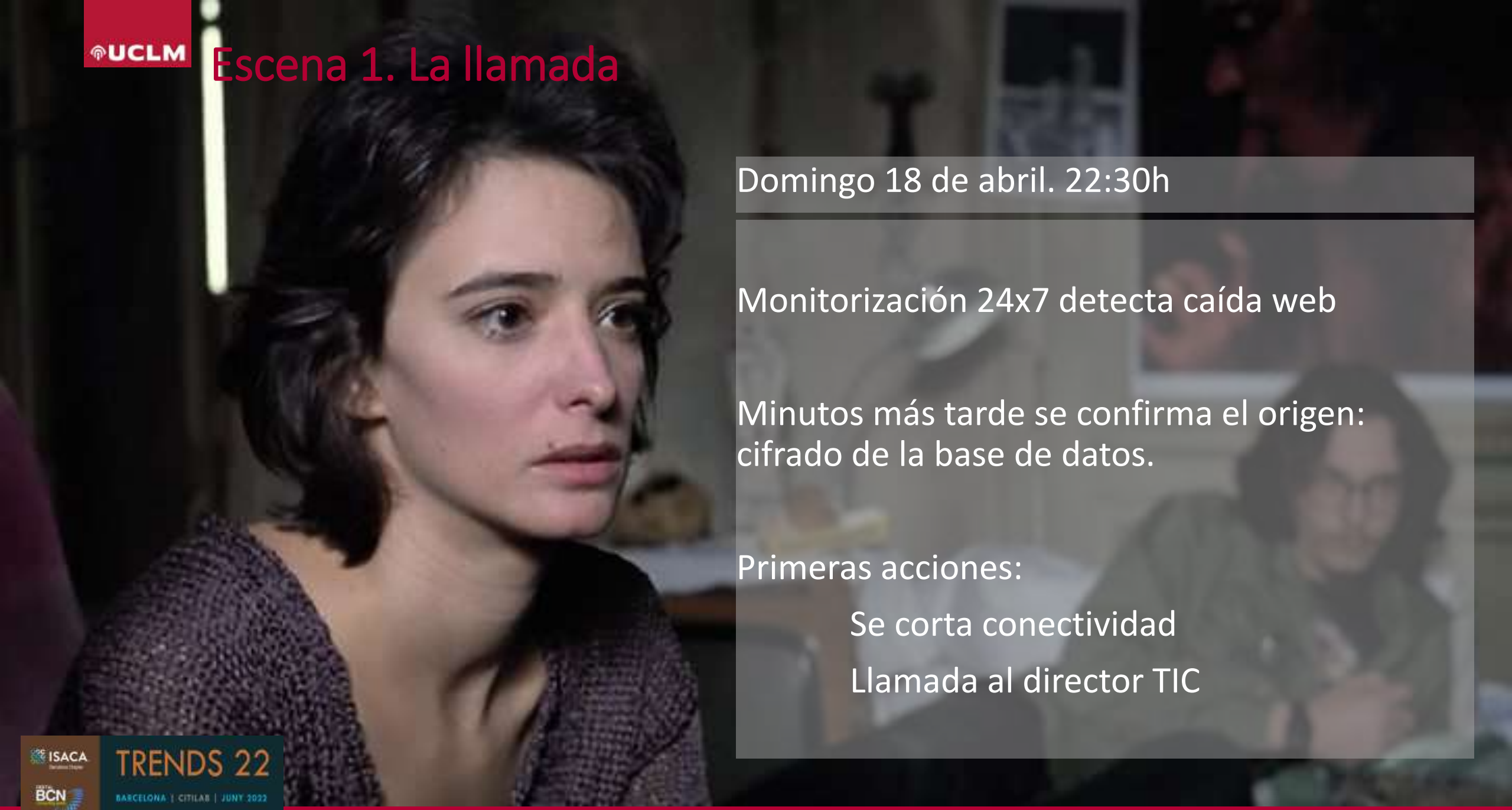
HOLA, ME LLAMO ANDRÉS. ME VAN A CIBERATACAR

