Ciberatac a la UAB “11/10/2021”

Descripció, anàlisi, febleses
Solucions
Accions immediates i a mig termini

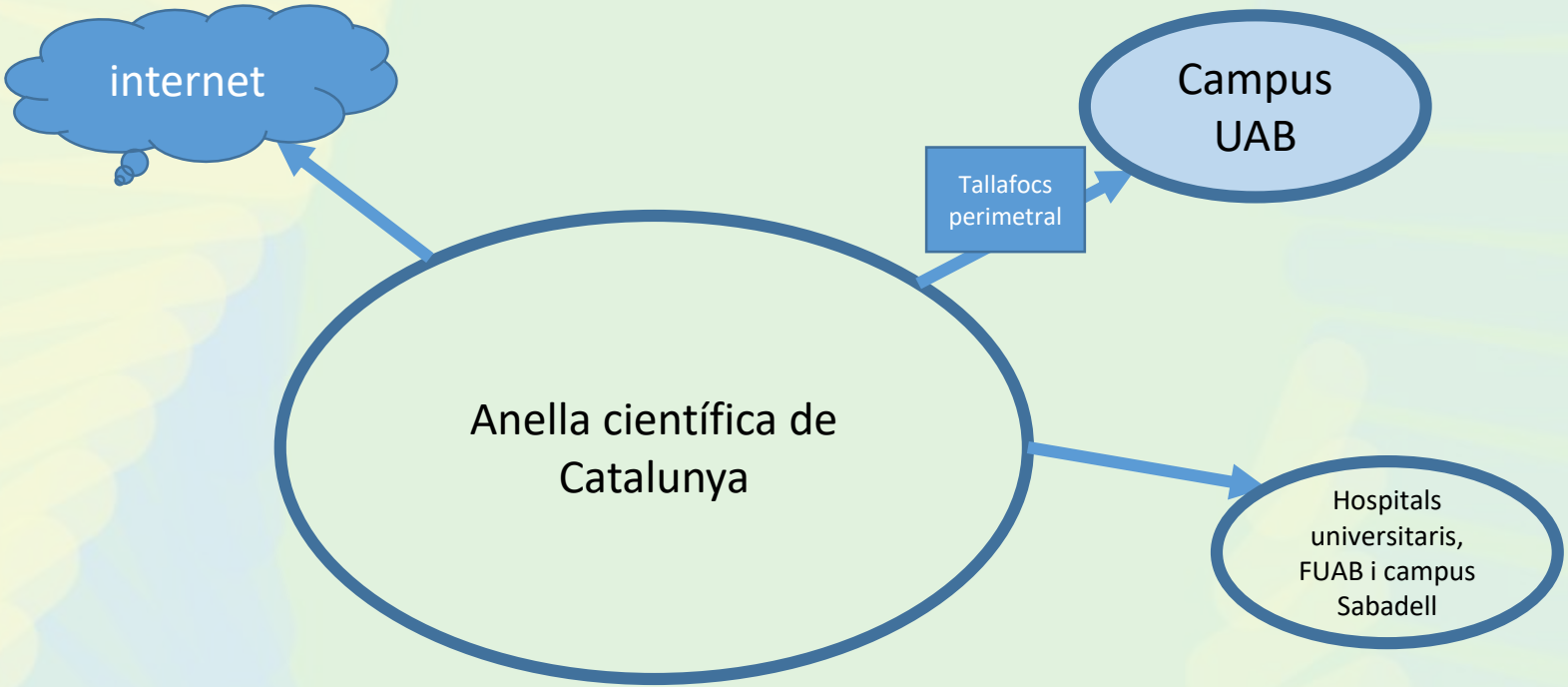
Les exigències de ciberseguretat s ’han disparat i ens igualen a tots els Serveis Públics sense distinció.

