

Informe justificatiu per decretar la urgència per risc crític al CPD del CAR

1. Objecte de l'informe

Aquest informe té per objecte justificar la necessitat de decretar la urgència en relació amb la infraestructura elèctrica crítica del CPD del CAR, arran de l'aturada completa del centre de procés de dades produïda després d'una aturada elèctrica programada i de l'estat no detectat del SAI principal.

L'objectiu d'aquest informe és acreditar que existeix una situació de risc greu, actual i no ordinari que pot comprometre novament la continuïtat dels serveis informàtics essencials del CAR i justificar les actuacions urgents necessàries per reduir aquest risc.

La situació és especialment crítica perquè el CAR ha estat 15 dies sense servei informàtic i només fa 3 dies que s'ha aconseguit reiniciar el SAI. A més, aquest model de SAI no es pot posar en marxa si no disposa de bateries en bon estat, fet que indica que la substitució de bateries ha permès recuperar temporalment la funcionalitat, però no elimina la situació de risc estructural del sistema.

2. Antecedents

El diumenge 14 de juny del 2026, el CPD del CAR va quedar aturat de manera inesperada arran d'una aturada elèctrica programada. Aquesta aturada va provocar la indisponibilitat generalitzada dels serveis TIC del centre.

Posteriorment, es va realitzar una intervenció tècnica sobre el SAI principal del CPD. Segons l'acta de treball de Schneider Electric, la intervenció va consistir en un manteniment preventiu amb substitució de bateries. El document identifica l'equip com un **APC Symmetra PX 32kW scalable to 96kW 400V with Modular Power Distribution**, producte **SY32K96H-PD**, número de sèrie **PD1119360107**.

L'acta tècnica indica que el diagnòstic del SAI era el següent:

- Bateries amb gairebé 15 anys
- Vida de disseny de les bateries: 5 anys
- Bateries deteriorades
- Bateries sulfatades
- **Bateries amb pèrdua d'àcid**
- **Bateries inflades**
- Targeta NMC amb fallada de comunicació
- **No consten evidències documentals suficients de manteniment vigent o traçable**

Aquesta informació confirma que l'estat del SAI requeria una actuació urgent i era incompatible amb el nivell de disponibilitat i fiabilitat que necessita un equip destinat a protegir un CPD institucional.

3. Situació actual

Després de la intervenció, s'han substituït **24 mòduls de bateria**, s'ha substituït la **targeta NMC**, s'han fet arrencada i proves funcionals i s'ha normalitzat parcialment la instal·lació. L'equip queda en funcionament normal i sense alarmes presents.

Aquest fet és positiu, però no elimina la situació la urgència. L'acta recomana la substitució d'alguns components per fi de vida i recomana formalitzar un contracte de manteniment del SAI.

Per tant, la situació actual és la següent:

1. El SAI ha estat recuperat funcionalment fa només 3 dies.
2. El SAI ha pogut arrencar perquè les bateries han estat substituïdes i ara permeten l'arrencada.
3. El sistema es troba actualment sense alarmes presents.
4. L'equip continua tenint components que han arribat o superat el seu període de vida útil recomanat.
5. El propi fabricant recomana substituir components addicionals.
6. El propi fabricant recomana establir un contracte de manteniment.
7. L'organització acaba de patir una aturada completa del CPD que ja acumula 15 dies d'afectació.
8. La incidència posa de manifest la necessitat de reforçar la resiliència de la infraestructura crítica davant actuacions elèctriques programades.

Això significa que la situació no es pot considerar completament normalitzada des del punt de vista de continuïtat de servei. S'ha restablert el funcionament, però no s'ha eliminat el risc.

4. Elements tècnics que justifiquen la urgència

4.1. Estat crític de les bateries

L'acta tècnica descriu unes bateries amb gairebé 15 anys, quan la vida de disseny és de 5 anys. Això significa que **les bateries havien superat aproximadament en 10 anys la seva vida útil** de disseny.

A més, no es tractava únicament d'un envelliment ordinari. L'acta indica que **les bateries estaven deteriorades, sulfatades, amb pèrdua d'àcid i inflades.**

Aquest estat suposa un risc crític per diversos motius:

- Risc de no subministrar autonomia en cas de tall elèctric
- Risc de fallada completa del SAI
- Risc de dany intern al sistema
- Risc elèctric
- **Risc químic per pèrdua d'àcid**
- **Risc d'incendi** o escalfament
- Risc per a la seguretat física de la instal·lació
- Risc de nova caiguda completa del CPD

Per tant, **no estem davant d'una incidència menor, sinó davant d'una situació tècnica crítica d'un element essencial de seguretat elèctrica.**

4.2. Fallada de comunicació de la targeta NMC

L'acta també indica una fallada de comunicació de la targeta NMC.

