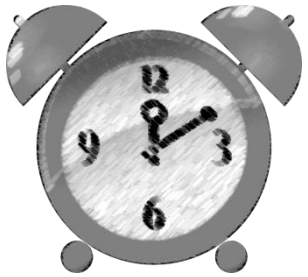
Unicane: Ejercicio de Cibercrisis en las Universidades Catalanas

Maria Isabel Gandía
CSUC/CATNIX

23º Foro ESNOG
MediaLab Prado, 16-05-2019

Una crisis cualquiera en una universidad cualquiera

- ✓ Estás trabajando tranquilamente en tu sitio.
- ✓ Cuando, sin que te dé tiempo a entrar en los equipos…



- ✓ Empieza la carrera contra el reloj!!

Curiosidades de la última “mini-crisis” (diciembre)

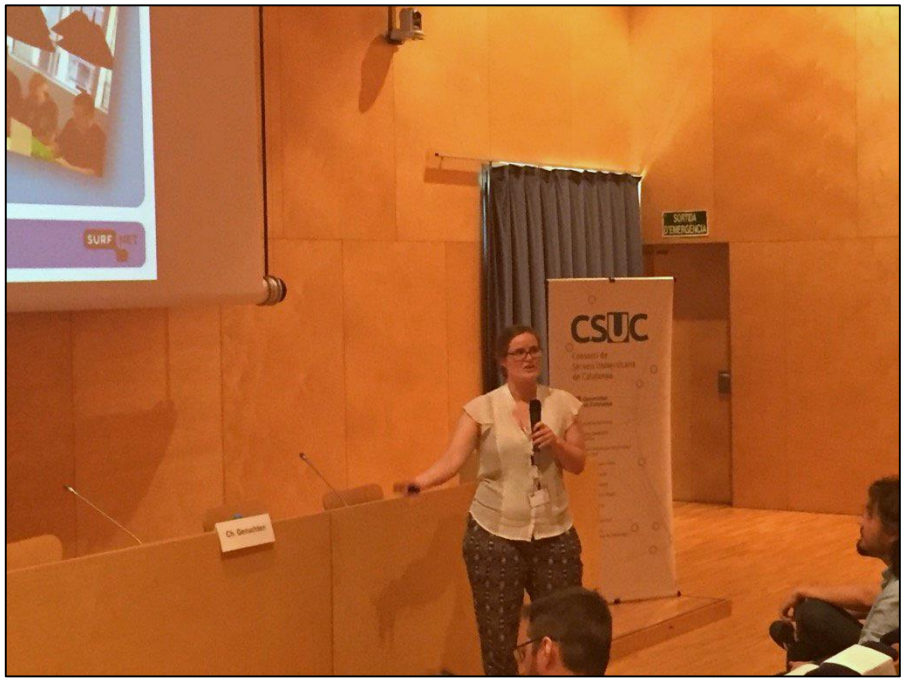
- ✓ Afectó a la Anella Científica (red académica de Catalunya).
- ✓ La red iba leeeentaaaaa.
- ✓ En 45 minutos recibimos:
  - 58 llamadas.
  - 300 alertas de pérdidas o cortes
  - 7 mensajes de usuarios preguntando
  - 1 tweet

- ✓ Consultamos 400 gráficas.

- ✓ Fue un ataque de DDoS contra 2 de nuestras IP, de 3 horas de duración (45 minutos de afectación).

¿Por qué organizamos una Jornada de gestión de crisis?

- ✓ SURFnet (red académica holandesa): OZON
- ✓ Presentación en 2017 a la Anella Científica (en la TAC).



- ✓ Las universidades nos pidieron que organizásemos una.
- ✓ Géant (red académica pan-Europea): CLAW Crisis Management Exercise.
- ✓ El CSUC participó en los “CLAW” de 2017 y 2018.

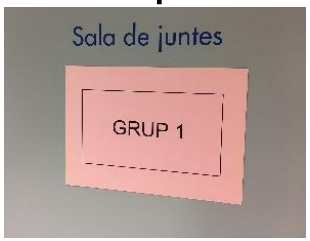
¿Cómo lo hicimos?