Andrés Prado. Director TIC. Universidad de Castilla-La Mancha

Escena 1. La llamada



Domingo 18 de abril. 22:30h

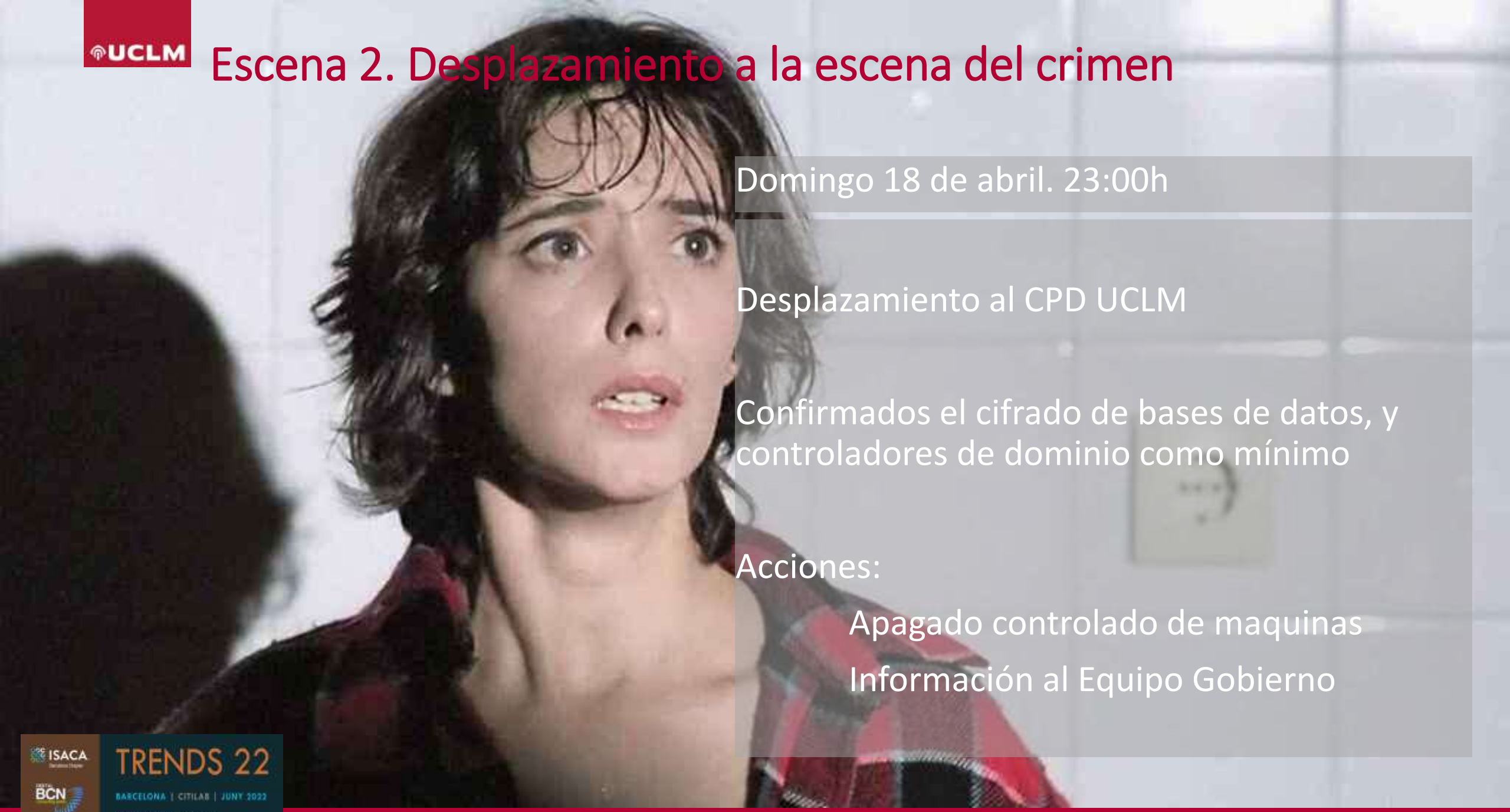
Monitorización 24x7 detecta caída web

Minutos más tarde se confirma el origen: cifrado de la base de datos.

Primeras acciones:

- Se corta conectividad
- Llamada al director TIC

Escena 2. Desplazamiento a la escena del crimen



Domingo 18 de abril. 23:00h

Desplazamiento al CPD UCLM

Confirmados el cifrado de bases de datos, y controladores de dominio como mínimo

Acciones:

- Apagado controlado de maquinas
- Información al Equipo Gobierno

Escena 3. Asumir la situación

Lunes 19 de abril. 02:00h

Apagado completo de equipos

Se asume la situación y no se considera asumible con medios propios

Acciones:

- Identificación de alternativas
- Comunicación

Escena 3. Asumir la situación

UCLMtic
@UCLMtic

Incidencia detectada en los servicios digitales de @uclm_es
Se está trabajando en su resolución.

2:09 a. m. · 19 abr. 2021 · Twitter for iPhone

Ver actividad del Tweet

50 Retweets **16** Tweets citados **69** Me gusta

https://twitter.com/UCLMtic/status/1383935635438768131?s=20

Escena 4. Necesitamos refuerzos

Lunes 19 de abril.

08:00h

Primera llamada a Telefónica Tech

09:15h

Reunión de diagnóstico Telefónica

12:00

Contrato procedimiento emergencia

Acciones:

