Protocol breu

de resposta davant un incident de seguretat

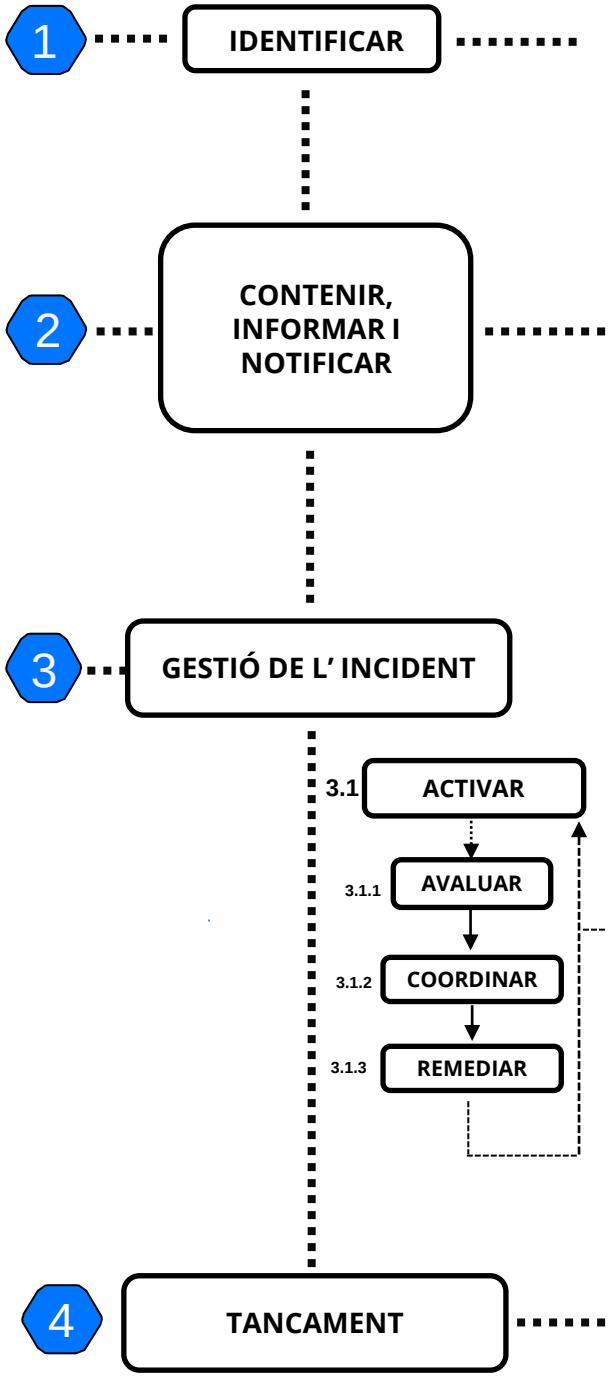
Localret

agenda digital dels municipis de Catalunya

Amb la participació de:

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Protocol d'actuació davant un incident de ciberseguretat



En el cas de detecció d'un problema de seguretat per part dels diferents sistemes de seguretat i equips associats a l'Ens local, serà l'equip dels Serveis TI qui identificarà en primera instància la gravetat de la situació per la qual se sospita o es té confirmació que pot esdevenir un incident de seguretat.

CONTENIR: El responsable de Sistemes (CTO) posarà en marxa les mesures tècniques d'urgència:

a) No apagar ni reiniciar els equips. No encendre equips apagats. Exclusivament en cas de Ransomware, aïllar els equips d'Internet i de la xarxa corporativa
b) Aïllar els servidors de fitxers i les bases de dades corporatives
c) Aïllar sistema de back-up
d) Intentar no donar pistes als atacants
e) Capturar proves volàtils

I avaluarà inicialment la magnitud per començar la fase de comunicació que coordinarà amb el Responsable de Seguretat

INFORMAR I NOTIFICAR:

En cas de ser un incident GREU:

1. Informar al Responsable de Seguretat de l'Entitat
2. **Trucar** al CATALONIA CERT i aplicació d'accions immediates. Anàlisi inicial de l'incident i identificació conjunta de les figures a implicar en els equips de treball. **Telèfon 24x7 (900 112 444)**
3. El responsable de Seguretat convocarà al Comitè de Crisi de l'Entitat i es formaran els equips de treball
4. En cas d'afectar a **dades personals, informar al DPD** que avaluarà si cal comunicar a APDCAT