Aquesta targeta és rellevant perquè permet la comunicació, supervisió i monitorització del SAI. Una incidència en aquest component limita la capacitat de supervisió remota i pot dificultar la detecció d'alarmes, evolució de l'estat de les bateries, esdeveniments elèctrics o avisos previs.

Aquesta circumstància reforça la necessitat d'actuar d'urgència perquè la continuïtat del servei depèn tant de la capacitat de suport elèctric com de la capacitat de supervisió i alerta.

4.3. Situació actual

Aquest element és especialment rellevant perquè el SAI és una infraestructura crítica. No és un equip auxiliar ni prescindible: és el sistema que ha de protegir el CPD davant talls, micro-talls, sobretensions, apagades programades i incidències elèctriques.

Cal considerar que:

- No es poden acreditar de manera completa les garanties objectives de funcionament
- Cal reforçar el control documentat de l'estat de les bateries
- Cal establir un seguiment formal del fi de vida dels components
- Cal disposar d'evidències documentals de proves periòdiques
- Cal reforçar la capacitat de prevenció i detecció anticipada
- El CPD manté una exposició elevada davant una nova incidència elèctrica

Això justifica una actuació urgent i extraordinària orientada a estabilitzar el servei i reduir el risc.

4.4. Components en fi de vida

Tot i que l'equip queda en funcionament normal i sense alarmes després de la intervenció, Schneider Electric recomana la substitució de molts components per fi de vida.

Aquesta recomanació és clau: l'equip funciona, però no està plenament renovat ni lliure de risc. El fet que hi hagi components en fi de vida implica que la probabilitat de fallada continua sent superior a l'acceptable per a un CPD institucional.

Per tant, no es pot concloure que el risc hagi desaparegut. Només s'ha corregit parcialment la situació més immediata: les bateries i la comunicació NMC.

4.5. Reinici recent del SAI

El SAI s'ha aconseguit reiniciar el dilluns 19 de juny del 2026 ja que, aquest model no pot posar-se en marxa si les bateries no estan en bon estat.

Aquesta dada és important per dues raons:

En primer lloc, confirma que l'estat anterior de les bateries era incompatible amb una operació segura i que la substitució era imprescindible per recuperar el funcionament.

En segon lloc, el fet que el SAI hagi arrencat no equival a tenir una situació plenament estabilitzada. El sistema acaba de tornar a servei després d'una incidència greu, amb components addicionals en fi de vida i sense que consti encara una estratègia completa de continuïtat i disaster recovery.

En conseqüència, el reinici del SAI no ha de ser interpretat com una resolució definitiva, sinó com una estabilització provisional que permet guanyar temps per executar actuacions urgents.

5. Impacte de l'incident sobre el CAR

La caiguda completa del CPD ha tingut un impacte directe sobre la continuïtat operativa del CAR.

La indisponibilitat TIC de 15 dies afecta a:

- **Comunicacions: telefonia i correu electrònic**
- **Seguretat física, control d'accés i presència**
- Serveis administratius
- Gestió interna
- Xarxa corporativa

- **Sistemes d'autenticació**
- Fitxers i repositoris interns
- Bases de dades
- Aplicacions de gestió
- Suport als equips
- Activitat ordinària del centre
- Relació amb usuaris, esportistes, tècnics i proveïdors
- Capacitat de resposta institucional
- Seguretat i control dels sistemes
- Compliment de les obligacions de transparència i accés a la informació pública
- Capacitat de resposta davant sol·licituds d'accés a informació pública
- Compliment de les obligacions derivades de la normativa de protecció de dades
- Exercici efectiu dels drets de les persones interessades en matèria de protecció de dades incloent-hi accés, rectificació, supressió, oposició, limitació del tractament i portabilitat
- Capacitat de localitzar, consultar, verificar i lliurar informació personal dins dels terminis legalment exigibles
- Gestió i documentació d'eventuals bretxes de seguretat o indisponibilitat de dades personals
- Capacitat de comunicar, si escau incidències o bretxes de seguretat a l'autoritat competent en protecció de dades
- Capacitat d'informar les persones afectades quan la normativa ho exigeixi
- Manteniment de la traçabilitat integritat, disponibilitat i custòdia documental
- Compliment de terminis legals, fiscals, comptables, administratius i de justificació documental

Aquest impacte supera l'àmbit purament tècnic, ja que afecta el funcionament general de l'organització i pot comprometre la capacitat del CAR per complir obligacions legals i administratives essencials.

En particular, la indisponibilitat dels sistemes pot afectar el compliment de la normativa de transparència i accés a la informació pública, atès que el centre pot veure limitada la seva capacitat de localitzar, consultar i lliurar la informació requerida dins dels terminis establerts. La legislació en matèria de transparència reconeix el dret d'accés a la informació pública i exigeix que les administracions puguin donar una resposta adequada a les sol·licituds

formulades.