Le llamamos UNICANE

- ✓ Reunimos a más de 40 participantes de las Universidades.
- ✓ Expertos de varios ámbitos:
  - Redes
  - Gestión TIC
  - Comunicación
  - Seguridad TIC
  - …y algunos unicornios

- ✓ Los participantes se distribuyeron en 4 grupos
- ✓ Nos distribuimos en 4 salas.
- ✓ Se repartieron 7 roles:
  - Coordinador/a de crisis
  - Director/a de Servicios Informáticos
  - Responsable de seguridad
  - Responsable de comunicación
  - Secretario/a
  - Responsable de red
  - Relaciones públicas

- ✓ Otros participantes de las universidades actuaban como observadores.
- ✓ Cuatro miembros del CSUC actuaban como líderes.
- ✓ Y empezó el ejercicio…

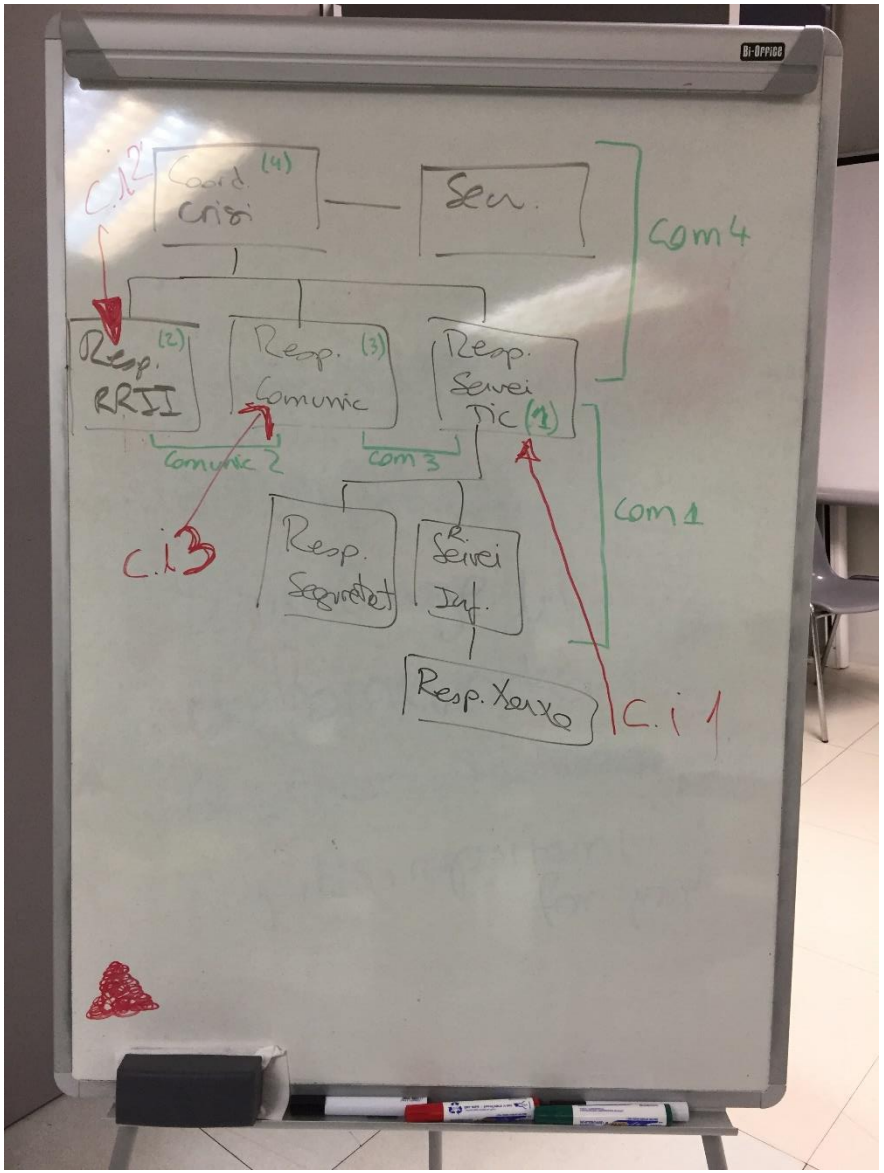


Equipo de gestión de crisis de la Universidad de los Pirineos

Asignación de roles

Asignación de roles

Asignando roles



Lectura del caso

Buscando alternativas

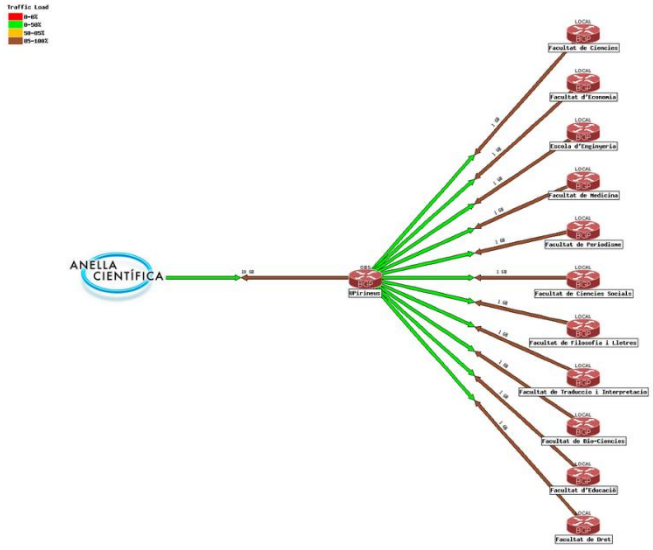
Buscando alternativas

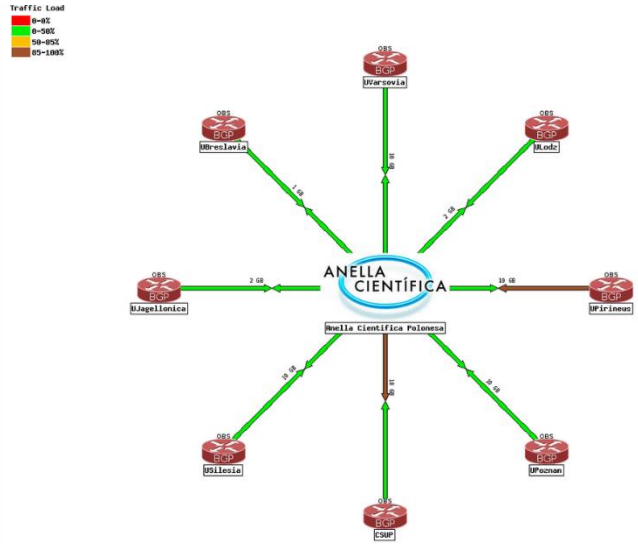
Interpretando pistas

Interpretando pistas

Canales y Timeline