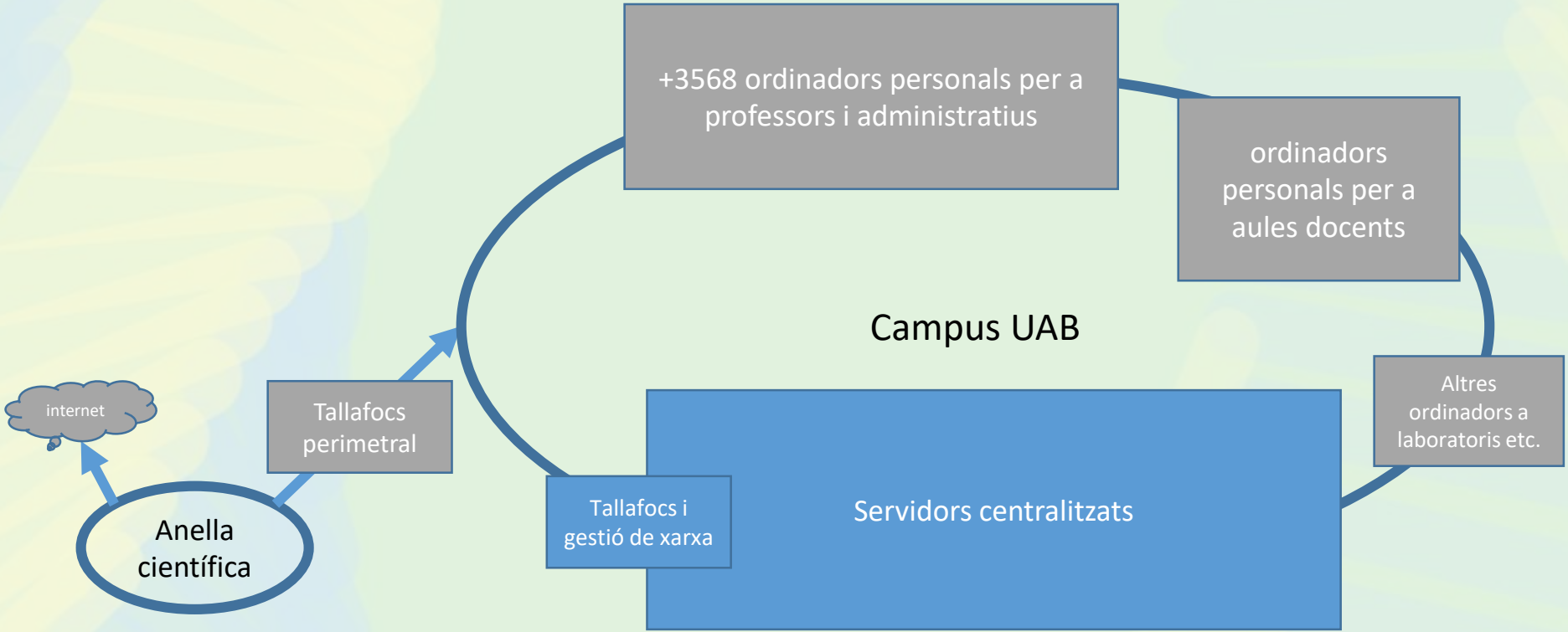
La qüestió no és si ens atacaran sinó quan.