Plan de acción coordinado

UCLMtic – Telefónica Tech

Información a CCN-CERT

Escena 5. Equipo de Respuesta

Lunes 19 de abril. 13:00h

Primera reunión equipo respuesta

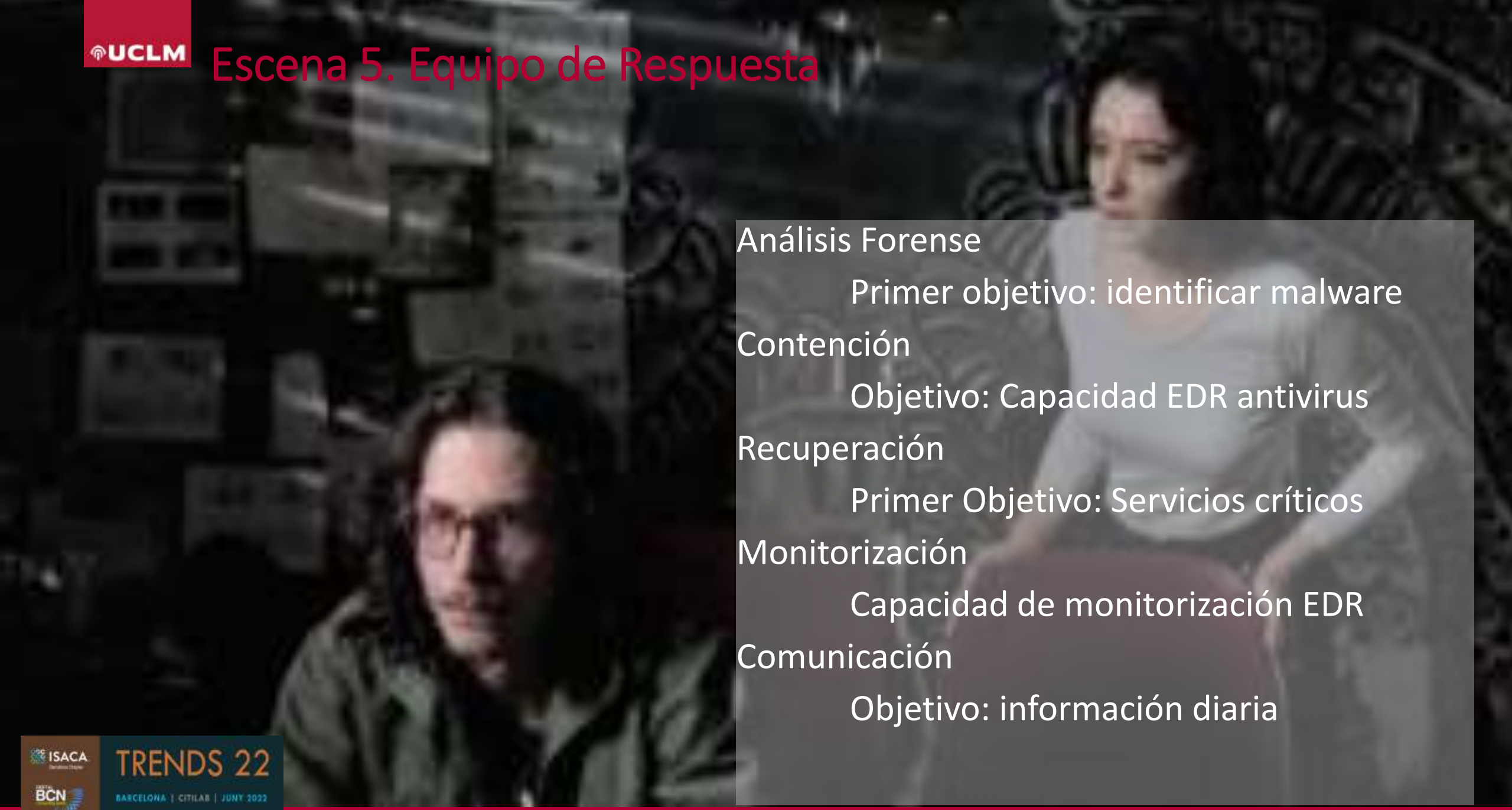
Comunicación Institucional

Acciones:

Plan de Recuperación

Plan de Comunicación

Escena 5. Equipo de Respuesta



Análisis Forense

Primer objetivo: identificar malware

Contención

Objetivo: Capacidad EDR antivirus

Recuperación

Primer Objetivo: Servicios críticos

Monitorización

Capacidad de monitorización EDR

Comunicación

Objetivo: información diaria

Escena 5. Equipo de Respuesta

UCLMtic

- Dirección: Coordinación
- Sistemas: Recuperación Servicios

Responsable Seguridad

- Interlocución CCN-CERT, AEPD

Vicerrectorado Estrategia Digital

- Coordinación Equipo de Gobierno

Gabinete de Comunicación

- Comunicación Coordinada UCLMtic

Telefónica Tech

- Coordinación respuesta técnica

Escena 5. Equipo de Respuesta

Retwitteaste

Universidad de Castilla-La Mancha
@uclm_es

Información ciberataque @uclm_es @UCLMtic pudo amortiguar parte de los efectos del ataque al cortar la conectividad externa en cuanto se detectó la intrusión. Se está evaluando su incidencia, aunque no hay evidencias de que se haya visto comprometida información sensible.

UCLM Rectorado

Es una incidencia similar a la que ha afectado a otras universidades y entidades públicas

La Universidad de Castilla-La Mancha trabaja en la recuperación de los servicios digitales tras sufrir un ciberataque

La Universidad de Castilla-La Mancha (UCLM) está trabajando en la recuperación de sus servicios digitales afectados por el ciberataque que sufrió la institución a las diez de la noche del domingo. La Universidad cortó inmediatamente la conectividad interna para amortiguar el alcance de la intrusión, del tipo *ransomware*.

Los profesionales del Área de Tecnología y Comunicaciones de la Universidad de Castilla-La Mancha (UCLM) están trabajando ininterrumpidamente para recuperar los servicios digitales afectados por un ciberataque producido en la noche de ayer, domingo. Se trata de un ataque de tipo *ransomware* como el que está afectando en los últimos meses a otras universidades españolas y extranjeras, y a otras instituciones públicas y privadas.

La UCLM ha denunciado el ataque al Centro Criptológico Nacional *Computer Emergency Response Team* (CNN-CERT), el organismo encargado de velar por la ciberseguridad de la administración y los organismos públicos y las empresas estratégicas del país.

