, un centre altern des d'on s'opera amb els serveis crítics • Prevenir, gestionar i respondre eficaçment als incidents. • Actuacions de contenció, erradicació i recuperació de xarxes, sistemes i serveis. • Revisa l'entorn comú a totes les aplicacions així com els específics de cada aplicació • Comunicar i coordinar-se amb el CERT de referència. • Assegurar accions d'investigació i cooperació efectiva.
Cap administratiu/va TIC	• Suport administratiu, en funcions de secretaria de Comitè de Crisi. Elaboració d'actes i informes derivats de la Coordinació d'actuacions i informe del ciberincident.

Tots els membres del Comitè de Crisi poden delegar en altres persones de la Organització, però continuaran assumint la responsabilitat de les decisions que es prenguin en el seu nom.

Els membres del Comitè de Cibercrisi mantindran sempre sota el seu control, una còpia EN PAPER del ***Pla de gestió de ciberincidents***.
En el ***Pla de gestió de ciberincidents*** hi haurà una annex amb les dades de contacte actualitzades (telèfons, correu electrònic, etc...) de tots els membres del Comitè i dels seus suplents.

3.3.1.3 Activació del comitè

El/la Responsable de Seguretat, l'Alcalde/ssa i el/la Regidor/a de Tecnologia tenen potestat per activar el Comitè de Cibercrisi.

Es convocarà després d'haver realitzar l'avaluació i classificació del ciberincident segons els criteris definits a la Guía CCN-STIC 817. Esquema Nacional de Seguridad. Gestión de ciberincidentes i haver definit que segons aquesta guia l'incident és de nivell alt, molt alt o crític (el que en aquest pla de gestió s'ha anomenat com a incident greu).

3.3.1.4 Dinàmica de les reunions

Convocatòria del comitè

La convocatòria de les reunions es farà per algun (o tots) dels següents mitjans:

1. Correu electrònic corporatiu
2. Aplicació de missatgeria corporativa
3. Trucada telefònica

Localització de les reunions del comitè

S'ha de determinar la sala de reunions o espai on es produiran les reunions presencials del comitè. Les reunions seran preferiblement presencials, però alternativament, davant una impossibilitat d'algun dels membres, i sempre que es disposi dels mitjans telemàtics operatius, podrà ser híbrida o per videoconferència.

Primera reunió

La reunió s'ha de fer amb la major brevetat possible (amb titulars o suplents) amb els següents objectius :

- Assumir les funcions encomanades
- Prendre el control de la situació
- Emprendre el procés formal de presa de decisions per a la gestió de la cibercrisi.
- Definir el pla de resposta a aplicar segons la classificació del incident.
- A la vista de la gravetat del incident i les possibles afectacions, es determinarà la periodicitat de les successives reunions i si cal convocar a alguna persona més a les properes reunions
- Activar els grups de treball
    - **Equip de Resposta a Incidents de Ciberseguretat (ERIC-TI)** amb el Responsable de seguretat, responsables de sistemes TIC, representants del CATALONIA-CERT així com especialistes interns i externs.

- **Equips de Comunicació d'Incidents de Ciberseguretat (ECIC)**, amb el/la Cap de Gabinet Alcaldia o en qui delegui, Responsable de Comunicació i Premsa, així com especialistes interns i externs, inclosos els del CATALONIA-CERT.

Agenda de les reunions

Cal una proposta d'agenda i temes a tractar a les diferents reunions del Comitè perquè sigui dinàmica i ajudi a la presa decisions. Un exemple seria el següent:

- Estimació de la durada de la reunió
- Revisió dels fets i actualització de la informació del incident. Quins fets ha produït l'incident fins al moment? Quines accions s'han pres i quin efecte han tingut?
- Comprovació de l'estat d'execució del Pla de Resposta.
- Rols Repàs de les funcions de cada membre, assignar les següents accions a executar als responsables corresponents clarificar les qüestions de coordinació entre ells.
- Fixar quan es realitzarà la propera reunió, i concretar aspectes a incloure-hi. La periodicitat de les reunions pot variar segons la fase del ciberincident i el seu impacte en l'organització. En els moments de major impacte és habitual que les reunions del Comitè es produeixin cada poques hores, per tal de tenir un punt de control informatiu actualitzat de com es desenvolupa l'incident.

Registre del ciberincident

És important registrar de forma contínua el desenvolupament del ciberincident. Tant els fets que produeixi el propi atac i les seves conseqüències, com les decisions que prengui el Comitè i els seus efectes. Aquesta informació serà molt útil tant en el moment de gestionar la crisi, com en l'anàlisi posterior en la fase de tancament.

Temps entre reunions

En el període de temps entre reunions, els membres del Comitè han de executar les tasques del Pla de Resposta que els hi hagin sigut assignades a l'anterior reunió, així com d'altres que estimin oportunes si les circumstàncies immediates ho requereixen. Al mateix temps han de fer arribar en temps real al coordinador del Comitè la informació que vagin recopilant de la situació.

3.3.1.5 Tancament i desactivació del comitè

Un pla de crisi pot no perseguir necessàriament restituir els serveis de forma segura com més aviat millor, operant al 100%, sinó a restituir-los de forma segura a uns nivells acordats, és a dir, es podria assumir treballar un temps de manera segura en mode degradat/precari però raonable.
En aquest cas, un cop superada la crisi, cal que es disposi d'un pla de tornada a la normalitat des de l'operativa de recuperació (post mitigació i contenció) acordat pel comitè.

La tornada a la normalitat pot allargar-se al temps i en aquest cas pot plantejar-se la desactivació del Comitè de Crisi com una de les accions necessàries, però no l'única; ja que el tancament de les crisis requereix un treball programat i estructurat que segueix implicant diferents parts de l'organització.
Es pot decidir la desactivació del Comitè si es compleixen els següents criteris:

- Si l'Equip de Resposta a Incidents de Ciberseguretat pot continuar treballant sense el suport del Comitè.
- Si ja no és necessària la implicació del personal del Comitè i les tasques pendents poden ser executades per altres persones dels seus respectius equips.
- Si es disposa d'un pla d'acció que garanteix que tots els temes oberts són tractats adequadament.

Independentment que s'hagi desconvocat el Comitè, el seu **Coordinador** ha de vetllar per:

- El correcte arxiu de la informació generada durant l'incident, prestant especial atenció a la informació que pugui ser d'utilitat a serveis jurídics en els mesos següents
- La realització de l'anàlisi post crisi i l'adopció de les lliçons apreses, vetllant especialment per les mesures de seguretat de la informació.

3.3.2 Equip de Resposta a Incidents de Ciberseguretat (ERIC-TI)

Aquest és l'equip operatiu i representa el nivell tàctic de la gestió dels ciberincidents. És l'encarregat de prevenir, gestionar i respondre a nivell tècnic als ciberincidents, realitzant les accions orientades a la contenció, erradicació i recuperació dels equips, xarxes i sistemes vulnerats.

Aquest equip està format habitualment pels següents membres:

- Responsable de Seguretat de la Informació de l'Ajuntament (CISO)
- Responsable de Sistemes TI de l'Ajuntament (CTO)
- Altres especialistes TI interns o externs a l'Ajuntament que el Responsable de Seguretat determini.
- **Gestor de la crisi** (o '*incident handler*', en anglès): sense esdevenir una funció en si, és un rol clau a tenir en compte. És la persona que **lidera com a facilitador** la coordinació dels elements que composen **la gestió de la crisi** (sigui un incident o una amenaça). Serà assumit per un integrant de la funció de Resposta a Incidents (habitualment el CISO o CTO) o en qui es decideixi delegar.
- En els casos d'incidents greus, representants del CATALONIA-CERT de l'Agència de Ciberseguretat.