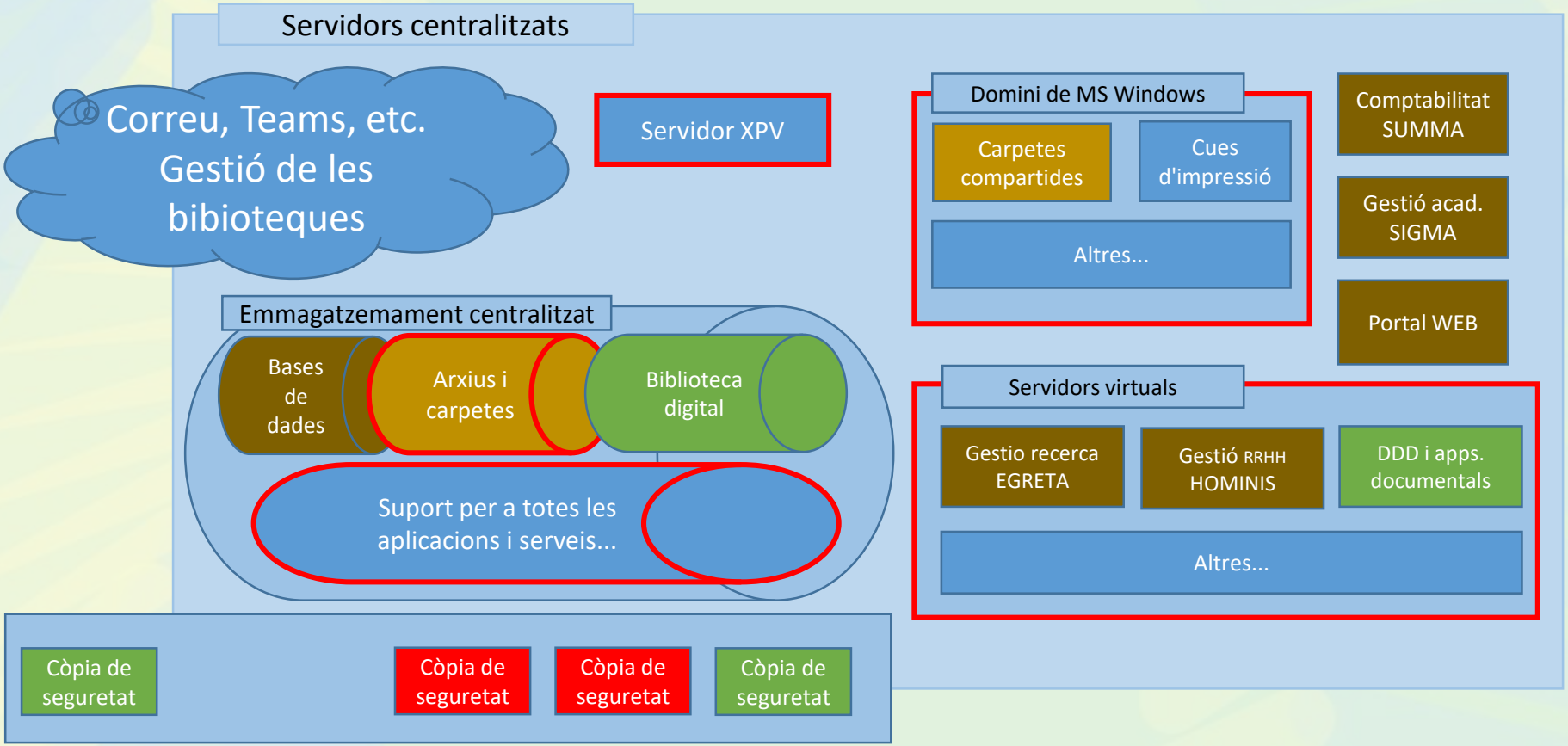
Agència de Ciberseguretat de Catalunya

01

Breu descripció de la infraestructura TIC de la UAB


internet
Campus UAB
Tallafocs perimetral
Anella científica de Catalunya
Hospitals universitaris, FUAB i campus Sabadell


+3568 ordinadors personals per a professors i administratius
ordinadors personals per a aules docents
Campus UAB
Altres ordinadors a laboratoris etc.
internet
Tallafocs perimetral
Anella científica
Tallafocs i gestió de xarxa
Servidors centralitzats


Servidors centralitzats
Correu, Teams, etc.
Gestió de les bibioteques
Servidor XPV
Domini de MS Windows
Carpetes compartides
Cues d'impressió
Altres...
Comptabilitat SUMMA
Gestió acad. SIGMA
Portal WEB
Emmagatzemament centralitzat
Bases de dades
Arxius i carpetes
Biblioteca digital
Suport per a totes les aplicacions i serveis...
Servidors virtuals
Gestio recerca EGRETA
Gestió RRHH HOMINIS
DDD i apps. documentals
Altres...
Còpia de seguretat
Còpia de seguretat
Còpia de seguretat
Còpia de seguretat

02

Com es va produïr l'atac

Cadena d‘esdeveniments

Fase preparatòria (del 22-set al 10-oct)

