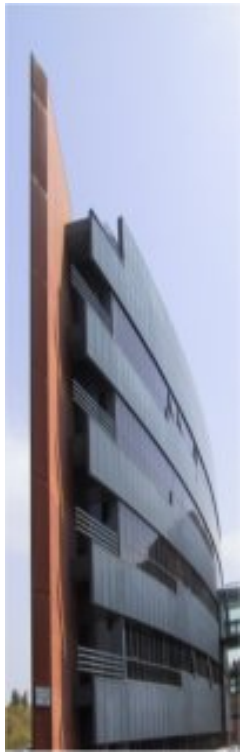
REJA

Su equipo está en cuarentena

GT2010 Córdoba

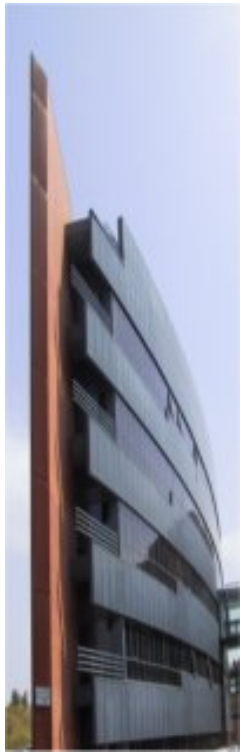
Víctor Barahona victor.barahona@uam.es

Carlos Ramírez carlos.ramirez@uam.es



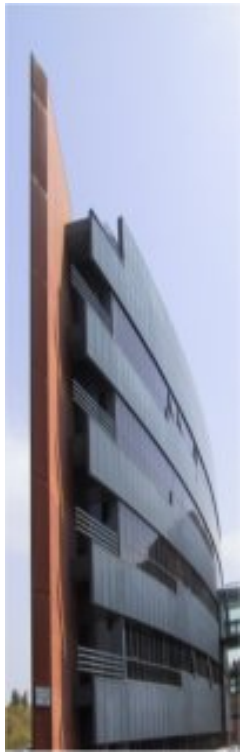
Agenda

- Gestión actual de incidentes
- Motivaciones y Objetivos
- Funcionamiento
- Tras las rejas
- Administración
- Conclusiones



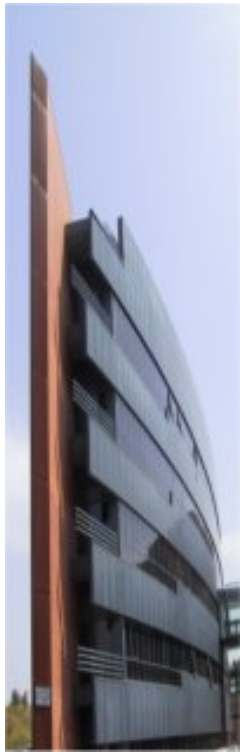
Agenda

- **Gestión actual de incidentes**
- Motivaciones y Objetivos
- Funcionamiento
- Tras las rejas
- Administración
- Conclusiones



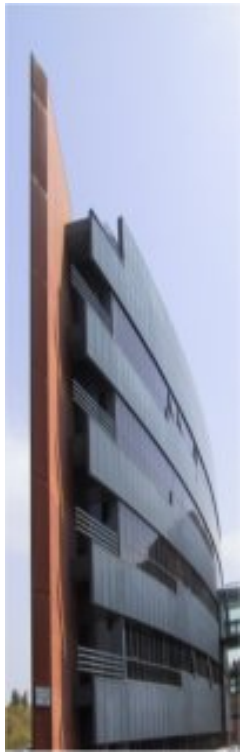
Gestión actual de incidentes

- Creación manual de la Incidencia
- Búsqueda manual del puerto
- Desconexión manual del equipo
- Documentación manual en lista negra
- Búsqueda manual del usuario del equipo
- Contactar con el usuario
- Resolución del problema



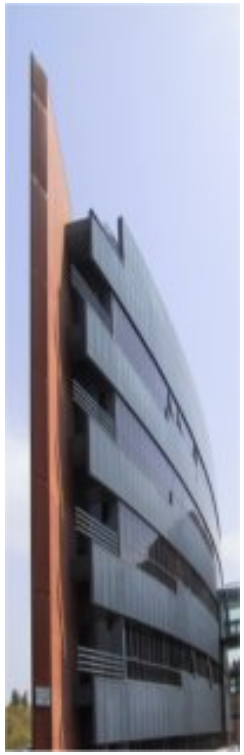
Gestión actual de incidentes

- Creación manual de la Incidencia
- Búsqueda manual del puerto
- Desconexión manual del equipo
- Documentación manual en lista negra
- Búsqueda manual del usuario del equipo
- Contactar con el usuario
- Resolución del problema



