# INFORME JUSTIFICATIU PER A LA CONTRACTACIÓ D'EMERGÈNCIA DE SERVEIS CRÍTICS DE CIBERSEGURETAT I INFRAESTRUCTURA TIC

## 1. Objecte de l'informe:

L'objecte del present informe és **justificar, amb fonament tècnic i jurídic, la necessitat d'activar un procediment de contractació per via d'emergència**, d'acord amb l'article 120 de la Llei 9/2017, de Contractes del Sector Públic (LCSP), per a la **contractació immediata de serveis especialitzats en ciberseguretat i infraestructura TIC.**

Aquests serveis són **estratègics i crítics per garantir la continuïtat operativa, la integritat dels sistemes d'informació i la protecció de dades sensibles** d'Infraestructures.cat, especialment en el context de l'atac sofert recentment que ha posat en risc la seguretat tecnològica i institucional de l'organització.

## 2. Detecció i justificació necessitat immediata:

El dilluns 2 de juny de 2025, l'Agència de Ciberseguretat de Catalunya va comunicar a Infraestructures.cat la detecció d'una publicació en un fòrum de la dark web, atribuïda al grup APOS Ransomware. En aquesta publicació es notificava el compromís d'un servidor d'Infraestructures.cat i s'hi incloïa una amenaça explícita d'exposar dades suposadament exfiltrades, en cas de no satisfer el pagament d'un rescat econòmic.

Posteriorment, el divendres 6 de juny de 2025, tant l'Agència de Ciberseguretat de Catalunya com l'empresa NTT DATA Spain —proveïdor contractat per Infraestructures.cat per a la prestació de serveis de gestió TIC— van confirmar que el ciberatac s'havia estès a altres servidors de l'organització, impactant de manera transversal sistemes crítics de la infraestructura tecnològica corporativa.

**Ens trobem, per tant, davant una situació de màxima gravetat, amb afectació directa a la continuïtat operativa d'Infraestructures.cat, a la integritat i confidencialitat de la informació —inclosa informació sensible, estratègica o protegida— i, de forma indirecta però no menys rellevant, a la confiança institucional i ciutadana envers aquesta entitat pública.**
La naturalesa de l'amenaça, la seva propagació i el grau de sofisticació detectat evidencien que no és possible gestionar ni contenir aquesta crisi amb mitjans ordinaris. L'atac ha posat en risc l'estabilitat del sistema d'informació corporatiu, i la resposta ha de ser immediata i tècnicament robusta. No actuar amb diligència pot derivar en una exposició pública de dades, paralització de serveis essencials i una escalada de danys reputacionals, legals i operatius de conseqüències imprevisibles. **La inacció o l'endarreriment de les mesures proposades suposaria un risc crític i inacceptable.**

D'acord amb les recomanacions emeses per l'Agència de Ciberseguretat de Catalunya, i amb l'objectiu imprescindible de contenir l'atac, restaurar la seguretat i prevenir futurs vectors d'amenaça, resulta absolutament necessari activar —mitjançant contractació per via **emergent**— les actuacions següents, de manera immediata, de conformitat amb el que preveu l'article 120 de la Llei 9/2017, de Contractes del Sector Públic (LCSP):

- **Desplegament d'una solució EDR (Endpoint Detection and Response)**, per assegurar la detecció i resposta proactiva i automatitzada davant de qualsevol nova intrusió o activitat maliciosa.
- **Activació d'un SOC (Centre d'Operacions de Seguretat) 24x7**, amb capacitat de monitoratge continu i resposta immediata a incidents de seguretat.
- **Implantació d'un sistema PAM (Privileged Access Management)**, per limitar i controlar els accessos privilegiats i reduir el risc de moviments laterals dins la infraestructura.
- **Segmentació de la xarxa i bastionat dels servidors crítics**, per aïllar els entorns vulnerables, limitar la propagació i protegir els actius més sensibles.

- **Desplegament de Microsoft Intune i de la suite EMS**, com a plataforma centralitzada per a la gestió segura de dispositius, aplicacions i identitats.
- **Remediació immediata de vulnerabilitats greus** detectades en el marc dels treballs d'anàlisi forense i d'auditoria tècnica postincident.