Així mateix, aquesta situació pot afectar el compliment de la normativa de protecció de dades, ja que les persones interessades tenen dret a exercir els drets d'accés, rectificació, supressió, oposició, limitació del tractament, portabilitat i la resta de drets reconeguts pel RGPD. La indisponibilitat dels sistemes pot comprometre la capacitat del CAR per consultar les dades i verificar la informació necessària, respondre dins dels terminis legalment establerts i acreditar documentalment les actuacions realitzades.

A més, una indisponibilitat greu dels sistemes o la pèrdua d'accés a dades personals pot requerir valorar l'existència d'una possible bretxa de seguretat de dades personals i, si escau, comunicar-la a l'autoritat de control competent. D'acord amb els criteris de l'AEPD, les bretxes que puguin suposar un risc per als drets i les llibertats de les persones han de ser notificades a l'autoritat de control, amb caràcter general, dins del termini de 72 hores des que se'n té constància.

Per tant, la caiguda del CPD no constitueix únicament un problema intern de disponibilitat dels sistemes d'informació, sinó que pot tenir conseqüències sobre el compliment de les obligacions legals i administratives del CAR en matèria de transparència i accés a la informació pública, protecció de dades personals, resposta a la ciutadania, justificació documental de les actuacions administratives i, quan correspongui, comunicació d'incidències davant l'autoritat competent.

Per aquest motiu, l'actuació no pot limitar-se a reparar un component. Cal actuar sobre la continuïtat global del servei informàtic i sobre la infraestructura crítica que el sosté.

6. Risc actual

El risc actual és alt perquè es donen simultàniament diversos factors:

1. El CPD acaba de patir una caiguda completa.
2. La indisponibilitat ha durat 15 dies.
3. El SAI tenia bateries en estat crític.
4. Les bateries havien superat àmpliament la seva vida de disseny.
5. Existia pèrdua d'àcid i inflament de bateries.
6. La targeta NMC presentava fallada de comunicació.
7. No consten evidències documentals suficients de manteniment vigent i traçable del SAI.
8. El fabricant recomana substituir components per fi de vida.
9. El fabricant recomana contracte de manteniment.
10. **No es pot garantir que una nova incidència elèctrica no torni a afectar greument el CPD.**

11. Una nova aturada en calent dels sistemes d'emmagatzematge podria provocar corrupció o pèrdua total/parcial d'informació crítica incloent dades mèdiques, científiques, administratives, econòmiques i contractuals.
12. Una nova indisponibilitat del CPD podria impedir el compliment de terminis legals, fiscals, comptables, administratius i de justificació documental.
13. El SAI ha estat reiniciat i posat novament en funcionament, però en el moment de redactar aquest informe encara es desconeix l'abast real dels possibles danys produïts sobre el sistema informàtic incloent servidors, sistemes d'emmagatzematge, bases de dades, plataformes de virtualització, comunicacions i integritat de la informació.

Aquests fets son especialment rellevants perquè la recuperació funcional del SAI no equival necessàriament a la recuperació completa i segura del CPD. Fins que no s'hagi verificat l'estat dels sistemes, la integritat de les dades, el funcionament dels serveis crítics i la capacitat de recuperació davant una nova incidència, el risc ha de considerar-se encara obert.

7. Justificació de la urgència

Es considera justificat decretar la urgència perquè concorren els elements següents:

7.1. Existència d'un risc greu

L'estat documentat del SAI demostra que l'equip es trobava en condicions en estat tècnic crític: bateries amb gairebé 15 anys, deteriorades, sulfatades, amb pèrdua d'àcid inflades i amb risc d'incendi.

Aquest estat compromet directament la capacitat del CPD de resistir una incidència elèctrica.

7.2. Afectació d'un servei essencial

El CPD dona suport als serveis informàtics essencials del CAR. La seva caiguda ha provocat una afectació generalitzada i prolongada. Per tant, la infraestructura afectada té caràcter crític.

7.3. Necessitat d'actuació immediata

Tot i que el SAI ha estat reiniciat, la situació no permet esperar a una tramitació ordinària si això implica mantenir durant setmanes o mesos components en fi de vida, necessitat de formalitzar un contracte de manteniment i necessitat de reforçar la redundància suficient.

La intervenció ha de ser immediata per reduir el risc de nova caiguda.

7.4. Risc de repetició

El fet que el SAI estigui actualment sense alarmes no elimina el risc de repetició. El propi informe tècnic recomana substituir components per fi de vida i establir contracte de manteniment.

Això acredita que resten actuacions pendents per consolidar una situació segura i estable.

