Informe d'impacte i d'actuacions relacionades amb la incidència TIC del dia 17 de novembre de 2018

El dia 17 de novembre de 2018 es va produir una incidència en els serveis TIC de la Universitat Autònoma de Barcelona. La causa de la incidència va ser un tall de subministrament elèctric seguit d'una sobretensió que va afectar a la climatització de Centre de Processament de Dades (CPD) de la Universitat. Els variadors que regulen la impulsió d'aire del sistema de climatització es van bloquejar degut a sobretensió, cosa que va fer augmentar ràpidament la temperatura del CPD, fins a arribar a nivells superiors als màxims especificats per l'equipament que hi ha instal·lat tot i la ràpida resposta dels equips de seguretat i manteniment del Campus. L'activació de les alarmes dels sistemes de monitorització també van mobilitzar els tècnics de la Direcció TIC així com els de l'empresa que ens dona suport, que van desplaçar-se a l'edifici D immediatament.

Com a conseqüència d'aquest augment de temperatura el sistema d'emmagatzematge on s'allotgen una gran part de les dades corporatives va patir la fallada de 5 discs. Tot i tractar-se d'un equip altament redundant i configurat per tal minimitzar la possibilitat de fallada segons les pràctiques recomanades pel fabricant, es va donar la circumstància de que van fallar simultàniament 2 discs d'un grup de 5 en configuració RAID5, cosa que va provocar la pèrdua de l'accés a les dades emmagatzemades al volum del què formava part aquest grup de discs.

La incidència es va escalar immediatament a l'equip d'especialistes de suport de l'empresa fabricant de l'equip. Després de múltiples intents de recuperació de dades que van involucrar especialistes europeus i nord-americans, cap a les 12 de la nit de dissabte dia 17 de novembre se'ns va informar que seria impossible recuperar les dades del sistema danyat.

El volum afectat per la incidència contenia les imatges dels sistemes operatius de la major part de màquines virtuals i el servei de carpetes compartides, entre d'altres. Cal remarcar que els volums que contenen les bases de dades corporatives (sistemes de gestió econòmica, docent, de recerca, de personal, etc.) no es van veure afectades per l'incident.

Vam procedir immediatament a la recuperació de les dades afectades a partir de la còpia de seguretat que s'havia dut a terme a primera hora del dia 15 de novembre. La major part de sistemes corporatius, incloent-hi els que afecten a les bases de dades corporatives estaven plenament operatius dimecres 21 de novembre. La recuperació de les dades de les carpetes compartides va finalitzar divendres 23 de novembre.

Al llarg de la setmana del 26 de novembre es van posar en funcionament la resta de serveis, incloent-hi els entorns de test i desenvolupament. El dia 1 de desembre es va fer una aturada programada dels sistemes per tal de recuperar el rendiment del sistema.

Afectació a les dades

Les dades incloses en les bases de dades corporatives (sistemes de gestió econòmica, docent, de recerca, de personal van estar no disponibles des del moment de la incidència fins dimecres 21 de novembre. La seva integritat o confidencialitat no van estar afectades en cap moment.

Pel que fa a les dades del servei de "carpetes compartides", van estar no disponibles des del moment de la incidència fins divendres 23 de novembre. Les modificacions produïdes al llarg de divendres 16 de novembre no es van poder recuperar, ja que l'última còpia de seguretat

completa disponible en el moment de l'incident és la que correspon al matí de divendres 16. La confidencialitat d'aquestes dades no va estar afectada en cap moment.

Mesures implementades

Per tal de disminuir riscs futurs, s'han instal·lat i connectat a la central d'alarmes sensors addicionals de temperatura, gir dels ventiladors, i pressió. S'han revisat els variadors afectats i s'han modificat per tal que es re-iniciïn automàticament en cas de parada. El sistema de monitoratge i d'alarmes ha estat comprovat realitzant diverses simulacions de diferents escenaris de desastre.

Mesures planificades

Per tal de millorar la resiliència del sistema en cas de fallades i el pla de contingència s'estan estudiant els requeriments per reforçar el CPD de l'edifici Rectorat i implementar-hi un sistema de replicació de dades, així com l'enviament diari dels fitxers de backup a una localització fora del Campus. Tot i que la resposta dels equips humans ha estat excepcional, estem revisant els procediments de resposta a nivell organitzatiu, comunicatiu i tècnic per identificar possibles millores i incloure totes les lliçons apreses a nivell preventiu i reactiu.