- Captura de credencials d‘un usuari (phishing?)
- Login a la nostra XPV (accés remot autenticat per usar serveis des de fora de la UAB)
- Es guanya visibilitat de certs recursos
- Elecció d‘un objectiu segons les eines d‘atac (servidor windows)
- Elevació de privilegis amb un *malware* (accés indegut a la RAM i captura de credencials d‘administrador)
- Explotació del status d‘administrador i propagació d‘eines a tots els servidors de domini
- Anàlisi de la nostra arquitectura de sistemes, de xarxa i de còpies de seguretat (Dart unix)
- Atac de la plataforma de virtualització amb altres *malware* (VMware)
- Desplegament de les eines de *ransomware* (desactivador de defenses, encriptador, etc.) a tots els entorns penetrats

Cadena d‘esdeveniments (II)

Fase d’execució (1.30h del dilluns 11/10/2021)

- Desactivació antivirus i altres defenses dels controladors de domini windows
- Encriptació de les unitats de xarxa
- Encriptació de les màquines virtuals
- Esborrat d‘alguns jocs de còpies de seguretat (tasca no finalitzada)
- Encriptació dels ordinadors personals de campus que estàven engegats a aquella hora (tasca no finalitzada)
- Esborrat automàtic d‘eines i evidències (tasca no finalitzada)

L‘atac en tres paraules:

Penetració
Anàlisi i desplegament
Encriptació d‘arxius

03

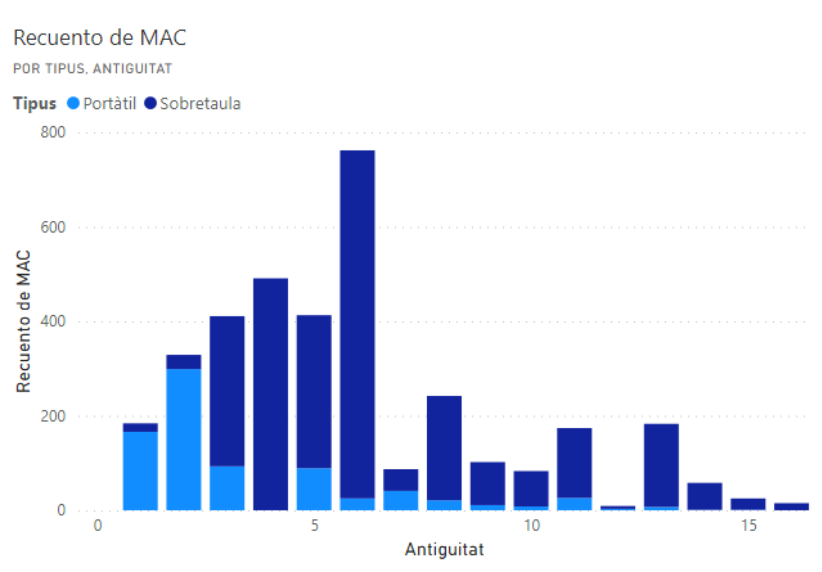
Febleses

Parc de PC i servidors amb greu obsolescència (I)

- PC's antics (problemes econòmics de renovació) amb sistema operatiu no actualitzable i, per tant, insegur.

- Servidors pendents d'actualitzar per:
  - si s'actualitzava, els pc's amb sistema operatiu més antic deixaven de funcionar
  - augmentava el cost anual
  - algunes aplicacions antigues deixarien de funcionar

Parc de PC i servidors amb greu obsolescència (II)



> 5 anys

Tipus	Recuento de MAC
Sobretaula	1596
Portàtil	144
Total	**1740**

TOTAL

Tipus	Recuento de MAC
Sobretaula	2777
Portàtil	791
Total	**3568**

Presentació de serveis a la xarxa (superfície d'atac).

- Moltes configuracions de teletreball durant la pandèmia van resultar un problema de seguretat
- Disseny de l'accés d'administrador massa transversal
- Disseny poc restrictiu per a maximitzar els usos

Feblesa en la gestió de la identitat digital

- Si una contrasenya quedava compromesa no hi havia un segon factor d'autenticació per a tota la comunitat (ja s'havia implementat a l'alumnat)

- No hi havia mecanismes per a comprovar la robustesa de la gestió de contrasenyes.