7.5. Impacte institucional desproporcionat

Una nova caiguda del CPD podria provocar un impacte institucional desproporcionat, molt superior al cost de les actuacions urgents necessàries per estabilitzar la infraestructura.

En primer lloc, una nova interrupció elèctrica podria comportar una nova aturada en calent dels sistemes informàtics. Aquest escenari és especialment greu en el cas dels sistemes d'emmagatzematge, bases de dades i plataformes de virtualització, ja que una aturada sobtada pot provocar corrupció de dades inconsistències, pèrdua d'integritat dels volums impossibilitat d'arrencada dels serveis o, en el pitjor dels casos, pèrdua total o parcial de la informació.

Aquest risc és crític perquè el CAR gestiona informació d'alt valor i d'alta sensibilitat incloent-hi dades mèdiques, dades científiques informació vinculada al rendiment esportiu, documentació administrativa, dades econòmiques informació contractual i altres dades corporatives essencials. La pèrdua, corrupció o indisponibilitat d'aquesta informació podria generar un impacte operatiu molt greu i també un risc legal significatiu, especialment pel que fa a la protecció de dades, la confidencialitat, la traçabilitat, la custòdia documental i la capacitat d'acreditar actuacions realitzades.

En segon lloc, la indisponibilitat dels sistemes informàtics pot afectar directament la capacitat del centre per complir amb les seves obligacions legals, administratives i econòmiques. Una nova aturada podria impedir o dificultar la presentació d'informes, justificacions imposts, documents comptables, facturació, tramitació d'expedients, gestió pressupostària, resposta a requeriments administratius, compliment de terminis oficials i altres obligacions davant organismes públics, proveïdors, auditors o entitats de control.

En tercer lloc, una nova caiguda podria comprometre la continuïtat de l'activitat ordinària del CAR, afectant no només l'àrea TIC, sinó també direcció, administració, serveis mèdics, unitats científiques, entrenadors, esportistes, personal tècnic i serveis generals. L'impacte no seria, per tant, una incidència limitada a un sistema, sinó una afectació transversal al funcionament institucional del centre.

Aquesta situació és especialment rellevant perquè l'acta tècnica del SAI acredita que l'equip es trobava en un estat tècnic que requeria actuació immediata: bateries amb gairebé 15 anys quan la vida de disseny és de 5 anys, bateries deteriorades, sulfatades, amb pèrdua d'àcid i inflades, fallada de comunicació de la targeta NMC i manca d'evidències documentals suficients de manteniment vigent i traçable.

Tot i que el SAI ha quedat en funcionament normal després de la substitució de 24 mòduls de bateria i de la targeta NMC, el propi informe recomana substituir components per fi de vida i formalitzar un contracte de manteniment. Això confirma que la situació s'ha estabilitzat parcialment, però no es pot considerar plenament resolta des del punt de vista de risc institucional.

Per tant, el risc d'una nova caiguda no es limita a una nova interrupció temporal del servei informàtic. Pot comportar pèrdua d'informació crítica incompliments legals, afectació de

dades sensibles, bloqueig administratiu impacte econòmic, dany reputacional i impossibilitat de garantir la continuïtat operativa del CAR.

Per aquest motiu, l'impacte potencial de retardar les actuacions urgents és superior al cost d'executar immediatament les mesures necessàries per estabilitzar el CPD, reforçar el SAI, garantir les còpies de seguretat implementar un pla de *disaster recovery* i dotar l'organització dels recursos humans i econòmics necessaris.

8. Actuacions que haurien de quedar emparades per la urgència

la urgència hauria de permetre executar de manera immediata totes les actuacions necessàries per estabilitzar el CPD, reduir el risc de nova caiguda i recuperar plenament la capacitat operativa dels sistemes informàtics. Aquestes actuacions han d'incloure no només les mesures sobre el SAI i la infraestructura elèctrica, sinó també la diagnosi, reparació o substitució dels elements TIC que hagin pogut resultar afectats per l'aturada en calent i que, en el moment de redactar aquest informe, encara no han estat completament identificats. Això pot incloure servidors, sistemes d'emmagatzematge, cabines de discos, electrònica de xarxa, sistemes de virtualització, bases de dades, còpies de seguretat, comunicacions i qualsevol altre component necessari per garantir la integritat, disponibilitat i recuperació segura dels serveis crítics del CAR.

Les actuacions recomanades són:

8.1. Actuacions sobre el SAI

Pel que fa al SAI, cal executar de manera urgent una revisió tècnica completa de l'equip i totes les actuacions necessàries per garantir-ne el funcionament segur i estable. Aquesta actuació ha d'incloure, de manera prioritària, la substitució dels components identificats en fi de vida, atès que el propi informe tècnic indica que, tot i que l'equip ha quedat en funcionament normal i sense alarmes, encara existeixen elements que han superat la seva vida útil i poden comprometre la fiabilitat del sistema.