En cas de ser un incident LLEU:

1. Informar al Responsable de Seguretat de l'Entitat
2. Notificar al CATALONIA CERT per **correu electrònic** cert@ciberseguretat.cat o Telèfon 24x7 (900 112 444)
3. Prendre mesures correctives als sistemes implicats (ERIC-TI)
4. En cas d'afectar a **dades personals, informar al DPD**

El comitè de crisi activarà:

1.- L'Equip de Resposta d'Incidents de Ciberseguretat de Tecnologia (ERIC-TI).
2.- L'Equip de Comunicació d'Incidents de Ciberseguretat (ECIC).

El comitè de crisi establirà:

3.- Els períodes d'actualització de la informació de l'estat de l'incident per part del ERIC-TI.
4.- Els equips de treball que es cregui necessaris per realitzar la contingència de la situació.

El comitè de crisi coordinarà:

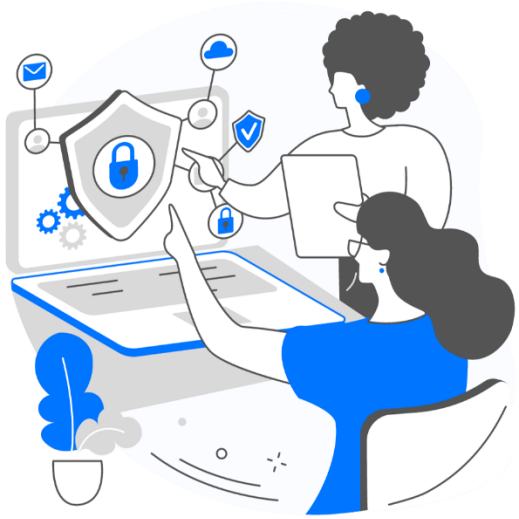
L'equip tècnic (ERIC-TI): El responsable de sistemes de la Informació (CTO) i el seu equip tècnic **avaluaran** i aplicaran les actuacions necessàries per restablir els serveis amb el suport del CATALONIA-CERT. **Informarà** en la periodicitat establerta al Responsable de Seguretat de l'entitat.

L'equip de comunicació (ECIC): El responsable de Seguretat coordinarà amb l'ECIC la informació que ha rebut del responsable de sistemes i informarà al comitè de crisi, qui determinarà la informació que es donarà a la ciutadania i agents implicats.

Els entorns implicats: El responsable de Seguretat 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.

Convocar el comitè de crisi per verificar la correcta tornada en servei dels sistemes afectats. En cas de confirmar-se, dissoldre el comitè de crisi i els grups de treball per part de la presidència del Comitè de Seguretat, i aprovació de l'acta, redactada pel secretari, de la majoria de membres. Realitzar informe post-crisi amb l'anàlisi de les causes i propostes de millora.

Com identificar la gravetat de l'incident



INCIDENT **GREU**

Es pot tractar d'un incident d'afectació greu en cas que es detecti algun o tots dels següents indicis:

- Detecció de gran volum de serveis o màquines virtuals crítiques caigudes.
- No es pot accedir al controlador de domini.
- Identificació de gran quantitat de fitxers encriptats.
- Confirmació d'una intrusió a la xarxa interna de l'entitat.

Si és un incident de **RANSOMWARE**, en el moment de la recuperació del sistema, es vetllarà per preservar les evidències digitals que es vagin trobant (si n'hi ha) fet que es comunicarà immediatament pels canals anteriors per tal que sigui recollida el més aviat possible.

INCIDENTS **LLEUS**

Es pot tractar d'altres tipus d'incident (lleus) en cas que es detecti alguns o tots dels següents indicis:

- Identificació de connexions (o intents) a direccions no conegudes des de la xarxa interna cap a l'exterior.
- Identificació d'un inici de sessió no autoritzat d'un usuari de l'entitat.
- Identificació d'un compte compromès de l'entitat.
- Identificació de correus sospitosos en bústies de correu corporatives.
- Detecció de comportaments sospitosos a les estacions de treball.
- Identificació de tancada de sessió en el moment d'ús de les estacions de treball.
- Aparició de fitxers desconeguts a l'escriptori o qualsevol altra ruta d'una estació de treball.
- Altres tipus d'indicis d'activitat maliciosa.