Aquest equip estarà liderat pel Responsable de Seguretat i el Responsable de Sistemes.

3.3.3 Equip de Comunicació d'Incidents de Ciberseguretat (ECIC)

És l'equip que ha de gestionar la comunicació tant interna com externa que es derivi de la cibercrisi, liderant-la en tot moment per a que la informació que es faci pública de la cibercrisi sempre tingui com a origen la nostra Organització.

Aquest equip està format habitualment pels següents membres:

- Cap de Gabinet d'Alcaldia o similar
- Cap de Comunicació
- Altres especialistes interns o externs a l'Ajuntament que el/la Cap de Comunicació determini
- En els casos d'incidents greus, Responsable de Comunicació de l'Agència de Ciberseguretat de Catalunya.

3.3.4 Coordinació

La coordinació és indispensable en la gestió dels ciberincidents. Una falta de coordinació en la presa de decisions organitzatives, tècniques o comunicatives així com en la seva execució, pot tenir efectes fatídics en la resolució de la crisi.

És important aplicar tots els esforços necessaris per a que la gestió del ciberincident sempre es realitzi de forma coordinada entre els diferents actors que hi participen.

Si el ciberincident en qüestió ha implicat la convocatòria del Comitè de Crisi, serà aquest òrgan l'encarregat de centralitzar i coordinar totes les decisions durant la gestió del incident.
En cas de no existir convocatòria del Comitè, serà la figura del **Responsable de Seguretat** l'encarregada de dur a terme i assegurar la correcta coordinació entre els diferents actors que si estiguin involucrats.

3.3.5 Grups d'interès

Els grups d'interès són persones o col·lectius de l'entorn de l'organització que es poden veure afectats per qualsevol activitat que aquesta realitzi.
Durant una cibercrisi és molt probable que hi hagi interacció amb algun, per ser part activa de la situació o fins i tot per ser part, tant o més afectada, que la pròpia organització.

La gestió de les parts interessades, afectades o no, és un dels pilars de la gestió dels ciberincidents. Totes les parts han de fer esforços per entendre quina la situació, on és el llindar mínim de responsabilitat que correspon a cadascú i comprometre's a assumir-la, així com disposar o crear ad-hoc els canals àgils i clars d'interlocució per pilotar la tornada a la normalitat.

La següent és una llista no tancada dels grups d'interès típics en el cas de les administracions locals:

Grup	Membres
Interns	Regidors/es del govern i de l'oposició Direcció de l'organització (directors d'àrea, de serveis, de les empreses municipals en cas d'haver-hi) Serveis jurídics Delegat/da de Protecció de Dades Empleats actuals i anteriors Recursos Humans Representants sindicals Policia Municipal
Tercers	Autoritats i Governs Altres AAPP amb qui hagi relació (DGCadastre, DGT, INE,...) Organismes reguladors i supervisors Ciutadania, públic en general Inversors Associacions Companyies d'assegurances Altres proveïdors afectats per la crisi
Mitjans de comunicació	Xarxes socials corporatives Mitjans on-line Mitjans tradicionals
Autoritats competents	CERT o CSIRT de referència (CATALONIA-CERT, CCN-CERT) Autoritat Catalana i Espanyola de Protecció de Dades Cossos de seguretat supramunicipals (Mossos d'Esquadra, Policia Nacional)
Proveïdors rellevants (aquells que tenen un paper rellevant en la gestió del ciberincident)	Backup, Emmagatzematge Infraestructura Comunicacions

La dependència de la cadena de subministrament és una cosa que s'ha d'estudiar i, en determinats casos, exigir certificacions o garanties als proveïdors, tant públics com privats, respecte a la seva protecció davant de ciberatacs.

Entre els proveïdors públics es troben els serveis electrònics que proveeixi a l'Ajuntament el Consell Comarcal i la Diputació corresponents, la Generalitat de Catalunya o l'Administració General de l'Estat. Entre els proveïdors privats es troben tots els proveïdors tecnològics de software, hardware, serveis i telecomunicacions entre d'altres.

És recomanable fer un llistat de tots els proveïdors que formen la cadena de subministrament de la nostra organització per tal d'exigir-los les certificacions o garanties corresponents, com per exemple el compliment de l'ENS o de la ISO 27001.

4 Fases d'un ciberincident

La gestió de ciberincidents consta de diverses fases durant el seu cicle de vida :

PREPARACIÓ	Fase prèvia al ciberincident en la que l'organització ha de preparar-se pel que pugui succeir. Una bona anticipació i entrenament previ són claus per realitzar després una gestió eficaç del incident, pel que fan falta tres pilars fonamentals: persones, procediments i tecnologia.
IDENTIFICACIÓ I ANÀLISI	Fase inicial en que es detecta el ciberincident i es classifica la seva tipologia i el seu grau d'afectació per a decidir el pla de resposta a adoptar. Si l'incident s'ha categoritzat com a greu, s'activarà el Comitè de Crisi. Es comunica a les autoritats competents que correspongui.
REMEDIACIÓ DE L'INCIDENT	Atenent l'estratègia definida en la fase anterior, es determinaran les fases adreçades a, en primera instància a contenir l'incident per mitigar-ne l'impacte, procedint després a la seva eliminació dels sistemes afectats i tractant finalment de recuperar el sistema al mode de funcionament normal. Durant aquesta fase caldrà, cíclicament, persistir en l'anàlisi de l'amenaça, dels resultats de la qual es desprendran, paulatinament, nous mecanismes de contenció i erradicació
TANCAMENT	En aquesta fase final es certifica el tancament del ciberincident, es dissol el comitè de crisi si n'hi ha hagut, i es realitza un informe post-crisi per analitzar les causes de l'incident, extraure'n lliçons i fer propostes de millora de cara al futur.

Tot i que les fases exposades són més o menys seqüencials, és possible que en alguns moments de la gestió d'un incident dues o més fases s'executin de forma simultània.

A continuació es descriuen amb més detall aquestes fases i processos genèrics a contemplar en la gestió de qualsevol ciberincident. Als annexos del present pla es detallen els protocols tècnics específics a aplicar per a cada tipus concret de ciberincident.

4.1 Preparació

1) Identificar i desplegar les mesures de seguretat adients per assolir un grau de protecció dels sistemes d'informació adequat, atenent al disposat als annexos I i II del ENS.
2) Realitzar anàlisi de riscos que permeti disposar d'un pla de tractament de riscos que permeti controlar-los podent ser mitigats, transferits o acceptats.
3) Crear l'Equip de Resposta a Incidents de Ciberseguretat (ERIC-TI) que gestionarà la part operativa i de resposta tècnica dels incidents, ja sigui amb personal intern, extern, o mixt.
4) Formació de l'equip humà per millorar les capacitats tècniques i operatives.
5) Execució de ciberexercicis per entrenar les capacitats i procediments tècnics, operatius, de gestió i coordinació.
6) Disposar d'informació actualitzada de contacte, tant de personal intern com a extern, a implicar en altres fases de gestió del ciberincident, així com les diferents vies de contacte disponibles en cada cas.
7) Dissenyar i aprovar els protocols tècnics i operatius de resposta a ciberincidents
8) Mantenir les polítiques i procediments actualitzats. Especialment tots els relatius a gestió d'incidents, recollida d'evidències, anàlisi forense o recuperació de sistemes.
9) Disposar de les eines que cal utilitzar en totes les fases de gestió d'un ciberincident.
10) Desplegament de les eines de detecció i configuració detallada dels seus paràmetres per disposar d'una capacitat de detecció adequada.
11) Conscienciar recurrentment als usuaris finals de la necessitat i obligació de notificar immediatament qualsevol activitat sospitosa que detectin al personal de TI.