Així mateix, cal revisar de manera immediata el contracte de manteniment existent, el seu abast, les obligacions previstes, les actuacions executades, les evidències documentals disponibles i el nivell de servei efectivament prestat. L'objectiu és garantir que el manteniment del SAI es presta de manera efectiva, verificable i documentada, amb revisions periòdiques, proves funcionals, control de bateries, monitorització, resposta davant incidències i emissió d'informes tècnics.

En cas que el contracte vigent no garanteixi de manera immediata aquests requisits, caldrà adoptar les mesures contractuals, tècniques o organitzatives necessàries per assegurar la continuïtat del manteniment del SAI sense interrupcions i amb un nivell de control adequat a la criticitat del CPD.

Aquestes mesures són necessàries per evitar que el SAI pugui tornar a quedar en una situació de degradació no detectada i per assegurar que el CPD disposa d'una protecció elèctrica efectiva davant noves incidències, micro-talls, sobretensions o aturades programades.

8.2. Actuacions sobre la infraestructura elèctrica del CPD

Pel que fa a la infraestructura elèctrica del CPD, cal executar una revisió urgent i integral de tota la cadena d'alimentació, no només del SAI de manera aïllada. La indisponibilitat funcional del SAI durant l'incident posa de manifest que el CPD ha estat exposat a una manca d'estabilització elèctrica, manca de tolerància davant micro-talls, sobretensions, caigudes de tensió i interrupcions programades o imprevistes. Aquesta situació és especialment greu perquè el SAI és l'element encarregat de protegir els sistemes crítics davant inestabilitats de xarxa i de permetre una transició segura entre l'alimentació ordinària, l'autonomia de bateries i, si escau, altres sistemes de suport. Per aquest motiu, cal revisar quadres elèctrics, línies d'alimentació, PDU's, proteccions, bypass, posada a terra, càrregues connectades, separació entre càrregues críiques i no críiques i comportament global de la instal·lació davant una nova aturada elèctrica. L'objectiu és garantir que el CPD disposa d'una alimentació estable, monitoritzada i resilient, capaç de protegir servidors, sistemes d'emmagatzematge, comunicacions i serveis essencials davant qualsevol nova incidència elèctrica. Aquesta actuació és urgent perquè l'acta tècnica acredita que el SAI havia arribat a una situació de situació tècnica crítica, amb bateries deteriorades, sulfatades, amb pèrdua d'àcid i inflades, fallada de comunicació de la targeta NMC i manca d'evidències documentals suficients de manteniment vigent i traçable.

8.3. Actuacions sobre la infraestructura TIC del CPD

A més de les actuacions sobre el SAI i sobre la infraestructura elèctrica, la urgència ha d'emparar també la diagnosi, reparació i, si escau, substitució dels elements TIC del CPD que hagin pogut resultar afectats per l'aturada en calent. En el moment de redactar aquest informe, el SAI ja ha estat reiniciat i posat novament en funcionament, però encara no es coneix l'abast real dels possibles danys sobre la infraestructura informàtica. Aquesta incertesa és especialment rellevant perquè una caiguda sobtada d'alimentació pot afectar no només l'arrencada dels sistemes, sinó també la integritat de les dades, l'estabilitat dels serveis i la fiabilitat dels components físics.

La infraestructura TIC que pot haver resultat afectada inclou els servidors físics, els nodes de virtualització, els sistemes d'emmagatzematge, les cabines de discos, els discos individuals, les controladores, les fonts d'alimentació, les targetes de xarxa, els commutadors, els tallafocs, els sistemes de còpia de seguretat, les bases de dades, els sistemes d'autenticació, els serveis de fitxers, les comunicacions internes i qualsevol altre component necessari per al funcionament dels serveis crítics del CAR. Una aturada sobtada pot provocar errors latents que no apareixen immediatament en el moment de l'arrencada, però que poden manifestar-se posteriorment en forma de degradació de rendiment, errors d'escriptura, corrupció de volums, fallades de discos inconsistències en bases de dades, problemes de sincronització o pèrdua parcial d'informació.

Per aquest motiu, cal dur a terme una revisió tècnica completa de l'estat de la infraestructura TIC del CPD, prioritzant els sistemes d'emmagatzematge, les plataformes de virtualització, les bases de dades i els serveis que suporten l'activitat essencial del centre. Aquesta revisió ha d'incloure la verificació de la integritat dels volums i sistemes de fitxers, la comprovació de l'estat dels discos i cabines, la revisió de registres d'errors, la validació de les bases de dades,

la comprovació de la consistència de les màquines virtuals, la revisió de l'estat dels backups i la verificació del funcionament dels serveis crítics.