Gestión actual de incidentes

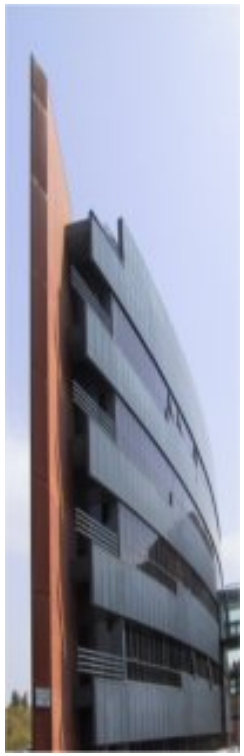
- Coordinación entre operador de red y helpdesk
- Reconfiguración manual del puerto
- Documentación manual en lista negra
- Cierre del incidente de seguridad



Gestión actual de incidentes

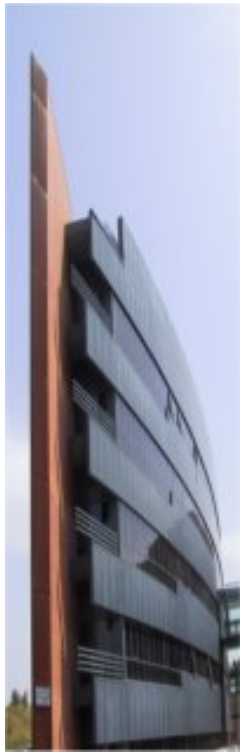
- Coordinación entre operador de red y helpdesk
- Reconfiguración manual del puerto
- Documentación manual en lista negra
- Cierre del incidente de seguridad

¡POR FIN!



Agenda

- Gestión actual de incidentes
- **Motivaciones y Objetivos**
- Funcionamiento
- Tras las rejas
- Administración
- Conclusiones



Génesis de REJA

+ Disp. de seguridad + Correlación

↓

+ Capacidad de Detección + Rapidez

↓

+ Incidentes Gestionados

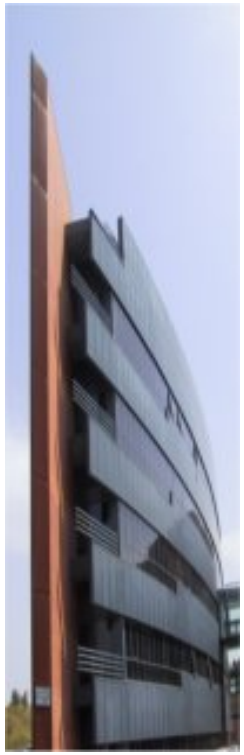
↓

= Personal + Usuarios

↓

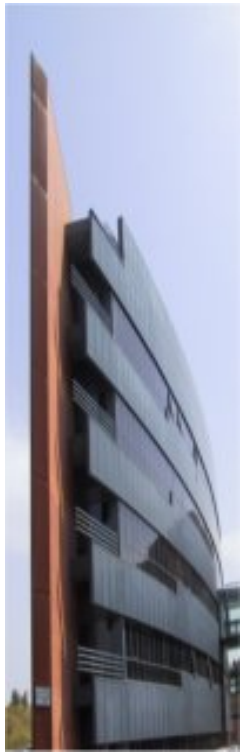
¡Caput!

REd JAula



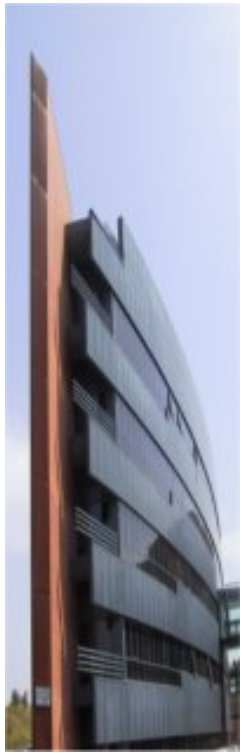
Motivaciones generales

- Mejorar la eficacia en TI
  - Proceso largo
  - Muchas personas implicadas
  - Por tanto lento y farragoso
  - Hay que localizar al usuario
- Mejorar la experiencia del usuario
  - Se queda sin servicio
  - Nadie le avisa
  - Cambia de roseta
  - Genera una incidencia a hardware
  - Indefensión