Composició del comitè de crisi i equips de treball. Normativa aplicable

COMPOSICIÓ DELS COMITÈS

Comitè de crisi

- Alcalde/ssa, o persona en qui delegui
- Cap de Gabinet d'alcaldia, o persona en qui delegui
- Secretaria municipal
- Gerència municipal
- Responsable de Serveis Jurídics
- Cap de Servei de TI
- Responsable de Seguretat (CSO)
- Inspector/a al cap de la Policia Local
- Cap de Comunicació
- Delegat/da de Protecció de Dades (DPD)
- Secretari de Telecomunicacions i Transformació Digital
- Director General de l'Agència Ciberseguretat
- Director/a de CATALONIA-CERT
- Responsable CATALONIA-CERT
- Responsable de comunicació de l'Agència de Ciberseguretat
- Responsable de l'àmbit de CATALONIA-CERT
- Suport administratiu, que assumirà les funcions de secretaria

Altres: En cas d'existir un fet il·lícit o afectació a dades personals, es valorarà la incorporació de representants del Cos de Mossos d'Esquadra i de l'autoritat competent en matèria de protecció de dades.

Òrgan estratègic

- Alcalde/ssa o Regidor delegat TIC
- Secretari Telecomunicacions i transformació digital
- Responsable de seguretat de la informació (CISO)
- Director General de l'Agència de Ciberseguretat
- Cap de Comunicació
- Comunicació de l'Agència de Ciberseguretat

Equip de treball de Resposta ERIC-TI

- Responsable de seguretat de la informació (CISO)
- Responsable de Sistemes TI
- Responsable Tècnic TI CATALONIA-CERT
- Especialistes (intern o externs de l'Ajuntament) que el Responsable de Seguretat determini que siguin necessaris

Equip de treball de Comunicació ECIS

- Cap Gabinet Alcaldia o similar
- Cap de Comunicació
- Responsable de comunicació de l'Agència de Ciberseguretat
- Especialistes (intern o externs de l'Ajuntament) que el Cap de Comunicació determini que siguin necessaris

Tractament de la informació

Qualsevol informació relacionada és de caràcter confidencial i no es pot compartir sense autorització prèvia

Normativa aplicable

- L'Agència de Ciberseguretat de Catalunya actua com a CERT competent en |'àmbit de Catalunya, en virtut d'allò establert a l'article 2.4.c de la Llei 15/2018, de juliol. En l'àmbit de la Generalitat de Catalunya aquest protocol es fonamenta en la norma de gestió d'incidents de ciberseguretat del marc normatiu que governa l'entitat.
- Es recomana tenir en compte qualsevol altra obligació de notificació a les descrites al punt 3 de la pàgina 1, segons possibles legislacions d'aplicació.

Telèfons de contactes

Interns

- Alcalde/essa, o persona en qui delegui : **(60X XX XX XX)**
- Responsable de Seguretat: **(60X XX XX XX)**
- Responsable de sistemes: **(60X XX XX XX)**
- Gerència municipal: **(60X XX XX XX)**
- Cap de Gabinet d'alcaldia, o persona en qui delegui : **(60X XX XX XX)**
- Cap de Comunicació: **(60X XX XX XX)**
- Secretaria/Intervenció/Tresoreria municipal: **(60X XX XX XX)**
- Responsable de Serveis Jurídics: **(60X XX XX XX)**
- Cap de Servei de TI: **(60X XX XX XX)**
- Delegat de Protecció de Dades: **(60X XX XX XX)**
- Inspector al cap de la Policia Local: **(60X XX XX XX)**