El Área TIC está evaluando la incidencia del ataque, aunque no hay evidencias de que información sensible se haya visto comprometida. La Universidad pudo amortiguar en parte los efectos del ataque al cortar la conectividad externa en cuanto se detectó la intrusión.

Gabinete Comunicación UCLM. Ciudad Real, 19 de abril de 2021

Universidad de Castilla-La Mancha

1:14 p. m. · 19 abr. 2021 · Twitter Web App

https://twitter.com/uclm_es/status/1384103117550022656?s=20

ISACA BCN TRENDS 22 BARCELONA | CITILAB | JUNY 2022 HTTPS://WWW.TRENDS.CAT

Escena 6. Identificación y Balance de Daños

Lunes 19 de abril.

- Variante conocida *ransomware* RYUK
- Cifrado de controladores de dominio
- Cifrado de bases de datos
- Cifrado de roles de telefonía
- Cifrado de maquina de *backup*
- Directorio Activo disponible
- Elementos no IaaS Azure disponibles

Acciones

- Inicio del Plan de recuperación
- Solución EDR -> Microsoft

Escena 6. Identificación y Balance de Daños

- Decisiones logísticas
  - Sesiones de coordinación Telefónica
    - Mínimo 2 sesiones diarias
    - No presenciales
  - Equipo de respuesta UCLMtic
    - Aislamiento
    - Centrados en recuperación
    - Interlocución limitada
      - Telefónica
      - Dirección UCLMtic
  - Descanso diario. No RedBull

Escena 6. Identificación y Balance de Daños

Decisiones técnicas

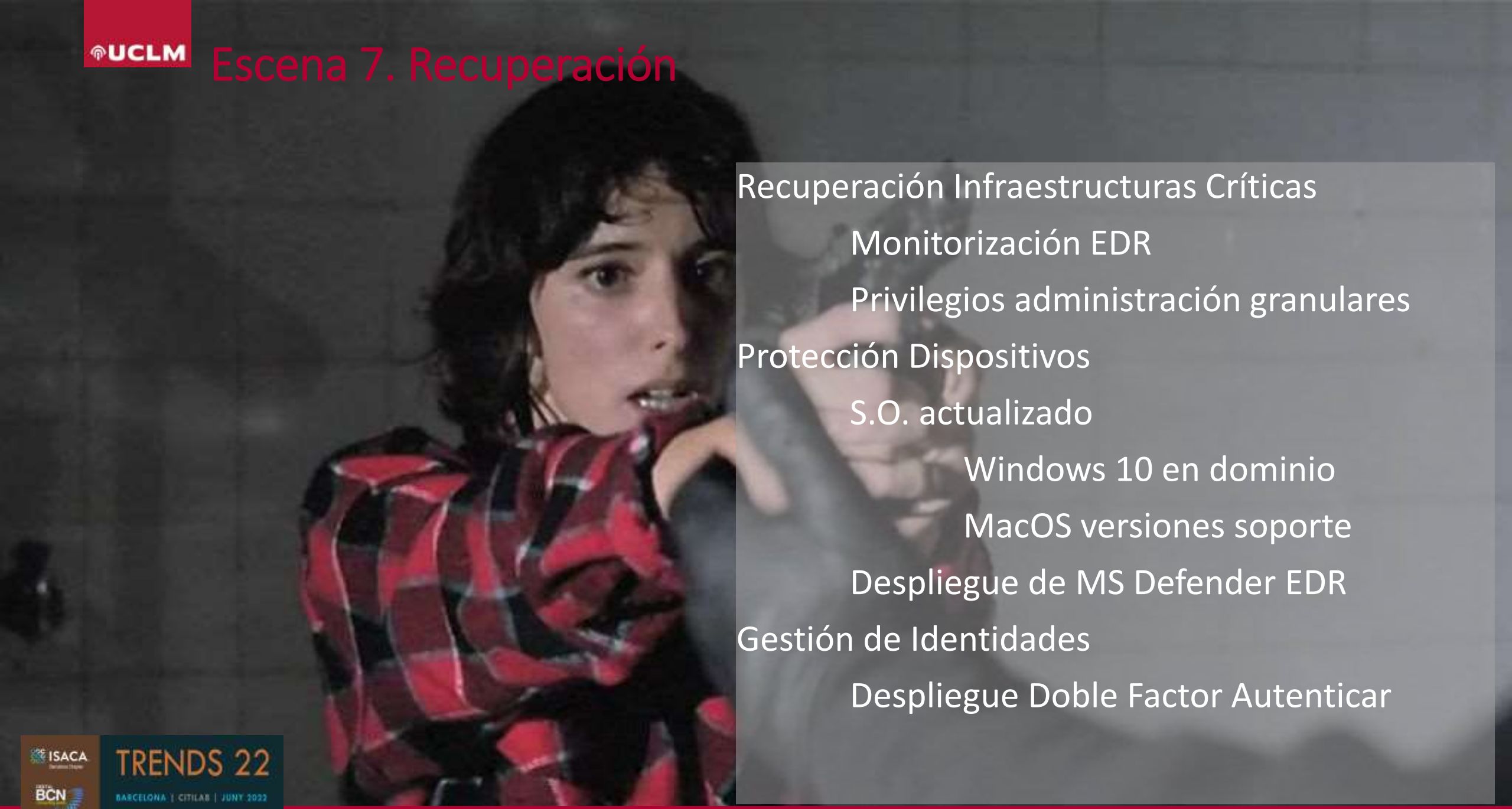
- Recuperación con mejora seguridad
- Incorporación de proyectos en cartera
- Despliegue de antivirus EDR
- Despliegue de MFA
- Limitación conectividad interna
- Limitación S.O. Windows 10 dominio
- Conectividad externa controlada