4.2 Identificació i Anàlisi

4.2.1 Detectar

La detecció d'un ciberincident es pot produir a través de diferents fonts: notificacions de les persones (usuaris finals, tècnics interns o externs), alertes dels sistemes de detecció automàtics, o per una auditoria dels sistemes.

Una bona capacitat de detecció es basa en els principis següents:

1) Registrar i monitoritzar els esdeveniments de les xarxes, sistemes i aplicacions mitjançant totes les eines necessàries que automatitzin aquesta tasca i correlacionin aquests esdeveniments per detectar anomalies i descobrir ciberincidents.
2) Protocol d'escalat una vegada es detecta
3) Compartir informació amb altres equips interns i externs de forma bidireccional per millorar les capacitats de detecció.
4) Informar en el mateix sentit a les empreses proveïdores externes.

4.2.2 Identificar i Analitzar

Aquesta fase la pot dur a terme el Responsable de Sistemes (RSIS, CTO) o el Responsable de Seguretat (RSEG), o els membres dels seus equips.
L'equip de seguretat de l'Ajuntament ha de fer un triatge de les notificacions i alertes rebudes, ja que poden existir falsos positius que no indiquin un ciberincident real. En cas de que el ciberincident sigui real, es passa a la següent fase d'identificació i anàlisi.
Es determinaran els següents aspectes de l'incident:

1) **Identificador**: Durant el registre del ciberincident, s'assignarà al cas un identificador que estarà present en totes les comunicacions (correus-e, etc) i tasques associades per facilitar el seguiment i traçabilitat del ciberincident.
   Aquest identificador pot ser creat per l'Ajuntament en base a la nomenclatura que decideixi, com per exemple la del seu sistema de ticketing. No obstant, es recomana enviar un correu al CATALONIA-CERT a l'adreça cert@ciberseguretat.cat amb els primers detalls de l'anàlisi de l'incident. Aquesta bústia retornarà automàticament un correu amb un codi d'identificació per aquest ciberincident, que és el que farà servir el CATALONIA-CERT durant tota la gestió del mateix, i que l'Ajuntament també pot fer servir.
   D'aquesta manera l'Ajuntament i el CATALONIA-CERT faran servir el mateix codi per identificar el ciberincident, simplificant la comunicació, i a més l'Ajuntament compleix amb la petició del CATALONIA-CERT de notificar-li tots els ciberincidents.
2) **Classificació:** es determinarà la tipologia de l'incident en base a les Guia 817 del CCN-CERT (taula 1 de l'apartat 4.1) per determinar el **Tipus d'atac**.
3) **Nivell de perillositat:** segons la guia 817 del CCN-CERT. A la columna de govern local de la taula 3, apartat 4.3 de la guia 817, es determinarà el nivell de perillositat de l'incident, dels 5 que proposa la guia, en funció de la tipologia que s'hagi obtingut a l'apartat anterior.
4) **Nivell d'impacte**: segons la guia 817 del CCN-CERT. A la taula 4, apartat 4.4 de la guia 817, es troben els criteris per determinar el nivell d'impacte del ciberincident dels 5 que proposa la guia.
5) **Priorització de l'incident:** d'entre el grau de perillositat i el grau d'impacte que s'hagin determinat per aquest ciberincident als apartats anteriors, s'escollirà el de major nivell per a representar el nivell d'afectació de l'incident de cara a les notificacions amb el CCN-CERT. Per exemple, si el incident té una perillositat mitja, però un impacte molt alt, el nivell d'afectació serà molt alt segons metodologia del CCN-CERT.
   Aquest pla de gestió proposa **resumir els 5 nivells del CCN-CERT en dos**, per a fer una gestió més simple i fàcil d'executar. Així doncs, els nivells del CCN-CERT Baix o Mitjà es definiran com un Incident Lleu, i els nivells Alt, Molt Alt i Crític del CCN-CERT es definiran com a Incident Greu.

Nivell risc CCN-CERT	Correspondència en aquest pla de gestió
Crític	Incident Greu
Molt Alt	
Alt	
Mitjà	Incident Lleu
Baix	

En funció del nivell del ciberincident, lleu o greu, es seguirà un pla d'acció diferent, tal com es descriu als següents apartats.

Cal tenir en compte que conformi avanci l'anàlisi de l'incident i es coneguin més detalls del mateix, el nivell de priorització pot variar (normalment de lleu a greu) i per tant també el pla d'acció a aplicar.

També és possible que el Responsable de Seguretat, tot i que un incident sigui classificat com a lleu segons els paràmetres indicats anteriorment, decideixi que concorren altres circumstàncies que recomanin classificar-lo com a greu per a fer una gestió més completa del mateix.

4.2.3 Informar

En cas que el Responsable de Seguretat de l'ajuntament no hagi estat informat prèviament del ciberincident, se l'informarà del mateix immediatament, facilitant-li tota la informació recopilada fins al moment a les fases prèvies: evidències de la detecció, classificació, accions de contenció executades, etc...

El Responsable de Seguretat revisarà aquesta informació i la classificació de l'incident, si no és que l'ha dut a terme ell mateix, i en cas d'incident de categoria greu convocarà al Comitè de Crisi.

Independentment de quin sigui el nivell de l'incident, hi ha una sèrie de notificacions que tots els organismes del Sector Públic estan obligats a fer en determinats casos, reglades en la seva forma i contingut, que són les següents:

1. **CCN-CERT/CATALONIA-CERT:** segons dicta el ENS en la seva instrucció tècnica de seguretat de notificació d'incidents de seguretat, és obligatori notificar immediatament al CCN-CERT de tots els ciberincidents de grau Alt, Molt Alt o Crític. Aquesta notificació es pot fer via correu electrònic xifrat o bé amb l'eina LUCIA del propi CCN-CERT (més detalls a Notificación de incidentes i a la guia 817).

Aquest requisit de notificació al CCN-CERT queda substituït en el cas dels organismes catalans per la notificació inicial al CATALONIA-CERT per correu electrònic que s'ha dut a terme a l'apartat anterior (Identificar i Analitzar). Serà el CATALONIA-CERT qui reportarà al CCN-CERT l'incident si ho creu oportú i demanarà més informació a l'ajuntament si fos necessari.