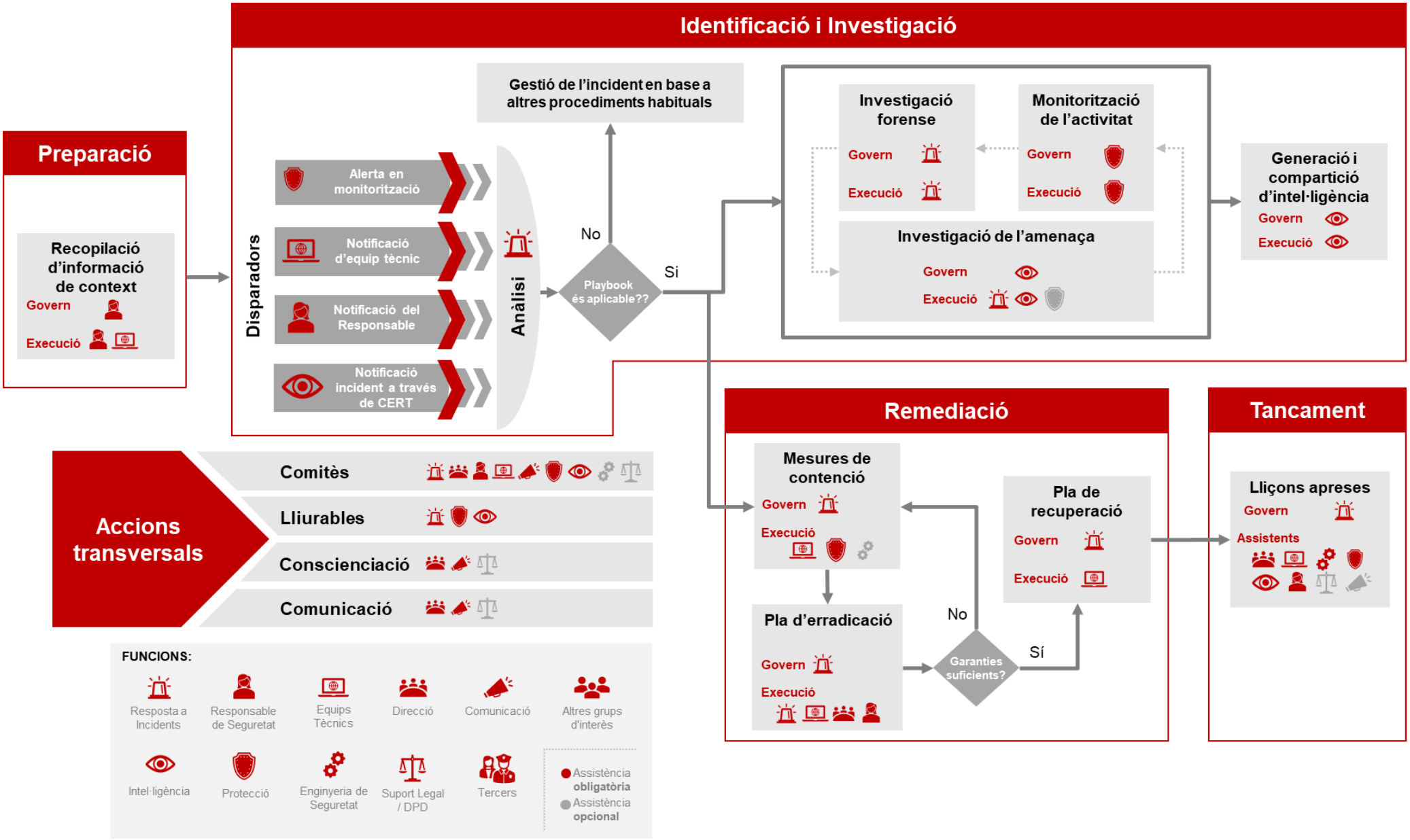
Proveïdors rellevants

- **EMPRESA 1** (Forense):
- **EMPRESA 2** (Antivirus):
- **EMPRESA 3** (Cabines):
- **EMPRESA 4** (còpies de seguretat):
- **EMPRESA 5** (SOC):

Autoritats competents

- **CATALONIA-CERT:** cert@ciberseguretat.cat **(telf. 24x7 - 900 112 444)**
- **COMUNICACIÓ AGÈNCIA DE CIBERSEGURETAT**: comunicacio@ciberseguretat.cat **(638 687 687)**
- **MOSSOS D'ESQUADRA:** mossosdti@gencat.cat
- **APDCAT:** https://apdcat.gencat.cat/ca/seu_electrónica/tramits/notificacio/ notificació mitjançant EACAT per les entitats donades d'alta en aquesta plataforma o a través d'eTRAM

Protocol de resposta



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 de les administracions locals. 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 2 – 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.