Manca d'eines de supervisió i vigilància

- Eines per l'auditoria de l'activitat d'administradors
- Altres específiques anti hacking
- Monitorització 24x7 en temes de seguretat (SOC)
- Eines automatitzades d'anàlisi de comportaments sospitosos

Resum febleses:

Obsolescència PC i Sistema Operatiu
Superfície d'atac inadequada
Feblesa gestió de contrassenyes
Manca d'eines de supervisió i vigilància

04

Solucions

Compromís de credencials (inici de l'atac)

- Implementació del doble factor (2FAS)
  - Nivell pc, nivell correu, nivell aplicacions (essencialment totes les presentacions de credencials)
- Utilització d'eines estàndard. L'usuari podrà escollir l'eina de segon factor:
  - Trucada al despatx, sms (s'ha de conèixer el número de telèfon)
  - app al mòbil o programari lliure instal·lat a un segon ordinador (no cal compartir cap element personal) *es genera un número a presentar segons l'hora-minut i un "secret" compartit entre la app i els nostres servidors. Protocol obert amb fiabilitat contrastada.*
- Detecció automàtica de comportaments sospitosos
  - intents múltiples, accessos simultanis des de diferents països, ús de protocols febles...

Control d’accés a la xarxa (segmentació de la visibilitat)

- verificació del nivell d’actualització del sistema operatiu i antivirus
  - autorització per usar xarxa restringida a aplicacions crítiques
  - derivació a subxarxes amb altres controls
    - xarxa per a alumnes, visitants
    - xarxa per a aparells de laboratori
    - **Totes les subxarxes que calgui per garantir el servei a tothom**

Mecanismes per a evitar elevació de privilegis d'administrador

- Utilització dels processadors de seguretat per a gestionar contrasenyes i/o PINs, que tenen els pc homologats
  - Això elimina la permanència d'informació sensible a la RAM

- Solució tecnològica per evitar les conseqüències de que l'usuari de cada PC és a l'hora administrador de la seva màquina.

Portal de programari verificat

- Sistema d'actualització, control de versions autèntiques i disponibilitat de programari per a pc.
- Comencem amb les eines bàsiques i anirem creant un espai tipus "play" on es trobaran les aplicacions actualitzades i garantides per a desenvolupar les tasques.

Renovació automàtica dels ordinadors amb més de 6 anys d'antiguitat

- A càrrec de la DTIC
- Maquinari amb capacitat per desenvolupar el teletreball (ordinador portàtil) i totes les tasques essencials tant de docència com de gestió i una part de les de recerca.
- **Totes les solucions esmentades estaran implementades en aquests ordinadors portàtils**

Resum solucions:

Implantació del doble factor (2FAS)
Control d‘accés a la xarxa (NAC)
Gestió restringida d‘administrador PC
Portal de programari verificat
Renovació automàtica del PC als 6 anys

05

Reconstrucció

Restauració de Serveis (trets generals)

- Valoració cas per cas entre recuperació i reconstrucció
  - En la majoria dels casos apostem per la reconstrucció per evitar contaminacions amagades
  - Aprofitem per fer canvis de S.O. (migració de Solaris a Linux) i actualitzacions
- Redisseny de les regles de tallafocs. Molt més restrictives
- Replanteig de serveis difícils de securitzar
  - Nou enfoc per a carpetes compartides i Nébula
- Demanem als administradors externs a DTIC (housing) que securitzin els seus sistemes
  - *Vam haver de tornar a tancar housing perquè només obrir-lo vam rebre avisos de ACC i de INCIBE de febleses detectades.*

Restauració de Serveis (I)

- Vam habilitar immediatament una web provisonal per comunicar amb la comunitat
- Fins al dia +4 no vam assegurar una còpia de seguretat vàlida
- La reconstrucció de l'entorn d'emmagatzemament va necessitar més d'una setmana
- Vam habilitar una xarxa wifi i les connexions amb cable a la setmana +1
- Es va garantir els cobraments de nòmina amb la col·laboració del proveïdor del programari fent els càlculs als seus ordinadors.
- Hem canviat TOTES les contrassenyes de la comunitat universitària
- Es van prioritzar les reconstruccions de les gestions econòmiques i acadèmiques atenent al periode comptable i les fites del calendari acadèmic
- Per al campus virtual es va decidir oferir una alternativa per a la resta del semestre
- L'entorn de la gestio de la recerca es va posar en marxa usant temporalment les infraestructures del proveïdor