2. **Protecció de dades:** si el ciberincident té afectació a la protecció de dades s'haurà de notificar al/la Delegat/da de Protecció de Dades de l'ajuntament. Aquesta figura serà l'encarregada de decidir si cal fer notificació de l'incident a l'Autoritat Catalana de Protecció de Dades. En cas afirmatiu:
    - Canal: tràmit web (enllaç)
    - Missatge: respondre a les preguntes incloses al formulari de la APDCAT. És probable que en la elaboració de les respostes col·laborin el/la DPO, el/la Responsable de Seguretat i el/la Responsable de Sistemes.
    - Temps: màxim de 72 hores un cop es té constància de l'incident. La APDCAT pot permetre l'ampliació d'aquest marge si es justifica degudament. Després de la notificació inicial és possible que siguin necessàries comunicacions posteriors segons les característiques del ciberincident.
    - Responsable de la comunicació: DPO

3. **Serveis jurídics:** en el cas que es sospiti que el ciberincident suposa un delicte tipificat, cal notificar el cas als Serveis Jurídics de l'Ajuntament per a que avaluï si cal interposar una denúncia davant els cossos de seguretat. Els Mossos d'Esquadra proposen els següents criteris per a decidir si cal o no realitzar una denúncia del ciberincident:
    - S'ha produït algun tipus de perjudici o afectació a l'organisme i aquest es pot quantificar (i justificar)
    - Hi ha indicis o evidències preservades que ens permeti iniciar la corresponent investigació tecnològica
    - Aquests dos criteris són estrictament policials, i els Mossos entenen que hi pot haver d'altres criteris diferents a tenir en compte, com podria ser la precaució de realitzar denúncia per a deixar constància a Mossos des del primer moment, en cas de que el ciberincident tingués conseqüència futures no esperades.

4. **Cossos de Seguretat**: en cas que es determinés amb Serveis Jurídics la necessitat d'interposar denúncia amb els Cossos de Seguretat el procediment és el següent:
    - El Responsable de Seguretat ha d'emetre i signar un informe exposant tots els fets coneguts fins al moment del ciberincident.
    - Una persona amb poders de representació de l'Ajuntament, un lletrat o lletrada de Serveis Jurídics, interposarà la denúncia a Mossos d'Esquadra (es recomana demanar cita prèvia), presentant l'informe tècnic en format físic, així com aportant si cal les evidències electròniques que es creguin oportunes amb un dispositiu extern (pendrive).
    - Si més endavant és necessari es pot realitzar una ampliació de la denúncia aportant la informació i evidències noves que s'hagin trobat.

Tal com es detalla al següent apartat, Remediació de l'incident, a tots els incidents greus i opcionalment als incidents lleus, s'activarà l'equip de Comunicació (ECIC) que executarà les accions comunicatives pertinents per informar als grups d'interès afectats, segons el Protocol de Comunicació que s'annexa a aquest document.

4.3 Remediació de l'incident

El procediment o les passes a seguir per donar resposta a l'incident seran determinades per l'estratègia/pla de resposta, que ha d'aconseguir les fites de contenir l'incident per mitigar les seves conseqüències, erradicar totalment l'actor maliciós dels sistemes afectats, i recuperar els sistemes i serveis fins tornar a una situació de normalitat a l'organització. Tot i això, caldrà tenir presents les premisses generals següents:

1) Seleccionar l'estratègia de resposta en base a les característiques de l'incident, segons l'anàlisi previ, i prioritzant :
    - Protegir la seguretat de les persones
    - Protegir la informació secreta i sensible
    - Protegir la resta de la informació
    - Protegir el hardware i software de l'atac
    - Minimitzar la interrupció dels serveis TI. Sovint mantenir actius els serveis TI que siguin afectats directa o indirectament durant l'atac pot augmentar les conseqüències d'aquest. És per això que minimitzar la interrupció d'aquests serveis tindrà una prioritat relativament baixa
2) Aplicar protocols de resposta i playbooks en base a les característiques de l'incident.
3) Comunicar als grups d'interès afectats.
4) Recopilar i emmagatzemar de manera segura totes les evidències i documentació de l'incident. Aquesta documentació serà bàsica per a anàlisis posteriors de l'incident o per a les corresponents accions legals si s'escauen
5) Realitzar un anàlisi forense
6) Recuperar el sistemes, xarxes i serveis afectats

4.3.1 Remediació d'un incident lleu

Característiques de la remediació d'un incident Lleu:

- El Responsable de Seguretat i el Responsable de Sistemes, com a caps de l'equip de Resposta a Incidents (ERIC-TI) escolliran el procediment de resposta a aplicar segons el tipus de ciberincident. El primer protocol de resposta a aplicar per defecte és el del Procediment TIC de Resposta a Ciberincidents que s'annexa a aquest document. En cas que aquest annex no contempli el tipus de ciberincident que cal tractar, es poden cerca d'altres playbooks de

referència, com els del annex 2 de la guia BP/29 del CCN-CERT. Si no es disposa de cap procediment de resposta adequat al ciberincident a tractar, cal identificar i preparar les mesures per contenir, solucionar i reparar l'afectació.

- L'equip de Resposta a Incidents (ERIC-TI) executarà les accions tècniques del procediment de resposta sota la supervisió/coordinació del Responsable de Seguretat i el Responsable de Sistemes.
- La comunicació en un incident lleu no és sempre és necessària, sinó que dependrà de cada cas. En els casos en que convingui, l'equip de Comunicació (ECIC), executarà les accions comunicatives pertinents per informar als grups d'interès afectats, segons el Protocol de Comunicació que s'annexa a aquest document.
- Durant tota la gestió de l'incident cal recopilar i emmagatzemar de manera segura totes les evidències i documentació de l'incident.
- Si és pertinent, segons criteri del Responsable de Seguretat, es realitzarà un anàlisi forense de l'incident.
- Un cop recuperats els sistemes, xarxes i serveis afectats es pot passar a la fase de tancament del ciberincident.

4.3.2 Remediació d'un incident greu

Característiques de la remediació d'un incident Greu:

- S'activa el Comitè de Crisi, l'equip de Resposta Incidents (ERIC-TI) i l'equip de Comunicació (ECIC).
- L'equip de Resposta a Incidents (ERIC-TI), dirigits pel Responsable de Seguretat i el Responsable de Sistemes, contribuirà amb tota la informació disponible sobre l'incident, en base al seu criteri tècnic, les millores pràctiques en gestió de ciberincidents i les troballes de la investigació forense, per habilitar una presa de decisions informada i justificada per part del Comitè. Així doncs, la gestió tècnica de l'incident, des del propi comitè de crisi, es desenvolupa majorment sobre les recomanacions aportades per l'Equip de Resposta a Incidents.
- Les decisions a nivell estratègic i executiu que afecten al negoci es prenen per part del Comitè de Seguretat, i sovint del propi Responsable de Seguretat, que són els responsables de prendre les decisions finals i d'assumir els riscos corresponents.
- El Responsable de Seguretat i el Responsable de Sistemes, com a caps de l'equip de Resposta a Incidents (ERIC-TI) proposaran al Comitè el procediment de resposta a aplicar segons el tipus de ciberincident. El primer protocol de resposta a aplicar per defecte és el del Procediment TIC de Resposta a Ciberincidents que s'annexa a aquest document. En cas que aquest annex no contempli el tipus de ciberincident que cal tractar, es poden cerca d'altres playbooks de referència, com els del annex 2 de la guia BP/29 del CCN-CERT. Si no es disposa de cap procediment de resposta adequat al ciberincident a tractar, cal identificar i preparar les mesures per contenir, solucionar i reparar l'afectació.
- L'equip de Resposta a Incidents (ERIC-TI) executarà les accions tècniques del procediment de resposta escollit pel Comitè sota la supervisió/coordinació del Responsable de Seguretat i el Responsable de Sistemes.