També cal preveure que, durant aquesta diagnosi, puguin aparèixer components malmesos o degradats que requereixin reparació o substitució urgent. L'emergència ha de permetre actuar sobre aquests elements sense esperar una tramitació ordinària, perquè qualsevol retard pot mantenir el CPD en una situació de risc o provocar una nova indisponibilitat. Això inclou la possible substitució de discos, fonts d'alimentació, controladores, equips de xarxa, elements de storage, servidors o qualsevol altre component afectat per l'aturada.

Aquestes actuacions són necessàries perquè la normalització elèctrica del SAI no garanteix, per si sola, la normalització de la infraestructura TIC. L'acta de treball acredita que el SAI es trobava en una situació en estat tècnic crític, amb bateries deteriorades, sulfatades, amb pèrdua d'àcid i inflades, fallada de comunicació de la targeta NMC i manca d'evidències documentals suficients de manteniment vigent i traçable; tot i que després de la intervenció l'equip queda en funcionament normal i sense alarmes, també es recomana substituir components per fi de vida i formalitzar un contracte de manteniment.

Per tant, la urgència ha d'incloure expressament les actuacions sobre la infraestructura TIC que siguin necessàries per confirmar la integritat dels sistemes, recuperar plenament els serveis, reparar els elements afectats i garantir que el CPD pot tornar a operar amb un nivell de seguretat i fiabilitat acceptable.

8.4. Actuacions indispensables de continuïtat TIC assumibles amb la dotació actual

Atesa la dotació actual de recursos humans del departament TIC (dos tècnics i el cap del departament), no és realista assumir de manera immediata totes les actuacions pròpies d'un pla complet de continuïtat TIC i *disaster recovery*. Per aquest motiu, en aquesta fase d'emergència cal limitar les actuacions a les mesures indispensables i assumibles amb el personal disponible, prioritzant aquelles que redueixen de manera més directa el risc d'una nova pèrdua de servei o de dades.

Les actuacions mínimes haurien de centrar-se en verificar l'estat de les còpies de seguretat dels sistemes crítics, assegurar que existeix una còpia recent fora del CPD principal identificar els serveis essencials que s'haurien de recuperar primer en cas de nova incidència, documentar un procediment bàsic d'apagada ordenada i arrencada prioritzada i establir una llista curta de contactes i proveïdors crítics per actuar ràpidament en cas d'emergència.

També caldria fer, com a mínim, una prova de restauració limitada sobre un sistema no crític o un conjunt reduït de dades representatives, amb l'objectiu de confirmar que les còpies són utilitzables. Aquesta prova no substitueix un pla de recuperació davant desastres complet, però permet reduir el risc immediat de descobrir massa tard que les còpies no són recuperables.

Amb els recursos actuals, aquestes actuacions han de tenir un abast limitat, pràctic i orientat a supervivència operativa. No es pot exigir a l'equip TIC actual que desplegui, mantingui i provi un model complet de continuïtat, entorn alternatiu, restauració integral, simulacres

periòdics i documentació exhaustiva sense una ampliació prèvia de personal i pressupost.

Per tant, aquesta fase ha de tenir un doble objectiu: d'una banda, executar les mesures mínimes imprescindibles per reduir el risc immediat; de l'altra, deixar constància que la implantació real d'un Pla de Continuitat TIC i *Disaster Recovery* requereix necessàriament més recursos humans propis del CAR i una dotació econòmica específica.

8.5. Actuacions organitzatives indispensables i assumibles amb la dotació actual

Atesa la dotació actual del departament TIC —dos tècnics i el cap del departament—, les actuacions organitzatives immediates han de limitar-se a aquelles que siguin imprescindibles per contenir el risc, ordenar la resposta i evitar noves actuacions sobre infraestructura crítica sense validació prèvia.

En aquesta fase d'emergència, el departament TIC hauria de centralitzar la informació tècnica de l'incident identificar els riscos més urgents, documentar les decisions adoptades i establir un circuit mínim d'autorització per a qualsevol actuació que pugui afectar al CPD, al SAI, a la xarxa, als servidors, a l'emmagatzematge o a les comunicacions. Aquest circuit hauria d'incloure una validació TIC prèvia obligatòria abans de qualsevol intervenció elèctrica o tècnica amb impacte potencial sobre els serveis informàtics.

També caldria designar formalment un responsable de coordinació de la crisi TIC i establir un canal únic de comunicació amb direcció, proveïdors i àrees implicades. Aquesta mesura és necessària per evitar actuacions disperses, decisions no coordinades o intervencions sobre elements crítics sense una avaluació prèvia del risc tecnològic.