Aquest conjunt d'actuacions s'estima en un cost aproximat de **650.000 euros**, justificats pel nivell de risc i abast de les intervencions requerides. Cal remarcar que es tracta d'accions crítiques, no ajornables i ineludibles per preservar la funcionalitat operativa i la seguretat dels sistemes d'Infraestructures.cat.

A més, cal destacar que **Infraestructures.cat actua com a ens instrumental de la Generalitat de Catalunya**, prestant serveis essencials a diversos departaments i organismes públics, entre els quals es troben:

- Departament de Territori
- Departament de Salut
- Departament d'Educació
- Altres entitats i organismes del sector públic

En aquest sentit, una vulneració de la seguretat, una interrupció dels serveis TIC o una fallada en la disponibilitat dels sistemes no només impactaria Infraestructures.cat, sinó que tindria **conseqüències directes sobre la capacitat de gestió d'inversions públiques** i en l'execució dels encàrrecs que es gestionen des d'Infraestructures.cat per compte dels seus clients. Per tant, **la protecció de la infraestructura tecnològica i de la informació corporativa no és un objectiu intern aïllat, sinó una condició indispensable per garantir la continuïtat d'un servei públic essencial i estructural** per a l'administració catalana.

**Qualsevol demora en l'execució suposaria posar en risc la continuïtat del servei públic, l'exposició massiva d'informació corporativa i de tercers, així com una pèrdua de confiança institucional difícilment reparable.**

A més, **la necessitat de l'actuació no ha pogut ser prevista amb antelació per part de l'òrgan de contractació i no ha estat provocada per una actuació negligent ni d'aquest ni dels seus serveis.** En el context d'emergència actual, **els procediments de contractació ordinaris no resulten adequats per donar resposta a la situació plantejada, especialment pel temps que comportaria la tramitació i execució de les actuacions necessàries**, la qual cosa comprometria greument la seguretat, la disponibilitat i la continuïtat del servei públic que Infraestructures.cat presta com a ens instrumental de la Generalitat de Catalunya.

Per tot l'exposat, i considerant que concorren de manera clara i objectiva les circumstàncies que preveu l'article 120 de la LCSP per a l'aplicació de la contractació d'emergència, es proposa procedir a la **contractació directa i immediata dels serveis esmentats**. Cap altra alternativa permet assolir en temps i forma les mesures de resposta requerides, i només aquest mecanisme pot garantir el restabliment segur i immediat de les operacions.

Per tot això, i atesa la necessitat de desplegar de forma immediata les actuacions descrites, **es proposa que l'adjudicació del contracte es formalitzi a favor de l'empresa NTT DATA Spain Infraestructures Engineering, S.L.U., proveïdor actual d'Infraestructures.cat per als serveis de gestió TIC**, per raó de **la seva solvència tècnica acreditada, la seva experiència contrastada en serveis especialitzats de resposta a incidents de ciberseguretat i el coneixement operatiu detallat de l'arquitectura TIC corporativa**. Aquesta condició permet garantir una resposta efectiva, immediata i coordinada amb l'ecosistema tecnològic existent, i ofereix la màxima garantia de continuïtat en un context d'emergència com l'actual.

**3. Conclusió:**

En virtut de tot l'exposat, i davant la gravetat i l'excepcionalitat de la situació descrita, es proposa:

- **Procedir a la contractació per via d'emergència** dels serveis tècnics detallats en aquest document, limitant-ne l'abast temporal al període estrictament necessari per garantir el restabliment de la seguretat, la continuïtat dels serveis i la contenció de la situació actual.
- Paral·lelament, Infraestructures.cat ja ha iniciat els tràmits ordinaris de **licitació dels serveis de continuïtat**, d'acord amb la planificació tècnica i jurídica prevista, per tal d'assegurar una transició ordenada cap a un marc contractual estable.
- **Formalitzar si escau la contractació emergent** d'acord amb el que estableix l'article 120 de la Llei 9/2017, de Contractes del Sector Públic (LCSP), amb la corresponent justificació documentada davant dels òrgans de contractació competents, atenent els principis de necessitat, proporcionalitat i interès públic que fonamenten aquesta actuació excepcional.

Alex Tablado Vergara
Cap de la Gerència de Projectes i Serveis TIC
Barcelona, 30 de juny de 2025