- El Comitè de Crisi determinarà quina és la informació que es donarà als diferents grups d'interès afectats. L'equip de Comunicació (ECIC) executarà aquestes accions informatives conforme al Protocol de Comunicació annex a aquest document.
- A les diferents reunions del Comitè s'actualitzarà la informació disponible de l'incident, es revisarà l'execució del protocol de resposta i de les accions informatives, i es definiran quines són les properes accions a executar, i qui són els responsables de dur-les a terme.
- Aquest cicle de reunió del Comitè -> execució d'accions -> reunió del Comitè, es repetirà fins a la resolució final de la crisi.
- Durant tota la gestió de l'incident cal recopilar i emmagatzemar de manera segura totes les evidències i documentació de l'incident.
- Es realitzarà un anàlisi forense de l'incident.
- Un cop recuperats els sistemes, xarxes i serveis afectats es pot passar a la fase de tancament del ciberincident.

4.3.3 Diàleg amb l'atacant

Aquest és un punt clau a considerar durant la gestió del ciberincident. Com a norma general:

- L'Ajuntament de XXXXXX, la víctima, no ha de dialogar amb l'atacant.
  Si es compleixen els criteris exposats a l'apartat anterior (Notificacions), posar una denúncia davant les Forces i Cossos de Seguretat de l'Estat (Mossos d'Esquadra generalment).

Actuacions de les autoritats competents:

- FCSE (Mossos d'Esquadra, Policia Nacional, Guàrdia Civil o altres): si s'hagués posat en coneixement, actuaran amb el seu criteri informant l'entitat també en cas de diàleg amb l'atacant.
- CCN-CERT o CERT de referència: actuarà en funció del seu criteri i pràctica, informant a l'Ajuntament, en cas de diàleg amb l'atacant, i si escau, compartir troballes amb altres possibles actors a la investigació.

Si de les actuacions esmentades de les autoritats competents es derivés algun perjudici per a l'Ajuntament de XXXXXX, l'autoritat en qüestió desplegaria les accions necessàries per restaurar o resoldre el problema causat.

4.4 Tancament

Una solució, i el tancament del ciberincident associat, no suposen sempre una resolució satisfactòria del problema. En alguns casos no és possible assolir una solució adequada per diferents raons, com poden ser la manca de resposta per part d'algun implicat o absència d'evidències que permetin identificar l'origen del problema.

El tancament d'incident contempla els següents passos:

1) Determinar el tancament de l'incident, En el cas d'incidents greus serà el comitè de crisi qui determinarà el moment d'aquest tancament. En els incidents lleus serà el Responsable de Seguretat qui el determinarà.
2) Realitzar les comunicacions adients, segons el Protocol de Comunicació annex a aquest document, per informar de la resolució de la crisi als grups d'interès que correspongui, transmetent l'agraïment al personal de la Corporació, als col·laboradors externs que han intervingut i a qui correspongui.
3) Si ja no és necessària la participació del Comitè de Crisi procedir a la seva dissolució (veure criteris de desactivació a l'apartat 3.3.1.5).
4) Realitzar un informe post-crisi, amb un anàlisi en profunditat del desenvolupament de la crisi, causes, quin ha sigut l'impacte a l'organització (reputacional, laboral, legal,...), lliçons apreses i propostes de mesures a implementar per evitar la seva repetició.
5) Reunió del Comitè de Crisi o del Comitè de Seguretat de l'Ajuntament per l'anàlisi de l'informe post-crisi. Revisió, repàs de les lliçons apreses i presa de decisions per implementar les mesures de millora proposades.
6) Actualització dels protocols de resposta/playbooks segons l'experiència guanyada en el ciberincident.

Tenir una informació detallada sobre les causes que han originat una certa activitat maliciosa permet, entre altres coses, ajudar altres afectats a resoldre problemes similars, així com tenir una font de coneixement de la qual es pugui treure'n profit.

5 Serveis Bàsics

Dins l'àmbit de competències de la Corporació i d'acord a la normativa legal aplicable, es determinen els següents serveis com a "bàsics i essencials", i per tant, prioritaris en l'establiment de la contingència per tal de poder-los mantenir operatius, garantint els drets de la Ciutadania i empleats municipals, així com la priorització vers els processos de recuperació i restabliment dels serveis.

1. Serveis socials, vinculats a prestacions garantides
2. Seguretat Ciutadana – Urgències i atenció
3. Recepció de documents al Registre Electrònic General
4. Pagament de la nòmina
5. Padró Municipal Habitants
6. Pagament a proveïdors
7. Tresoreria i recaptació municipal
8. Serveis territorials. Ordenació i tramitació de llicències, inspecció i disciplina.
9. Expedients de contractació administrativa
10. Comptabilitat municipal
11. Suport i assistència òrgans de Govern - Acords, decrets i resolucions
12. Accés a Seu Electrònica
13. Consulta expedients serveis jurídics
14. Serveis i instal·lacions esportives

Per tal que l'Ajuntament de XXXXX, sigui el més resilients possible en el cas que el ciberincident impacti a algun dels serveis bàsics considerats per la Corporació, caldrà elaborar el ***Pla de contingència de serveis bàsics***, que s'annexarà al present pla de gestió, per tal de minimitzar l'impacte del ciberincident, i poder continuar garantint el màxim el servei.

Annex I. Referències

1. RD 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat
2. RD 951/2015, de 23 de octubre, de modificació del RD 3/2010, de 8 de gener, pel que es regula l'Esquema Nacional de Seguridad en l'àmbit de l'Administració electrònica.
3. Llei 40/2015, de 1 d'octubre, de Règim Jurídic del Sector Públic.
4. Protocol de resposta a incidents, Agència de Ciberseguretat de Catalunya
5. RD Llei 12/2018, de 7 de setembre, de Seguretat de Xarxes i Sistemes d'Informació.
6. Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.
7. Guia Nacional de Notificació i Gestió de Ciberincidents.
8. Aproximació al Marco de Governança de la Ciberseguretat (CCN).
9. Promptuari de Ciberseguretat per a les Entitats Locals del Centre Criptològic Nacional (CCN) y la Federació Española de Municipis i Províncies (FEMP).
10. CCN-STIC 800 Glossari de termes i abreviatures del ENS.
11. CCN-STIC-801 Responsabilitats i Funcions en l'ENS.
12. CCN-STIC-802 Auditoria de l'ENS.
13. CCN-STIC-803 Valoració de Sistemes en l'ENS.
14. CCN-STIC-804 ENS. Guia de implantació.
15. CCN-STIC-805 Política de Seguretat de la Informació.
16. CCN-STIC-806 Pla d'Adequació a l'ENS.
17. CCN-STIC-808 Verificació de l'acompliment de les mesures de l'ENS.
18. CCN-STIC-809 Declaració, certificació i aprovació provisional de conformitat amb l'ENS i distintius d'acompliment.
19. CCN-STIC-815 Indicadors i mètriques en l'ENS.
20. CCN-STIC-821 Normes de Seguretat en l'ENS.
21. CCN-STIC-822 Procediments de Seguretat.
22. CCN-STIC-882 Guia d'Anàlisis de Riscos per les Entitats Locals.
23. CCN-STIC-883 Guia d'implantació de l'ENS per a Entitats Locals.
24. Guia Nacional de Notificació y Gestió de Ciberincidents aprovat pel Consell Nacional de Ciberseguretat.
25. CCN-STIC 817. Esquema Nacional de Seguretat. Gestió de Ciberincidents.
26. CCN-CERT BP/ 20 Bones Pràctiques en la Gestió de Cibercrisi.
27. CCN-CERT BP/29 Gestió de Crisis por Ciberincidents en Entitats Locals.

Annex II. Protocol breu de resposta a ciberincidents

Tot i que el protocol està identificat i establert en numeració seqüencial, algunes de les fases i actuacions poden executar-se en paral·lel.