Amb els recursos actuals, el departament TIC pot assumir la coordinació tècnica, la identificació de riscos, la definició de prioritats i la proposta de mesures urgents. Tanmateix, no pot assumir en solitari totes les tasques organitzatives, contractuals, pressupostàries i operatives necessàries per estabilitzar definitivament la situació. Per aquest motiu, és imprescindible que direcció assumeixi formalment el lideratge institucional de l'emergència, validi les prioritats, garanteixi la col·laboració de totes les àrees implicades i faciliti els recursos necessaris.

Les actuacions organitzatives mínimes haurien de ser:

- Establir formalment que qualsevol actuació o accés, físic o lògic, que pugui afectar el CPD o qualsevol dels seus elements associats (SAI infraestructura elèctrica, xarxa, servidors, emmagatzematge, comunicacions o sistemes crítics) requerirà validació prèvia del Departament d'Informàtica i autorització expressa abans de la seva execució
- Centralitzar en TIC la informació tècnica relativa al SAI, CPD, xarxa, servidors i sistemes d'emmagatzematge
- Designar un interlocutor únic amb direcció per al seguiment de la crisi
- Crear un registre bàsic de riscos, decisions i actuacions pendents

- Revisar de manera prioritària les obligacions, prestacions i canals d'escalat dels proveïdors crítics
- Elevar a direcció les necessitats urgents d'inversió, manteniment i reforç de personal propi
- Establir un calendari mínim de seguiment fins a la normalització de la situació

Aquestes actuacions no substitueixen una governança completa de continuïtat TIC, però permeten reduir el risc immediat i evitar que es repeteixin actuacions no coordinades sobre infraestructura crítica. La implantació real d'un model estable de governança, continuïtat i *disaster recovery* requerirà necessàriament suport efectiu de direcció, col·laboració transversal de les àrees implicades, recursos econòmics específics i ampliació de l'equip TIC propi del CAR.

Amb la dotació actual, el departament TIC pot contenir el risc i ordenar la resposta immediata, però no pot garantir per si sol la governança completa d'una emergència que afecta infraestructura crítica de tota l'organització.

9. Necessitat d'inversió urgent

L'emergència no es justifica únicament per la substitució de bateries. La documentació tècnica mostra una situació de situació tècnica que requereix actuacions correctives de la infraestructura de suport elèctric del CPD.

El fet que les bateries tinguessin gairebé 15 anys, amb una vida de disseny de 5 anys i que no constin evidències documentals suficients de manteniment vigent i traçable, posa de manifest la necessitat d'un model més robust de seguiment, renovació i manteniment preventiu.

Cal una inversió urgent en:

- Estabilització del SAI
- Substitució de components en fi de vida
- Substitució dels equips obsolets i en fi de vida
- Monitorització
- Manteniment preventiu
- Revisió elèctrica del CPD
- Redundància
- *Disaster recovery*
- Documentació
- Proves periòdiques
- **Recursos humans TIC**

Aquesta inversió ha de considerar-se una inversió en continuïtat institucional, no una despesa tècnica ordinària.

10. Necessitat de reforç de recursos humans

La situació també posa de manifest la necessitat d'ampliar els recursos humans TIC.

La continuïtat d'un CPD no es garanteix únicament amb equipament. Requereix personal suficient per:

- Supervisar proveïdors
- Revisar informes de manteniment
- Controlar fi de vida dels equips
- Planificar renovacions
- Monitoritzar sistemes
- Respondre a alertes
- Documentar procediments
- Fer proves de recuperació
- Revisar còpies
- Executar simulacres
- Gestionar riscos
- Coordinar actuacions elèctriques
- Mantenir un pla de recuperació davant desastres viu i provat

Sense personal suficient propi del CAR, l'organització queda exposada a un model reactiu, en què els problemes es detecten quan ja han provocat una crisi. La supervisió d'una infraestructura crítica com el CPD no pot dependre exclusivament de proveïdors externs ni de personal subcontractat. Els proveïdors poden executar manteniments, aportar especialització tècnica puntual i donar suport en actuacions concretes, però la responsabilitat permanent de control, seguiment, validació, priorització i resposta ha de recaure en personal intern del CAR.

Per tant, la urgència hauria d'incloure també la justificació de reforçar l'equip TIC propi del CAR, com a mesura necessària per reduir el risc de repetició. Aquest reforç ha de materialitzar-se en places internes, estables i amb coneixement directe de la infraestructura, dels serveis crítics, dels procediments interns i de les necessitats operatives del centre. Subcontractar més serveis pot ajudar puntualment, però no substitueix la necessitat de disposar d'un equip TIC propi dimensionat per governar, supervisar i garantir la continuïtat tecnològica del CAR.