Escena 6. Identificación y Balance de Daños

Decisiones Comunicación

- Información clara y completa
- Comunicado diario
- Gabinete Comunicación – Dir UCLMtic
- Validación por Equipo de Gobierno
- Uso de medios externos: RRSS

Escena 7. Recuperación

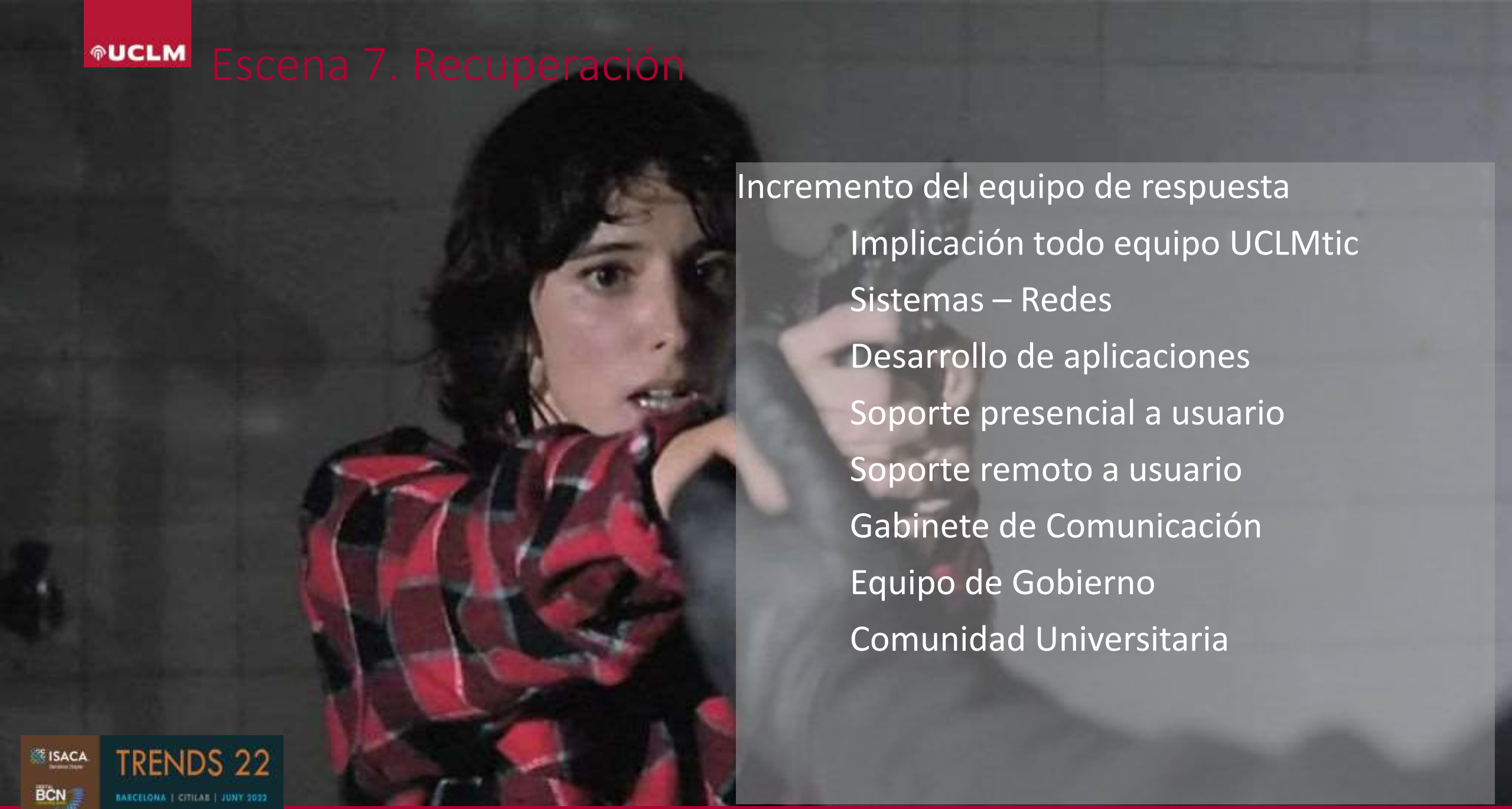


- Recuperación Infraestructuras Críticas
  - Monitorización EDR
  - Privilegios administración granulares
- Protección Dispositivos
  - S.O. actualizado
    - Windows 10 en dominio
    - MacOS versiones soporte
  - Despliegue de MS Defender EDR
- Gestión de Identidades
  - Despliegue Doble Factor Autenticar