En tot cas, qualsevol tasca associada a un incident categoritzat com d'impacte Alt o superior haurà de ser validada pel Comitè de Crisi, prèviament a la seva execució.

Id	Fase	Actor	Activitats
1	Detectar Identificar i Classificar	Equip seguretat TIC	1. Aquesta alerta pot ser rebuda pels diferents sistemes de seguretat i equips de treball associats a la Corporació 2. Es reportarà al Servei TIC, pels canals habilitats 3. Cal autenticar actor que ho comunica 4. Classificar en primera instància la gravetat de la situació per la qual es sospita o es té confirmació que pot esdevenir un incident de seguretat i identificar possibles sistemes afectats
2	Contenir, Informar i Notificar	Equip seguretat TIC	El Responsable de Sistemes, posarà en marxa les mesures tècniques d'urgència, de resposta incidents: 1. No apagar ni reiniciar els equips. No encendre equips apagats. En cas de Ransomware, aïllar els equips de Internet i les xarxes corporatives. 2. Aïllar equips i servidors de fitxers i les bases de dades corporatives i còpies de seguretat. 3. Intentar no donar pistes als atacants. 4. Capturar proves volàtils 5. Classificació i avaluació d'impacte del ciberincident que coordinarà amb el Responsable de Seguretat
2.1	Comunicació i notificació	Equip seguretat TIC	**En cas de ser un incident LLEU:** 1. Informar al Responsable de Seguretat de l'Ens i a la Comissió de seguretat. 2. Notificar al CERT (Centre de resposta a incidents de referència). - **CATALONIA-CERT preferiblement per email: cert@ciberseguretat.cat (Telf. 24x7 900 112 444)** 3. En cas d'afectar a **dades personals, informar al DPD** 4. Prendre mesures correctives als sistemes implicats. **En cas de ser un incident amb impacte GREU:** 5. Informar al Responsable de Seguretat de l'Ens 6. En cas d'afectar a **dades personals, informar al DPD** 7. Notificar al CERT (Centre de resposta a incidents de referència). -

		DPD	**CATALONIA-CERT, preferiblement per telèfon 24x7: 900 112 444. (Email cert@ciberseguretat.cat)** 8. Responsable de seguretat, Convocar el Comitè de Crisi de la Corporació. 9. Aplicació d'accions immediates de contenció 10. Establir Equips de Treball de Resposta a Incidents de Ciberseguretat (ERIC-TI) i de Comunicació de Incidents de Ciberseguretat (ECIC). En cas d'afectar a **dades personals**: 11. DPD avalua l'impacte i si cal procedir o no a la Comunicació a APDCAT 12. Comunicació a l'APDCAT (DPD) https://apdcat.gencat.cat/ca/seu_electrónica/tramits/notificacio/ notificació mitjançant EACAT o a través d'eTram
3.2	Coordinació - Comitè de Crisi	Comitè de Crisi Equip tècnic Equip Comunicació	1. Avaluació del ciberincident 2. Activar el l'equip tècnic (ERIC-TI) i l'equip de comunicació (ECIC) 3. Establir els períodes d'actualització de la informació de l'estat de l'incident per part de l'equip tècnic ERIC-TI 4. Altres equips de treball necessaris per realitzar la contingència de la situació. 5. Coordinar els diferents grup de treball. • **Coordinació Tècnica -** El responsable tècnic de Sistemes, treballà amb el seu equip tècnic **avaluant** i aplicant les actuacions necessàries per restablir els serveis. **Informarà** en la periodicitat establerta, els informes de situació al Comitè o en qui aquest delegui. • **Coordinació de la Comunicació -** El Responsable de Comunicació**,** coordinarà amb la informació que ha rebut del responsable de seguretat, informar al Comitè de Crisi, des de on es determinarà la informació que es donarà a la ciutadania i agents implicats. Coordinació amb l'equip de comunicació del CERT comunicacio@ciberseguretat.cat **(638 687 687)** • **Coordinació d'entorns i implicats** - **El responsable de Seguretat** , o en qui delegui el Comitè, informarà amb caràcter reservat i confidencial, a les entitats a l'entorn directe de l'àmbit afectat per tal d'estar alerta davant possibles propagacions o afectacions derivades de l'incident actiu.
3.3	Gestió de l'incident	Equip Seguretat TIC Equip Forense Equip CERT	1. Aplicar protocols de resposta i playbooks de referència - *Procediment TIC de resposta a ciberincidents* vers a. Actius d'Informació i Xarxa Corporativa b. Comptes d'usuari c. Resiliència infraestructura alternativa

			d. Accessos d'usuaris 2. Anàlisi forense. Recopilar i emmagatzemar de manera segura totes les evidències. a. Detecció; cadena atac amb atributs b. Examinar sistemes de detecció c. Redactar informe forense 3. Analitzar persistència externa-interna
3.4	Recuperació	Equip Seguretat TIC	1. Planificar la restauració 2. Xarxa de quarantena 3. Reconstrucció en entorn segur, prioritzant els serveis essencials
4	Tancament	Tancament	1. Informe tancament incident 2. Dissolució del Comitè de Crisi, si procedeix. 3. Avaluació per la millora tècnics i operativa del pla i protocol de resposta a incidents.

Annex III. Contactes de resposta a un Ciberincident

Aquest annex recull les dades de contacte dels principals agents implicats en la resposta d'un ciberincident, tals com membres del Comitè de Crisi, equips de resposta interns i externs, autoritats a les que cal notificar i proveïdors de serveis de ciberseguretat. És important mantenir aquest llistat actualitzat en tot moment per a poder respondre de forma ràpida i eficaç als ciberincidents.

INTERNS / CORPORATIUS		
Equip	**Contacte**	**Suplent/Complementari**
Alcalde/essa		
Cap de Gabinet d'alcaldia		
Cap de Servei de TI		
Responsable de Seguretat de la Informació		
Responsable de Sistemes		
Secretari/a municipal		
Gerència municipal		
Responsable de Serveis Jurídics		
Delegat/da de Protecció de Dades		
Cap de comunicació i premsa		
Inspector/a al cap de la Policia Local		

AGENTS I INSTITUCIONS		
Equip	**Contacte**	**Suplent/Complementari**
Equip de resposta a incidents (CATALONIA-CERT)		
Equip d'investigació forense (CATALONIA-CERT)		
Proveïdors de serveis de ciberseguretat gestionats		
Equip de comunicació (CATALONIA-CERT)		
Cossos de seguretat (Mossos d'Esquadra)		
APDCAT		

Annex IV. Informe Ciberincident

Núm Incident	*#ID de referència (#Ticket obert)*	Núm Incident CERT	*#ID de ref del CATALONIA-CERT*
Assumpte	*Descripció general de l'incident.*		
Descripció	*Descripció amb detall del succés.*		
Afectat	*Ajuntament de XXXX o organisme autònom o empresa municipal, corresponent*		
Data i hora incident	*Indicar amb la major precisió quan ha passat el ciberincident (dia, hora, min, seg)*	Data i hora detecció incident	*Indicar amb la major precisió quan s'ha detectat*
Classe i taxonomia incident	*S'especificarà: classificació i tipus d'incident.*		
Regulació afectada	*ENS RGPD / NIS / PIC / Altres*		