- ✓ Contenido multimedia previamente cargado en un canal de Rocket.
- ✓ Los líderes teníamos un canal paralelo y unas instrucciones comunes.
- ✓ Íbamos introduciendo las “cápsulas informativas” a la vez.
- ✓ La información llegaba con cuentagotas:
  - 12:05: Los sistemas de monitorización del CSUP muestran incremento de tráfico.
  - 12:07: Llamada del Decano.
  - 12:10: Llega un *weathermap* de la Universidad y otro del CSUP.





Timeline (2)

- ✓ 12:12: Llamada de Rectorado.
- ✓ 12:15: El CSUP-CSIRT informa de que la Universidad está atacando al CSUP.
- ✓ 12:17-12:20: Llaman de varios periódicos.
- ✓ 12:30: El CESIPOL (Centro de Seguridad Informática de Polonia) relaciona el problema con el bug memcrashed y aporta una regla para el router o firewall para solucionarlo.
- ✓ 12:40 VC del Director General de Universidades.
- ✓ 12:45: No funciona Eduroam.
- ✓ 12:50: Llama el Decano.
- ✓ 12:57: Llamadas de la Universidad.
- ✓ 13:00: Game over

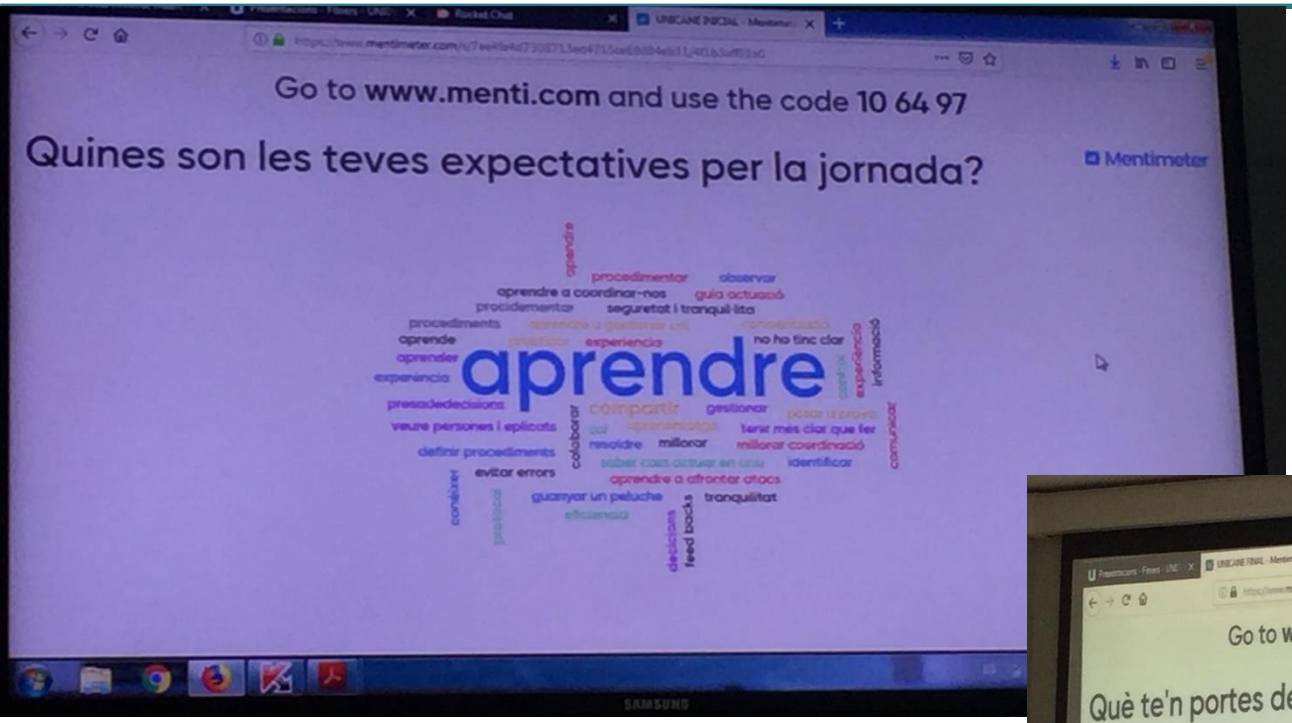
Algunas conclusiones de la jornada, sobre las crisis