Escena 7. Recuperación

- Recuperación de Servicios
  - Factores Impacto - Esfuerzo
  - Despliegue vinculado a seguridad
- Priorización
  - Servicios Infraestructura Dominio
  - Sistema autenticación SSO
  - Campus Virtual
  - Aplicaciones internas *cloud* nativo
  - ERP Módulos comerciales
  - Web institucional
  - Aplicaciones internas adaptadas

Escena 7. Recuperación



Incremento del equipo de respuesta

- Implicación todo equipo UCLMtic
- Sistemas – Redes
- Desarrollo de aplicaciones
- Soporte presencial a usuario
- Soporte remoto a usuario
- Gabinete de Comunicación
- Equipo de Gobierno
- Comunidad Universitaria

Escena 7. Recuperación

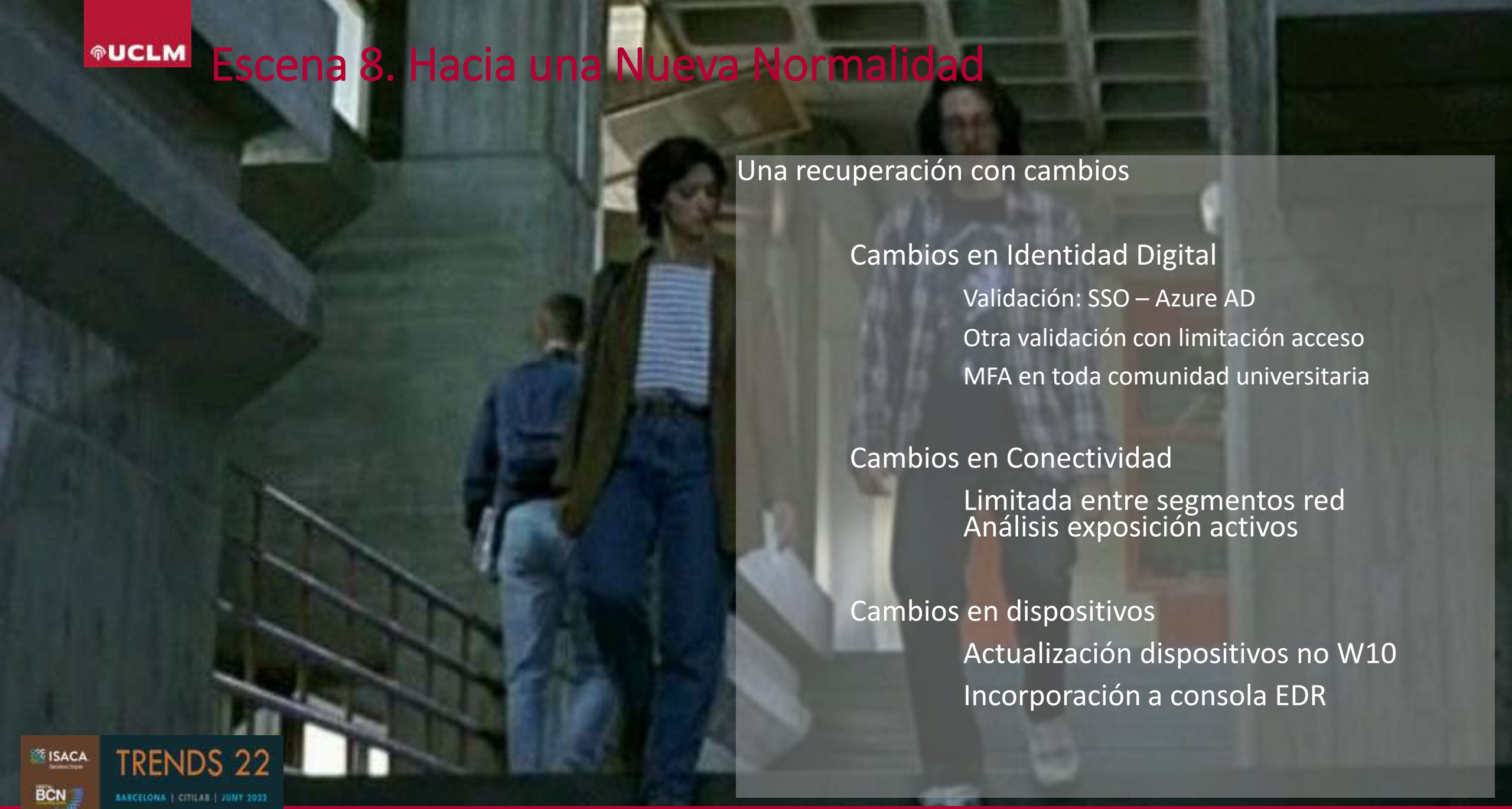
https://www.linkedin.com/posts/pradoandres_el-rector-reconoce-el-trabajo-de-los-profesionales-activity-6790716775865569280-0EBq

Escena 8. Hacia una Nueva Normalidad

Recuperación Progresiva de servicios

- Miércoles 21. Conectividad externa
- Jueves 22. Single Sign-On
- Jueves 22. Campus Virtual 100%
- Jueves 22. Office365. Correo 100%
- Viernes 23. Apps *cloud* nativas
- Lunes 26. ERP módulos comerciales
- Martes 27. Web Institucional
- Siguientes semanas
  - Aplicaciones internas

Escena 8. Hacia una Nueva Normalidad



Una recuperación con cambios

Cambios en Identidad Digital

- Validación: SSO – Azure AD
- Otra validación con limitación acceso
- MFA en toda comunidad universitaria