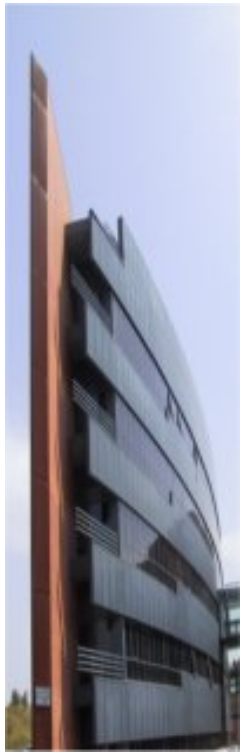
Objetivos I

- Automatizar la detección
- Automatizar el aislamiento
- Informar al usuario inmediatamente
- Identificar al usuario inequívocamente
- Que sea el usuario quien contacte con el CAU
- Dejar que el usuario trabaje durante la resolución del incidente si el tipo de incidente lo permite



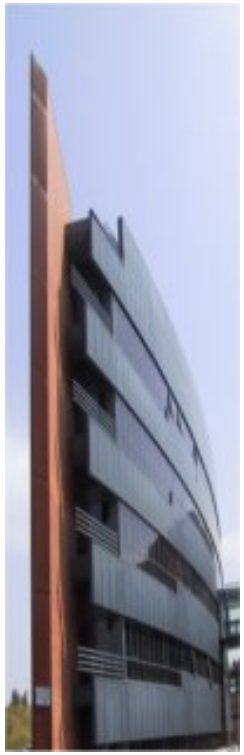
Objetivos II

- Automatizar la gestión de la lista negra
- Integrarse con el gestor de incidencias
- Posibilitar la auto-remediación
- Automatizar la reconexión y delegarla en el CAU
- Soporte para IPs estáticas y dinámicas
- Soporte para asistencia remota desde el CAU



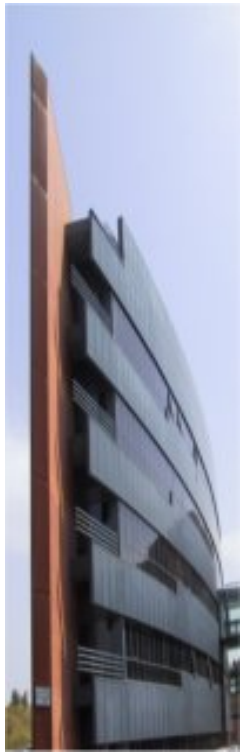
Agenda

- Gestión actual de incidentes
- Motivaciones y Objetivos
- **Funcionamiento**
- Tras las rejas
- Administración
- Conclusiones