Restauració de Serveis (II)

- S'ha construit una nova solució de desplegament d'ordinadors personals completament diferent a l'anterior (el que en diem el planxat)
- Estem realitzant tasques sense bona part dels sistemes de gestió de la infraestructura que disminueixen la velocitat del desplegament d'ordinadors (Corregit a l'inici de gener).
- Hem de mantenir un equilibri de tasques de reconstrucció entre fites inajornables i els sistemes d'infraestructura esmentats
- Al llarg dels mesos de gener i febrer augmentarem la velocitat de reconstrucció progressivament. A títol d'exemple:
    - *Autenticació préstec Biblioteques* — *avui mateix*
    - *Seu electrònica* — *10 de gener*
    - *Correcció d'exàmens* — *14 de gener*
    - *Nexus* — *19 de gener*
    - *Apps (PDS, TPD, Guies docents, etc.)* — *28 de gener*
    - *DataWareHouse* — *31 de gener*

Resum reconstrucció :

En menys de 10 dies teniem normalitat de correu i connectivitat bàsica
Les infraestructures bàsiques es reconstrueixen simultàniament als entorns prioritzats
Moltes tasques es fan sense automatització i tenen baixa velocitat
En les primeres setmanes de 2022 augmentarem la velocitat de reconstrucció

06

Accions

Accions immediates de contingència

Aportació específica de 3.7 Milions d'euros per part de la Generalitat

• Despeses confecció anàlisi forense i supervisió i validació de les accions de recuperació. Serveis urgents d'operació i actuacions en infraestructura.	500.000 €
• Adquisició de 1.200 ordinadors personals per a substituir el material obsolet	1.200.000 €
• Adquisició de 1.100 ordinadors d'aula per a retirar els més obsolets	880.000 €
• Virtualitzacio d'escriptoris i aplicacions de docència	100.000 €
• Contractació de les llicències de complements de seguretat per als 3.568 pc's dels treballadors de la UAB.	240.000 €
• Contractació d'un servei de vigilància contínua de la ciberseguretat	120.000 €
• Construcció d'un DRS (Disaster Recovery Service). Es tracta d'una instal·lació a campus que garantiria la posada en marxa immediata d'un sistema de contingència.	750.000 €

Accions a mig termini (I)

- Revisió i proposta de traslladar alguns serveis al núvol
  - Ara tenim el correu i la gestió de les biblioteques
  - Es preveu consolidar la gestió de la recerca EGRETA i recursos humans HOMINIS de forma immediata.
  - Allotjarem el portal web al núvol als voltants de setmana santa.
  - Altres opcions en estudi
- Eliminació definitiva de servidors amb opcions tecnològiques sense continuïtat (Sun Solaris sobre Sparc)
- Millora de la resiliència de serveis i bases de dades
  - Implantació de la elasticitat de recursos (UAB + NÚVOL)
  - Implantació de bases de dades distribuïdes (CPD1, CPD2, NÚVOL)

Accions a mig termini (II)

- Finalització de la renovació de la xarxa amb gestió dinàmica i garanties de seguretat addicionals.
- Automatització completa de les configuracions i servidors fins a arribar a complir el concepte de Datacenter as Code (DaC o IaC per la infraestructura).
    - Aquesta fita evita la intervenció manual en les reconfiguracions i ampliacions. Es realitzen a la velocitat del maquinari (minuts vs. hores o dies)
    - També, en cas de contingència parcial, les reconstruccions es fan a velocitat del maquinari i no de l'operador humà.
    - El disseny complet del DaC també alimentaria el sistema de recuperació de desastres.
- Continuació dels treballs per a complir l'Esquema Nacional de Seguretat
- Revisió de les habilitats i coneixements necessaris a la plantilla DTIC, propiciant els canvis, formacions i habilitacions professionals que siguin necessaris.

Resum accions :

Anàlisi forense del ciberatac
Compra extraordinària renovació PCs antics
Adquisició de programari de seguretat
Servei de cibervigilància contínua
Creació d'un bunker de contingència
Redisseny de sistemes
Automatització avançada
Esquema Nacional de Seguretat (certificació)
Reciclatge i modernització de la plantilla DTIC.