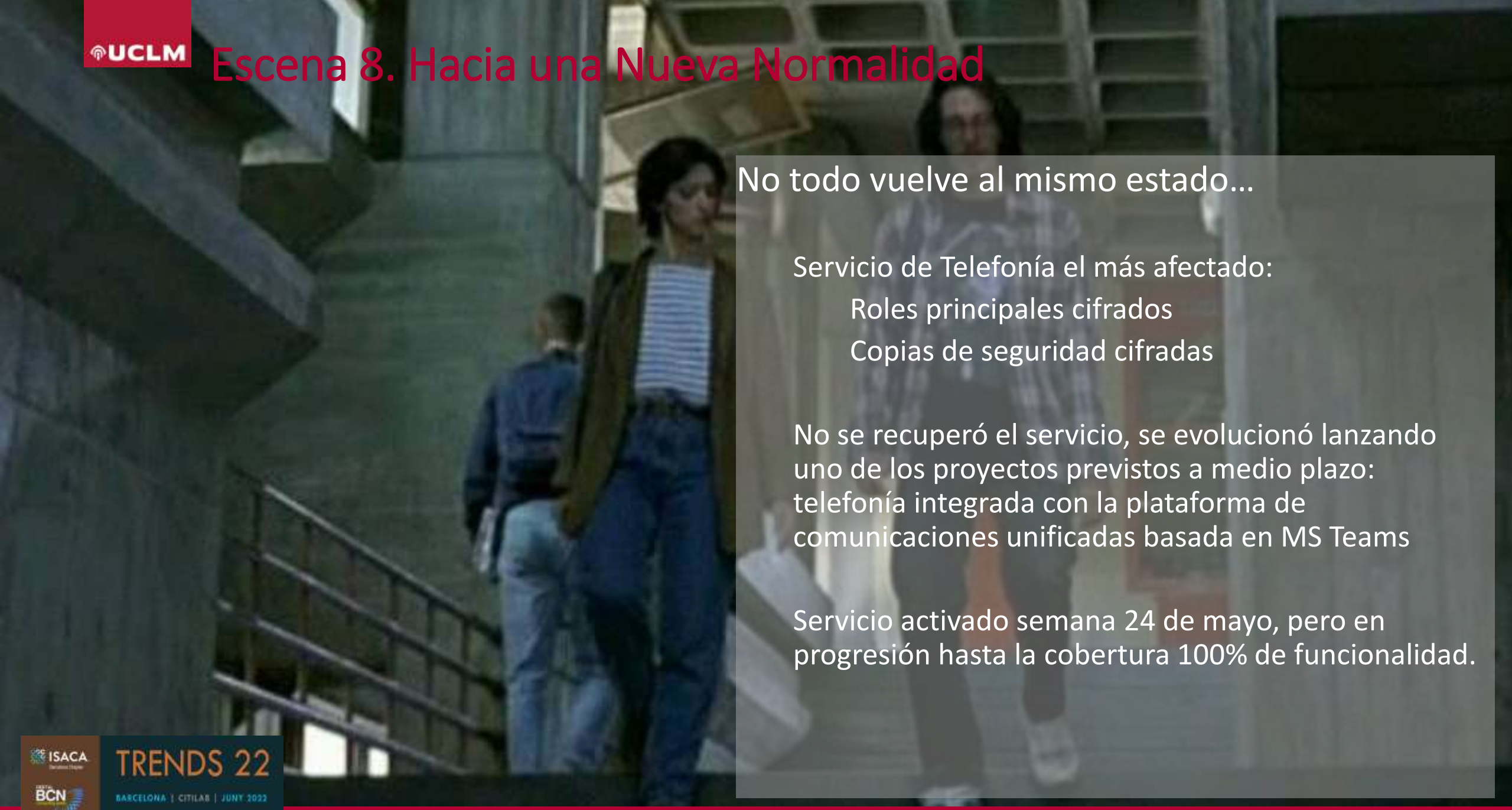
Cambios en Conectividad

- Limitada entre segmentos red
- Análisis exposición activos

Cambios en dispositivos

- Actualización dispositivos no W10
- Incorporación a consola EDR

Escena 8. Hacia una Nueva Normalidad



No todo vuelve al mismo estado…

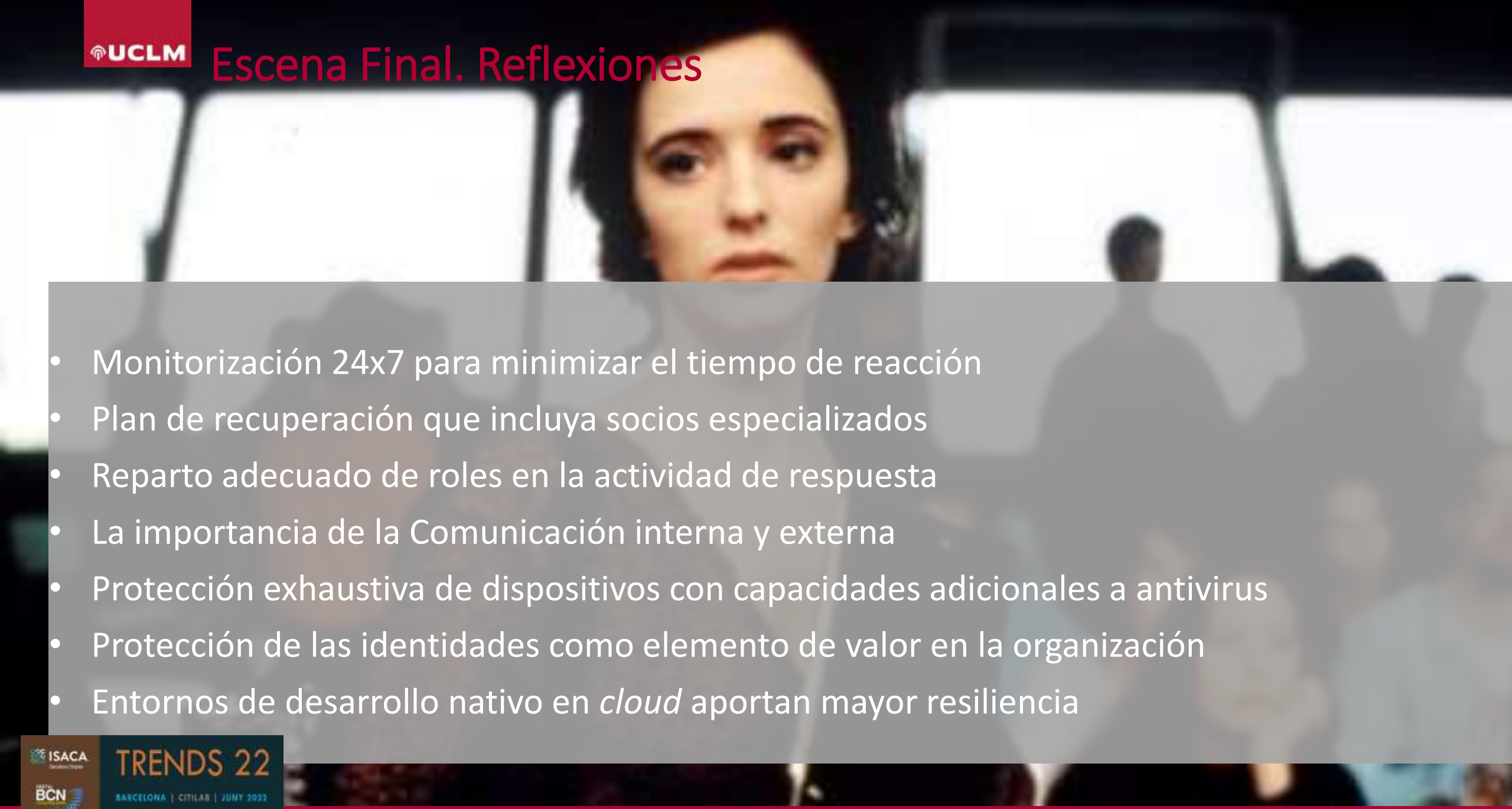
Servicio de Telefonía el más afectado:

- Roles principales cifrados
- Copias de seguridad cifradas

No se recuperó el servicio, se evolucionó lanzando uno de los proyectos previstos a medio plazo: telefonía integrada con la plataforma de comunicaciones unificadas basada en MS Teams

Servicio activado semana 24 de mayo, pero en progresión hasta la cobertura 100% de funcionalidad.

Escena Final. Reflexiones



- Monitorización 24x7 para minimizar el tiempo de reacción
- Plan de recuperación que incluya socios especializados
- Reparto adecuado de roles en la actividad de respuesta
- La importancia de la Comunicación interna y externa
- Protección exhaustiva de dispositivos con capacidades adicionales a antivirus
- Protección de las identidades como elemento de valor en la organización
- Entornos de desarrollo nativo en *cloud* aportan mayor resiliencia

La crítica

*"La perspectiva de la ciberseguridad desde la **prevención** es necesaria pero **no suficiente**.*