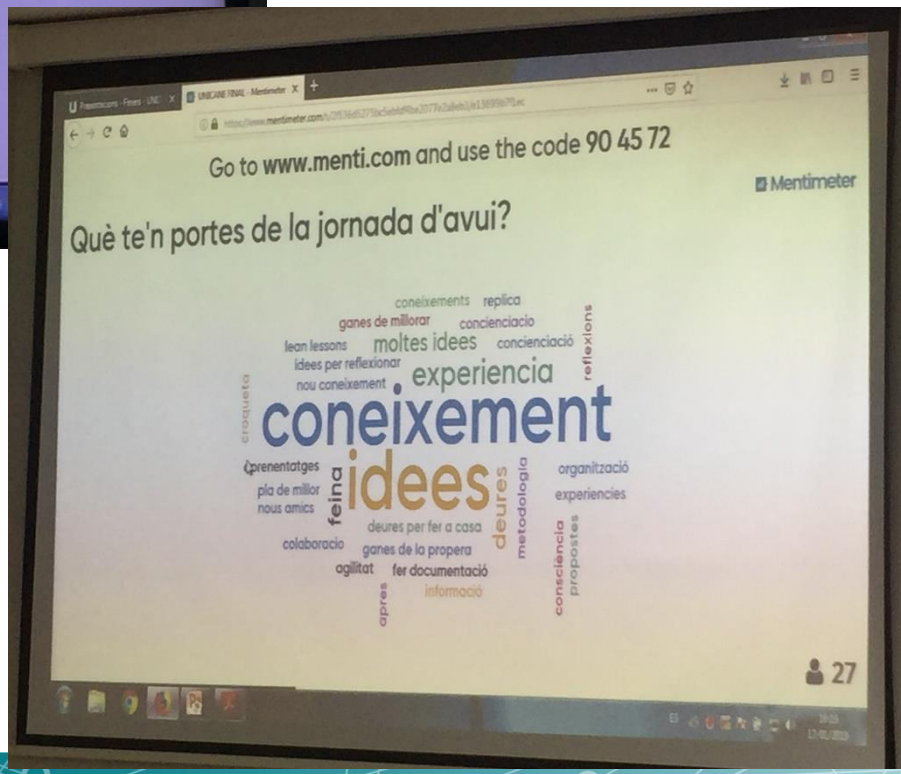
- ✓ Hay que tener un plan de gestión de crisis, aunque sea muy básico. Luego ya se irá puliendo (mejora continua).
  - Roles
  - Flujos de comunicación
  - Procesos
- ✓ A nivel de coordinación:
  - Aunque los técnicos se coordinen, hay que implicar al equipo de Comunicación. La imagen de la universidad es importante.
  - Aconsejable que los técnicos se centren en resolver la incidencia.
- ✓ A nivel de comunicación:
  - Las redes sociales son cada vez más relevantes.
  - No se pueden obviar sus mensajes, ni contestar sin contrastar.

Algunas conclusiones de la jornada, sobre el ejercicio

- ✓ Los 4 equipos consiguieron encontrar alguna solución creativa, aunque no fuese perfecta.
- ✓ El *feedback* fue muy positivo.
- ✓ Los que estaban más contentos eran los equipos de Comunicación.
- ✓ Interés en futuras ediciones.
- ✓ Para las próximas:
  - Interacción entre grupos durante el ejercicio.
  - Compartir *feedback* entre grupos al final.
  - Traer a más participantes de cada universidad.

Antes y después





Antes de empezar, buscaban aprender.

Al acabar, se llevaban conocimiento e ideas.

Consorci de Serveis Universitaris de Catalunya

¡Gracias por vuestra atención!

¿Preguntas?

mariaisabel.gandia@csuc.cat