Recursos afectats i evidències lliurades	*Informació tècnica sobre el Num i tipus d'actius afectats pel ciberincident, incloent adreces IP, sistemes operatius, aplicacions, versions, així com informació que l'usuari o reportador de l'incident aporta o lliura.* *...*
Origen / Causa	*Causa de l'incident si es coneix. (obrir Arxiu sospitós, connexió dispositiu USB, accés pàgina web maliciosa, etc.)* *....*
Impacte Estimat	*Impacte estimat en la entitat, en funció del nivell de afectació del ciberincident.* *...*

EQUIPS I PERSONES PARTICIPANTS

Data	Equip/persona	Data	Equip/Persona

ACTUACIONS/DECISIONS

Data	Equip/Rol	Actuació	Resultat

Adjunts	*Informes, documents, arxius adjunts a l'informe que complementi la informació sobre actuacions i traçabilitat de l'incident.* *...*

TANCAMENT DE L'INCIDENT

Resum de les accions realitzades	*Resum genèric de les accions realitzades per a la:* - *Contenció del ciberincident* - *Erradicació del ciberincident* - *Recuperació dels sistemes afectats* *...*
Lliçons apreses i accions de millora	*Descripció de les lliçons apreses en el ciberincidents i de les accions de millora a executar en el futur per evitar o minimitzar la seva repetició* *...*

Annex V. Protocol de Comunicació

És molt important que a la comunicació d'un crisi, la principal font informació sigui **la pròpia organització**. Si no és així es corre el risc de que altres publiquin informació falsa i que l'Ajuntament vagi a remolc d'aquesta situació.

Perquè això passi és imprescindible que la Corporació sigui **proactiva** i porti la **iniciativa**, encara que sense caure a la precipitació.

A més, és molt important que el Comitè de Crisi fixi:

- **Un portaveu** com únic interlocutor/a entre l'Ajuntament i els grups d'interès identificats, i de forma pública, amb els mitjans de comunicació. Habitualment aquest interlocutor públic serà l'Alcalde/ssa o regidora/a en qui delegui.
- **Missatges** clars dels quals ningú de la organització hauria de sortir-se, per la qual cosa sigui quin fos el format i canal escollit, la informació serà la mateixa, sense caure en contradiccions.

Per tant, en situació de crisi, és necessari establir un grup de treball per a la comunicació als grups d'interès, pels canals establerts i segons el pla de comunicació definit prèviament.

5.1 Aspectes claus de la comunicació

En la comunicació de la crisi cal aplicar els següents principis:

- És molt important que els missatges estiguin basats en els **fets** que s'han produït i en les **decisions** que s'han pres. Mai no s'ha de negar la realitat.
- Els comunicats no poden incloure especulacions, ni voluntarismes ni mentides, que s'acabaran tornant en contra nostre.
- Alguns punts de la crisi és millor no revelar-los, o com a mínim no de forma immediata, pel bé de la resolució de la mateixa. Per exemple, fer pública la crisi massa aviat pot revelar als atacants que els hem descobert, o que el seu atac ha tingut èxit, i dificultar la seva resolució. En cas de no poder comunicar determinats aspectes de la crisi, no cal fer-ho, però en cap cas mentir.
- En aquest sentit és prudent evitar esmentar, com a mínim al principi de la crisi, les causes de l'incident, el seu responsable, dades que la investigació pugui revelar o les possibles conseqüències per a l'organització o per un altre grup d'interès. La coordinació és clau. Donar sempre la versió de l'organització, situant-vos com la font d'informació més creïble i precisa. Donar missatges contradictoris és un error que cal evitar en tot moment.
- Els missatges caldrà que s'adaptin per a cada fase d'evolució de la gestió del ciberincident, així com segons la informació disponible del mateix i el seu impacte.
- Transmetre confiança. Actuar amb serenitat, fermesa i professionalitat
- Demostrar una atenció acurada, respecte i un compromís total cap a tots els involucrats

- Demanar disculpes i assumir les responsabilitats si fos necessari (no culpar-ne d'altres)
- Posar en valor totes les accions realitzades per solucionar la crisi, tant preventives com correctives.
- Assegurar que l'activitat/negoci és viable
- Els comunicats han de ser clars, senzills, útils, regulars. Les comunicacions als grups d'interès no tecnològics han de ser en un llenguatge entenedor per a ells.
- Cal tenir plantilles dels comunicats preparades prèviament, per evitar improvisacions que poden conduir a errors en la comunicació. Així es poden adaptar ràpidament i tenir en poc temps comunicats de qualitat.
- Moltes de les comunicacions poden ser bidireccionals, i la resposta a aquestes que donin els grups d'interès pot tenir repercussions en les decisions que prengui el comitè de crisi.

Sobre la comunicació interna:

- La comunicació interna és tant important com l'externa. Cal atendre les necessitats d'informació del personal intern.
- Només es faran servir per a les comunicacions internes els canals oficials corporatius per a que tot el personal tingui clara la seva autenticitat.
- És important donar al personal intern instruccions precises de com han d'actuar, i aclarir-los la situació en base als fets.
- De forma prèvia als ciberincidents és molt recomanable fer una petita formació sobre com han d'actuar els usuaris interns en cas de produir-se un.

5.2 Llistat de comunicacions

En situació de Cibercrisi, és fonamental procedir a l'elaboració de la informació més adequada tenint en compte: temps o prioritat i grup d'interès.
En aquest apartat es defineixen, en funció d'aquest dos paràmetres (el moment de la crisi i el grup d'interès afectat) el tipus d'informació a oferir, els missatges clau, el format i el canal o mitjà.

Així mateix es recullen les plantilles dels missatges tipus per a les diferents comunicacions. Tot i que aquestes plantilles s'han d'adaptar a cada cas concret de ciberincident, permeten tenir una base amb la que poder elaborar aquests comunicats de forma molt més ràpida i evitant improvisacions que poden conduir a errors en la comunicació. Així es poden preparar en poc temps comunicats de qualitat.

Grup d'interès afectat	Categoria de l'incident	Comunicació
Personal intern	Lleu	• Canal: canals de comunicació interna oficials (correu electrònic corporatiu, eina de col·laboració corporativa, intranet corporativa, telèfon corporatiu, etc...). S'escolliran uns o altres depenent del número de persones afectades. • Destinataris: grup concret de personal intern afectat. • Missatges clau: què ha passat de forma resumida, quina afectació tenen, què han de fer. • Temps: en quant que el Responsable de Seguretat consideri que es pot fer la notificació. Actualitzacions posteriors segons sigui necessari i comunicació final de tancament. • Responsable de la comunicació: departament de Comunicació Interna
	Greu	• Canal: canals de comunicació interna oficials (correu electrònic corporatiu, eina de col·laboració corporativa, intranet corporativa, telèfon corporatiu, etc...). S'escolliran els que puguin tenir ressò a un major número de persones en menor temps. • Destinataris: tot el personal intern. • Missatges clau: què ha passat de forma resumida, quina afectació tenen, què han de fer. • Temps: en quant que el Responsable de Seguretat consideri que es pot fer la notificació i el Comitè de Crisi l'aprovi. Actualitzacions posteriors segons sigui necessari i comunicació final de tancament. • Responsable de la comunicació: departament de Comunicació Interna
Regidors/es i Direcció de l'organització	Lleu	• Canal: correu electrònic amb els detalls de l'incident. Trucada telefònica si fos necessari. • Destinataris: en principi només direcció de l'àrea de la depèn el servei de Tecnologia i/o de l'àrea concreta afectada. • Missatges clau: què ha passat, quina afectació existeix a la disponibilitat de serveis i/o privacitat de la informació, quines decisions s'estan prenent, quines accions han de prendre (i quines no). • Temps: immediatament després d'identificar i classificar l'incident. Actualitzacions posteriors segons sigui necessari i comunicació final de tancament. • Responsable de la comunicació: Responsable de Tecnologia
	Greu	• Canal: correu electrònic amb els detalls de l'incident i trucada telefònica. • Destinataris: Tota la direcció de l'organització i els representants polítics del govern i de l'oposició. • Missatges clau: què ha passat, quina afectació existeix a la disponibilitat de serveis i/o privacitat de la informació, quines decisions s'estan prenent. • Temps: immediatament després d'establir el comitè de crisi i d'activar el protocol de comunicació. Actualitzacions