Juez: Consola de gestión

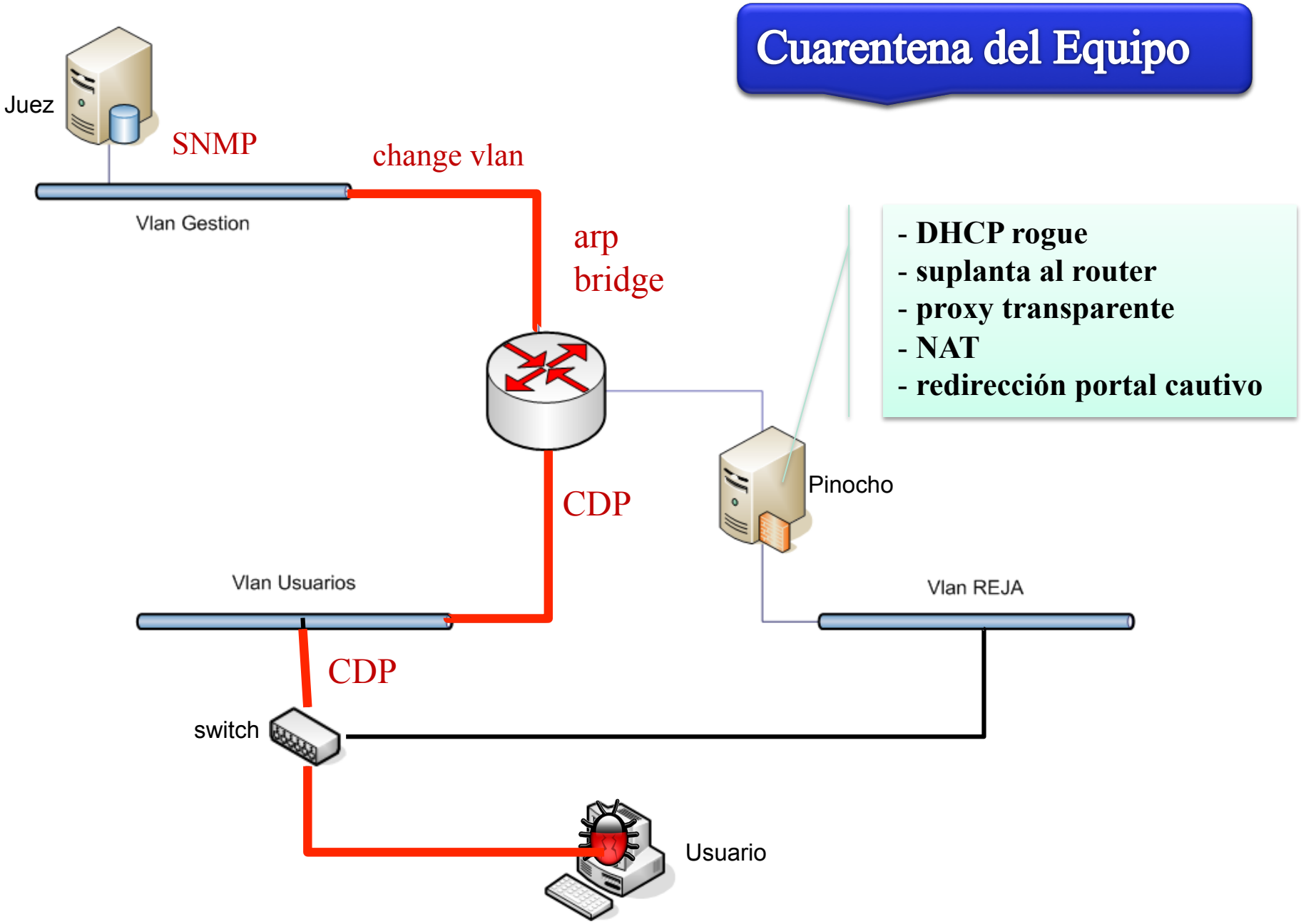
- Linux
- Apache2
- MySQL
- PERL
- Expect
- SNMP
- CDP

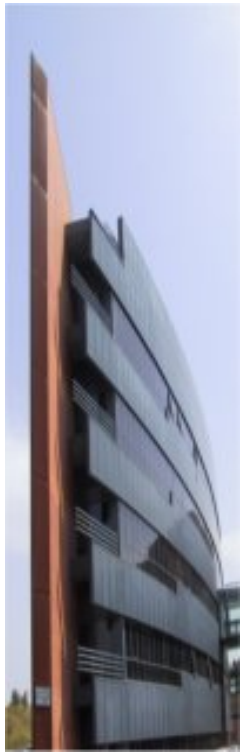


Pinocho: Portal Cautivo

- Linux
- Iptables
- Apache2
- PHP
- PERL
- SQUID
- DHCP

Funcionamiento





Agenda

- Gestión actual de incidentes
- Motivaciones y Objetivos
- Funcionamiento
- **Tras las rejas**
- Administración
- Conclusiones

Este equipo está en cuarentena

¿Qué siginifica que mi PC está en cuarentena? su PC ha sido aislado de la red por razones de seguridad. Siga las instruciones que le iran apareciendo y podra acceder a una serie de servicios mientras se soluciona el incidente.

¿Por qué ha entrado mi PC en cuarentena? Su equipo está enviando correos electrónicos masivos, es muy posible que un virus o un programa malicioso que tenga instalado sin su conocimento sea el causante del problema.

¿Puedo seguir trabajando mientras estoy en cuarentena? en este momento su PC esta aislado de la red, pero cuando acabe el proceso tendrá acceso a los siguientes servicios:

- Acceso de su cliente de correo para la consulta.
- Navegación por internet.