11. Conclusió

L'acta tècnica del SAI acredita una situació tècnica crítica en un element essencial del CPD: bateries amb gairebé 15 anys, deteriorades, sulfatades, amb pèrdua d'àcid i inflades; fallada de comunicació de la targeta NMC; i absència d'evidències documentals suficients de manteniment vigent i traçable.

Tot i que s'han substituït 24 mòduls de bateria i la targeta NMC i que el SAI ha quedat en funcionament normal i sense alarmes, el propi document recomana substituir components per fi de vida i formalitzar un contracte de manteniment.

Per tant, la situació no pot considerar-se plenament resolta. El servei s'ha recuperat, però el risc residual continua existint fins que no s'executin les actuacions pendents.

Atès que el CPD ha estat 15 dies sense servei, que el SAI només fa 3 dies que s'ha pogut reiniciar, que el model no pot arrencar sense bateries en bon estat i que encara resten components en fi de vida, es considera justificat decretar la urgència per garantir la continuïtat dels serveis essencials del CAR.

La finalitat de l'emergència ha de ser establir definitivament el CPD, reduir el risc de nova caiguda, assegurar el manteniment del SAI implementar mesures de continuïtat i recuperació davant desastres i dotar el CAR de la inversió i els recursos humans necessaris per evitar que una situació similar es torni a repetir.

La conclusió executiva és:

El SAI torna a funcionar, però el risc no ha desaparegut. L'incident posa de manifest que el CPD del CAR necessita una actuació urgent, estructural i dotada de recursos per garantir la continuïtat institucional.

La recuperació funcional del SAI no equival a la recuperació completa i segura del CPD. En el moment de redactar aquest informe encara es desconeix l'abast real de l'impacte que l'aturada en calent ha pogut tenir sobre els elements TIC del centre: servidors, sistemes d'emmagatzematge, cabines de discos, electrònica de xarxa, bases de dades, plataformes de virtualització, sistemes de còpia de seguretat, comunicacions i integritat de la informació.

De moment, ja s'ha identificat afectació sobre com a mínim un element crític de la infraestructura TIC: un commutador de nucli, fet que ha obligat a modificar la configuració del nucli central de xarxa del CPD. Aquest fet confirma que l'incident no s'ha limitat al SAI ni a la infraestructura elèctrica, sinó que ha tingut impacte directe sobre components essencials del sistema informàtic.

Aquesta circumstància incrementa el nivell de risc, perquè poden existir danys latents encara no detectats. Una aturada sobtada pot provocar errors que no es manifesten immediatament, però que poden aparèixer posteriorment en forma de fallades de discos, degradació de rendiment, corrupció de volums inconsistències en bases de dades, problemes de comunicació, pèrdua de redundància o indisponibilitat de serveis crítics. Per aquest motiu, cal considerar que el risc continua obert fins que no s'hagi verificat tècnicament l'estat complet de la infraestructura TIC i la integritat de les dades.

No estem només davant el risc de quedar-nos sense informàtica «uns dies». Estem davant el risc de perdre informació crítica incórrer en incompliments legals i comprometre la capacitat institucional del CAR per funcionar i complir les seves obligacions.

Aquest risc és especialment greu perquè el CAR gestiona informació d'alt valor i d'alta sensibilitat incloent dades mèdiques, científiques, esportives, administratives, econòmiques i contractuals. La pèrdua, corrupció o indisponibilitat d'aquesta informació podria afectar la continuïtat operativa del centre, la protecció de dades, la transparència, la capacitat de resposta davant requeriments legals, la presentació d'informes, la comptabilitat, la fiscalitat, la justificació documental i la relació amb altres administracions o organismes de control.

Per tant, l'emergència no ha de limitar-se a la substitució de bateries o a la posada en marxa del SAI. Ha d'incloure la revisió completa del SAI, la substitució dels components en fi de vida, la formalització immediata d'un contracte de manteniment, la revisió de la infraestructura elèctrica, la diagnosi i reparació dels elements TIC afectats, la verificació de la integritat de dades, la comprovació de les còpies de seguretat, la definició d'un pla de continuïtat i recuperació davant desastres i la dotació dels recursos econòmics i humans necessaris.

La situació actual ha de ser considerada una estabilització provisional, no una normalització definitiva. El CPD ha recuperat part de la seva operativitat, però encara no es pot afirmar que el sistema hagi recuperat un nivell acceptable de seguretat, fiabilitat i resiliència. Fins que no s'hagin identificat i corregit els danys, verificat els sistemes crítics i implantat les mesures estructurals necessàries, el CAR continua exposat a una nova afectació greu.

La conclusió és clara: el SAI ha tornat a funcionar, però la urgència continua justificada perquè el risc real afecta la continuïtat institucional del CAR, la integritat de la informació, el compliment legal i la capacitat del centre per operar amb garanties.

Cap del Departament d'Informàtica