		posteriors segons sigui necessari i comunicació final de tancament. • Responsable de la comunicació: qui designi el comitè de crisi
Ciutadania	Lleu	• Si l'incident no té repercussions per a la ciutadania no cal realitzar cap comunicació. • En cas que sí existeixi impacte a la ciutadania: o Canal: web municipal, xxss, comunicat de premsa segons criteri de l'equip de Comunicació. També mitjançant l'atenció ciutadana presencial o per telèfon quan hi hagi afectació d'aquests serveis. o Missatges clau: què ha passat, quina afectació existeix per a la ciutadania en quant a la disponibilitat de serveis i/o privacitat de la informació, quines decisions s'estan prenent, què han de fer? o Temps: en quant que el Responsable de Seguretat consideri que es pot fer la notificació. Actualitzacions posteriors segons sigui necessari, i comunicació de final de tancament. o Responsable de la comunicació: Cap de Comunicació
	Greu	• Canal: web municipal (activació de lloc web alternatiu si fos necessari), xxss, roda de premsa de representant polític, radio i televisió municipals, oficines d'atenció al ciutadà, 010... segons criteri de l'equip de Comunicació i aprovació del Comitè de Crisi. També mitjançant l'atenció ciutadana presencial o per telèfon quan hi hagi afectació d'aquests serveis. • Missatges clau: què ha passat, quina afectació existeix per a la ciutadania en quant a la disponibilitat de serveis i/o privacitat de la informació, quines decisions s'estan prenent. • Temps: immediatament després d'establir el comitè de crisi i d'activar el protocol de comunicació. Actualitzacions posteriors segons sigui necessari, i comunicació de final de tancament. • Responsable de la comunicació: qui designi el comitè de crisi
Mitjans de Comunicació	Greu	En principi queden coberts amb les comunicacions que es facin a la ciutadania en cas d'incident greu, però l'equip de Comunicació pot proposar d'altres comunicacions, com per exemple entrevistes a premsa.
Proveïdors i altres AAPP amb qui hagi relació	Lleu i Greu	Només si el ciberincident afecta o pot afectar als proveïdors tecnològics de l'Ajuntament o bé a d'altres AAPP amb les que hi hagi relació tecnològica. Els paràmetres de la comunicació són

		iguals en els dos escenaris de ciberincident (lleu i greu) ja que el grau d'impacte d'aquestes entitats externes pot ser molt diferent segons el ciberincident i estar desvinculat del grau d'impacte per a l'Ajuntament. • Canal: correu electrònic i/o trucada telefònica als responsables del contracte dels proveïdors (Service Managers) o als contactes tècnics de les altres AAPP. • Destinataris: el grup específic de proveïdors o AAPP que poguessin ser afectats. • Missatges clau: què ha passat, quina afectació existeix per als proveïdors en quant a la disponibilitat de serveis i/o privacitat de la informació, quines decisions s'estan prenent. • Temps: comunicació inicial tant bon punt el comitè de crisi o el responsable de Tecnologia estableixi que hi ha algun risc per als proveïdors i/o AAPP externes. Actualitzacions posteriors segons sigui necessari i comunicació final de tancament. • Responsable de la comunicació: Responsable de Tecnologia.

5.3 Plantilles de comunicats

Comunicat breu per a la ciutadania i mitjans de comunicació

L'Ajuntament de XXXXXX ha patit un ciberincident, el qual està afectant al desenvolupament normal dels seus serveis.

Tot i no disposar encara de resultats concrets, s'està fent tot el possible per aconseguir-los mitjançant el desplegament de mitjans i recursos, tal com s'havia planificat.

Per tal de garantir els serveis essencials, l'informem que s'ha habilitat tant al web municipal com en les oficines d'atenció presencial, informació sobre els canals i serveis actius per tal de tramitar així com consultar els seus assumptes.

Esperem entengui la situació i estem a la seva disposició per ajudar-lo en el que necessiti.

Comunicat detallat per a la ciutadania i mitjans de comunicació

Revisar el text en detall i modificar el que sigui convenient a cada situació:

Ciberincident afecta els serveis de l'Ajuntament: Mesures preses i informació per als ciutadans

L'Ajuntament de XXXXXX vol informar a la ciutadania sobre un ciberincident que ha afectat els nostres serveis. Els detalls són els següents:

1. **Naturalesa del Ciberincident**: Hem detectat un atac informàtic que ha compromès la seguretat dels nostres sistemes i xarxes. Aquest incident ha afectat diversos serveis municipals, incloent l'accés a tràmits en línia, pagaments, i altres recursos digitals.
2. **Mesures Preses**:
    - Hem tancat temporalment els serveis afectats per investigar l'abast del ciberatac.
    - Hem contactat les autoritats competents i estem col·laborant activament amb els experts en ciberseguretat per resoldre la situació.
    - Estem informant els ciutadans a través de les nostres xarxes socials i el lloc web oficial.
3. **Impacte als Ciutadans**:
    - Si heu intentat accedir a serveis en línia i heu experimentat problemes, us demanem disculpes i us preguem que tingueu paciència mentre treballem per restablir-los.
    - Si heu realitzat pagaments o transaccions en línia durant aquest període, us recomanem que reviseu els vostres comptes bancaris i feu un seguiment de qualsevol activitat sospitosa.
4. **Contacte i Recursos**:
    - Per a més informació, podeu trucar al nostre servei d'atenció al ciutadà al telèfon 010 (o +34 XXXXXXXXX des de fora del municipi).
    - Actualitzarem regularment la nostra pàgina web oficial i les xarxes socials amb noves informacions i instruccions.

L'Ajuntament de XXXXXX està treballant diligentment per resoldre aquesta situació i garantir la seguretat dels nostres serveis. Us agrairem la vostra comprensió i col·laboració mentre investiguem i prenem les mesures necessàries.

Altres possibles plantilles de comunicats a preparar:

Comunicat per al personal intern, comunicats específics segons el tipus de ciberincident (ransomware, DDoS, phishing, etc...).

5.4 Lloc web

Cal tenir present, la previsió de disposar d'un lloc web "darksite" o extern als sistemes corporatius amb pàgines i continguts prèviament confeccionats de cara a la possible interrupció del servei de la web municipal oficial degut a un ciberincident. Aquest lloc web no serà visible públicament fins que es presenti la necessitat de posar-ho on-line. Aquesta precaució permet :

- Estar preparats per a reaccionar immediatament en el cas que s'entri en crisi
- Tenir un lloc web on dirigir tots els públics involucrats en una crisi (periodistes, autoritats, familiars, entre d'altres usuaris).
- Disposar dels enllaços dels serveis digitals establerts com alternatius durant la cibercrisi.

Localret

https://localret.cat