¿Por qué debo facilitar mi dirección de correo? Al introducir su dirección de correo sabremos que es usted el usuario del PC y un tecnico podrá contactar con usted lo antes posible para resolver la incidencia. Si tiene algúna duda puede llamar al Centro de Atención de Usuarios al 4029 indicando el número de ticket que aparece a la derecha.

Por favor, introduzca su dirección de correo y siga la instruciones hasta completar el proceso.

Enviar

Información de referencia:

Incidencia: #341190
Causa: SPAM

Centro de Atención de Usuarios (CAU):

Correo electrónico: cau@uam.es
Teléfono: 4029

PC en cuarentena

Este equipo está en cuarentena

ERROR: Dirección de correo erronea

La dirección de correo **carlos.ramirez@terra.es** no pertenece a la Universidad Autónoma de Madrid.

¿Por qué la dirección de correo debe pertenecer a la UAM? La UAM proporciona una cuenta @uam.es a todos sus usuarios. No se atenderán las peticiones de usuarios que no pertenezcan a la UAM. Si no dispone de una dirección @uam.es, contacte con el Centro de Atencion a Usuarios en el 4029 informando del numero de ticket que aparece a la derecha.

Por favor, introduzca su dirección de correo y siga la instruciones hasta completar el proceso.

Enviar

Información de referencia:

Incidencia: #341190

Causa: SPAM

Centro de Atención de Usuarios (CAU):

Correo electrónico: cau@uam.es

Teléfono: 4029

PC en cuarentena

Este equipo está en cuarentena

Mensaje enviado

Se le ha enviado un correo electrónico a la dirección **carlos.ramirez@uam.es**. Ahora debe seguir los siguientes pasos:

- **Desde este equipo**, conectese al webmail de la UAM https://webmail.uam.es para leer el mensaje que se le ha enviado.
- Haga click en el enlace que contiene.

Este proceso es necesario para verificar que la dirección usada le pertenece.

En caso de error, puede modificar la dirección de correo donde recibir el mensaje:

Enviar

Precaución: Este nuevo mensaje invalidará el enlace enviado anteriormente.

Información de referencia:

Incidencia: #341190

Causa: SPAM

Centro de Atención de Usuarios (CAU):

Correo electrónico: cau@uam.es

Teléfono: 4029

PC en cuarentena

Abrir carpeta Entrada

Entrada | Vaciar (x) | Redactar | Carpetas | Buscar | Traer | Filtros | Opciones | ¿Problemas? | Ayuda | Salir

Estado del espacio asignado: 6,37 MB / 500,00 MB (1,27%)

Entrada: [TI #341190] Equipo en cuarentena (1 de 74)

Marcar como: | Trasladar | Copiar | Este mensaje a | Regresar a Entrada (k)

Eliminar | Responder | Reenviar | Redirigir (g) | Ver conversación | Lista negra | Lista blanca | Origen del mensaje | Guardar como (w) | Imprimir | Cabeceras

Fecha: Thu, 20 May 2010 13:10:21 +0200 [13:10:21 CEST]
De: CAU <cau@uam.es>
Para: carlos.ramirez@uam.es
Responder-A: cau@uam.es
Asunto: [TI #341190] Equipo en cuarentena

¿Mostrar este HTML en una ventana separada?

Estimado/a carlos.ramirez@uam.es,

Ha recibido este mensaje porque su ordenador se encuentra en cuarentena y ha introducido esta dirección como usuario del equipo. Si no fue usted quien facilito su dirección, se trata de un error y puede sin ningún problema ignorar este mensaje.

Una vez finalizado el proceso de cuarentena y durante la resolución de la incidencia podrá acceder a los siguientes servicios:

- Acceso de su cliente de correo para la consulta.
- Navegación por internet.

Para terminar el proceso de cuarentena de su ordenador debe hacer click en el siguiente enlace DESDE EL ORDENADOR EN CUARENTENA:

Finalizar proceso

Terminado este proceso, pongasé en contacto con el Centro de Atención a Usuarios **cau@uam.es** o a través del teléfono **4029** , indicando el número de incidencia que aparece en el asunto de este mensaje. En caso de no hacerlo, un técnico se pondrá en contacto con usted los antes posible.

Atentamente.

Tecnologías de la Información.

Eliminar | Responder | Reenviar | Redirigir (g) | Ver conversación | Lista negra | Lista blanca | Origen del mensaje | Guardar como (w) | Imprimir | Cabeceras

Marcar como: | Trasladar | Copiar | Este mensaje a | Regresar a Entrada (k)

Este equipo está en cuarentena

Por favor, espere **39** segundos y habrá finalizado el proceso.