*La **Amenaza** a la que nos enfrentamos dispone de dimensiones y **capacidades** en ataque muy superiores a los recursos que las universidades podemos destinar a protección.*

***Asumir** el ataque para minimizar impacto y mejorar la recuperación así como impulsar una **reflexión seria y coordinada** que favorezca una estrategia compartida son vías a recorrer necesariamente."*

Andrés Prado, 14 de octubre de 2021

Créditos

- Comunicación Institucional
  - https://www.uclm.es/noticias/noticias2021/abril/ciudad-real/ciberataque_1
  - https://www.uclm.es/noticias/noticias2021/abril/ciudad-real/ciberataque_2
  - https://www.uclm.es/noticias/noticias2021/abril/ciudad-real/ciberataque_3
  - https://www.uclm.es/noticias/noticias2021/abril/ciudad-real/ciberataque_recuperacion_web
  - https://www.uclm.es/noticias/noticias2021/abril/ciudad-real/ciberataque_secretariavirtual
  - https://www.uclm.es/es/Noticias/Noticias2021/Mayo/Ciudad-Real/Ciberataque_030521

- Guion:

  "Hola, me llamo Andrés. Me van a ciberatacar" • Publicado en revista bit (coit.es)

  https://bit.coit.es/hola-me-llamo-andres-me-van-a-ciberatacar/

Todas las imágenes: Alejandro Amenábar "Tesis". United International Pictures, 1995.