Por favor, espere un minuto y podrá seguir navegando con normalidad.

Terminado este proceso, pongasé en contacto con el Centro de Atención a Usuarios **cau@uam.es** o a través del teléfono **4029** , indicando el número de incidencia que aparece en la columna de la derecha. En caso de no hacerlo, un técnico se pondrá en contacto con usted los antes posible.

Información de referencia:

Incidencia: #341190

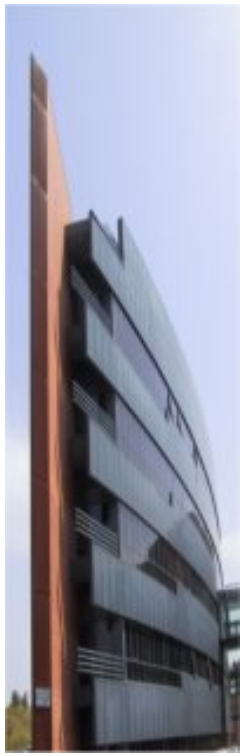
Causa: SPAM

Centro de Atención de Usuarios (CAU):

Correo electrónico: cau@uam.es

Teléfono: 4029

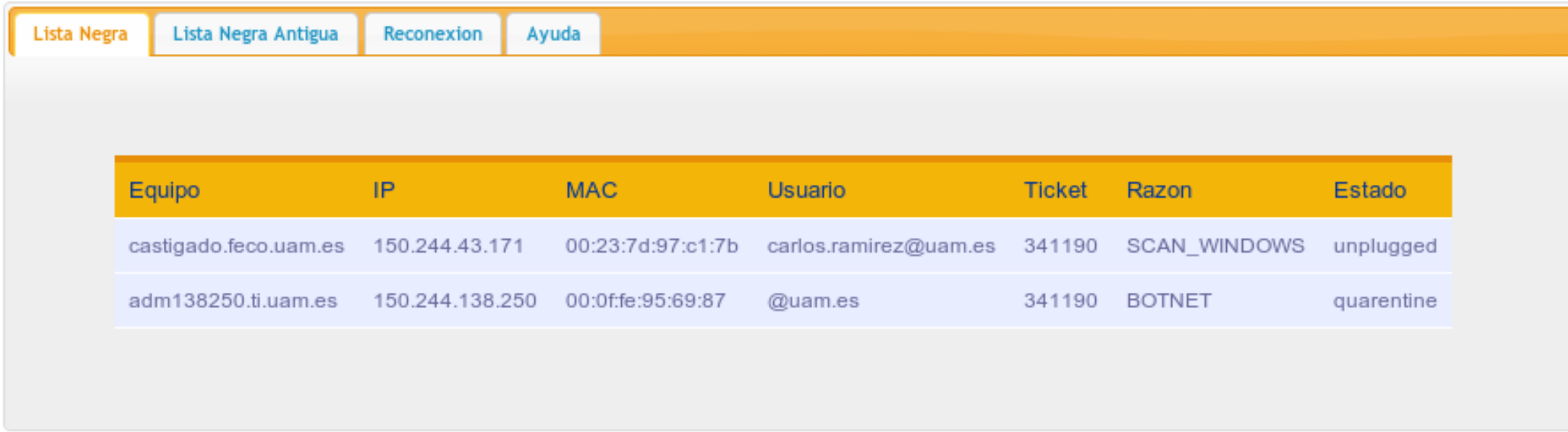
PC en cuarentena



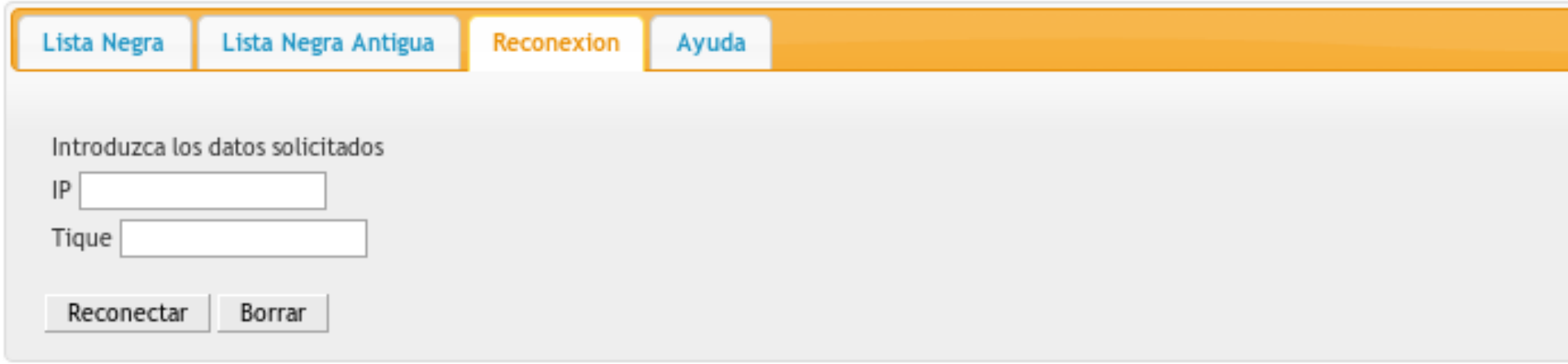
Agenda

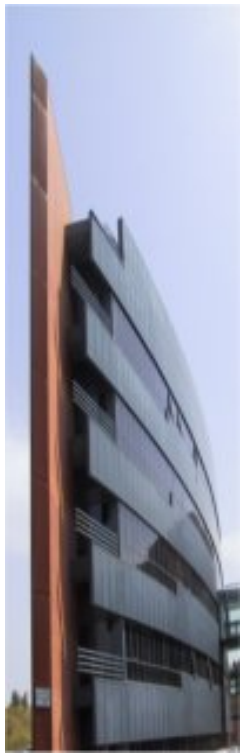
- Gestión actual de incidentes
- Motivaciones y Objetivos
- Funcionamiento
- Tras las rejas
- **Administración**
- Conclusiones

REJA: REd JAula



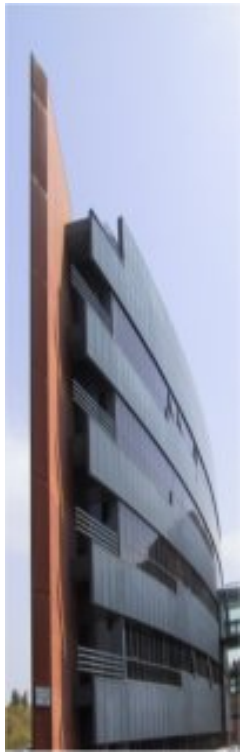
REJA: REd JAula





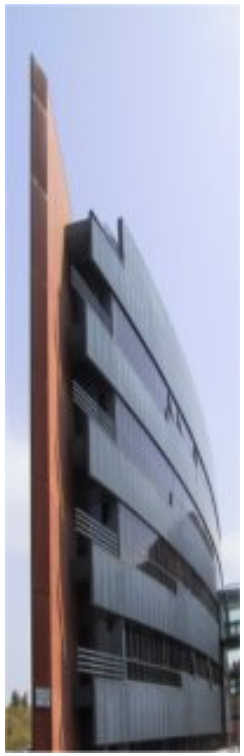
Agenda

- Gestión actual de incidentes
- Motivaciones y Objetivos
- Funcionamiento
- Tras las rejas
- Administración
- **Conclusiones**



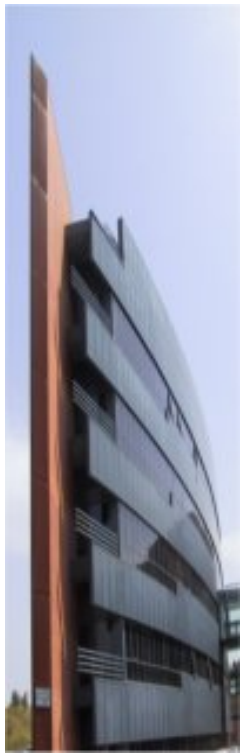
Conclusiones

- Hemos cumplido todos los objetivos
- Perturbación “cero” en la electrónica
- Flexible y extensible
- Usando al 99% código libre
- Piloto exitoso
- El CAU esta deseando su implantación



Futuro

- Integrar histórico para la cuarentena de equipos NO conectados
- Equipos no UAM
- Red inalámbrica
- 802.1x



Agradecimientos

MUCHAS GRACIAS

victor.barahona@uam.es
carlos.ramirez@uam.es