



VNIVERSITAT
DE VALÈNCIA

ACMEBOT: Gestión automatizada de certificados SSL en la UV

Autores: Héctor M. Rulot Segovia y M. Carmen Mifsut Herrera
Ponente: M. Carmen Mifsut Herrera

Jt 2026
Red IRIS



A CORUÑA

22-25 JUNIO Universidade da Coruña



GOBIERNO DE ESPAÑA

MINISTERIO DE CIENCIA, INNOVACIÓN Y TURISMO

COMISIÓN EUROPEA

CONSEJO REGULADOR DE LAS TELECOMUNICACIONES

red.es



Red IRIS



ICTS

INSTITUTO TECNOLÓGICO DE CANTABRIA

UNIVERSIDADE DA CORUÑA



Introducción

Jt 2026
Red IRIS


A CORUÑA
22-25 JUNIO Universidade da Coruña



Origen y necesidad de una solución soberana

- Reducción progresiva de vigencia en los certificados TLS
- Inviabilidad de la gestión manual para cientos de dominios
- Primera solución ACME: certi + daemon + certideploy
- La migración anticipada: detonante para automatización total



Magnitud de la infraestructura gestionada

- **Gestión centralizada de 354 dominios institucionales**
- **Servicio prestado a 26 entes universitarios diferentes**
- **Convivencia de modelos: 176 dominios automatizados y 152 manuales, automatización progresiva**



Centralización y Soberanía Tecnológica

- Cuenta ACME únicamente para el servidor ACMEBOT
- Gestión orientada a Dominios: facilita nuevas migraciones
- Independencia de Clientes



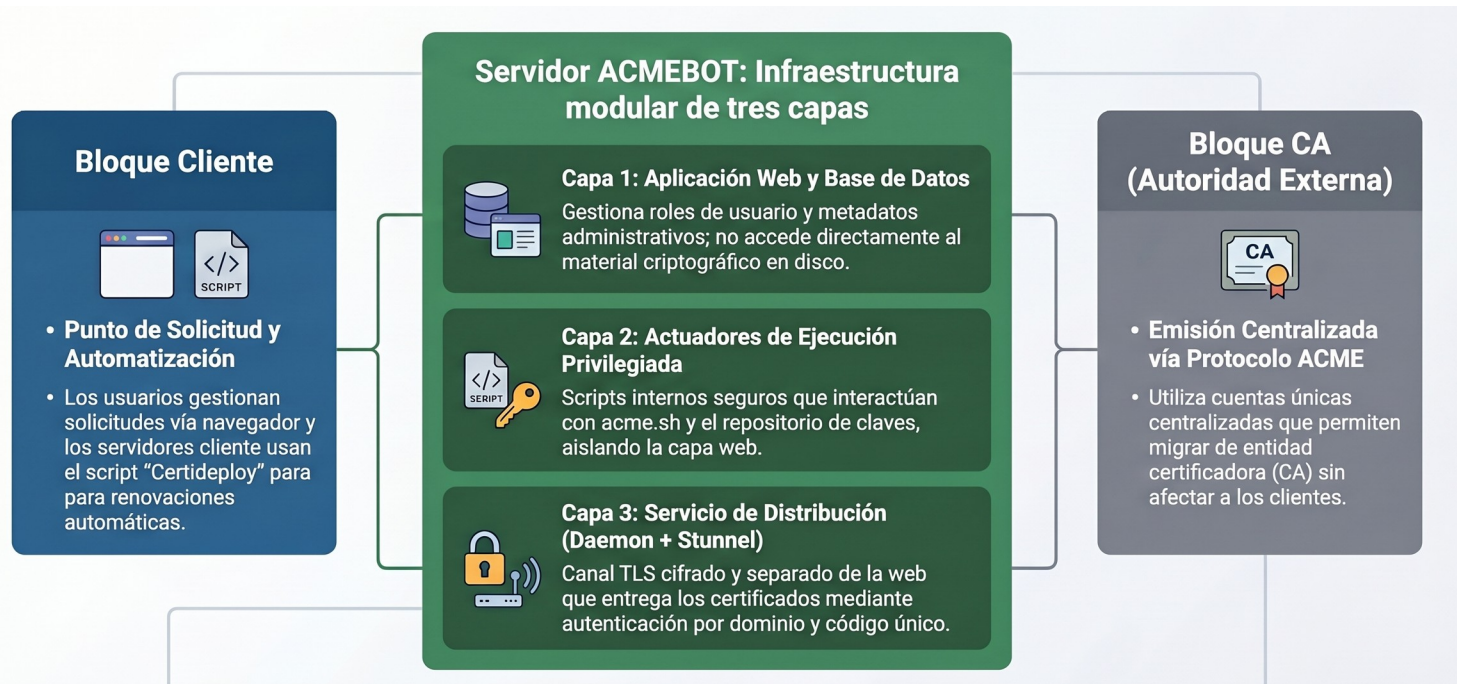
Arquitectura

Jt 2026
Red IRIS


A CORUÑA
22-25 JUNIO Universidade da Coruña



Arquitectura Centralizada



El modelo de despliegue autónomo (certideploy)

- Script modular de ejemplo configurado una sola vez por el administrador del cliente
- Ejecución programada vía cron con lógica de descarga inteligente por fecha
- Independencia de herramientas externas adicionales en el cliente (uso de openssl)



Seguridad por Diseño

Jt 2026
Red IRIS


A CORUÑA
22-25 JUNIO Universidade da Coruña



Seguridad por diseño



Control de Acceso e Identidad



Restricción de Red y Validación DNS

Acceso limitado por firewall perimetral y validación previa obligatoria contra el DNS institucional.



Vinculación de Personal en Activo

La titularidad de los certificados está estrictamente ligada a personal institucional con vinculación contractual vigente.



Doble Factor de Descarga

Autorización obligatoria por Nombre Canónico del host y código de acceso único por dominio.



Blindaje Arquitectónico y Criptográfico



Canal de Distribución Cifrado (Stunnel)

Distribución autenticada de certificados a través de un canal TLS dedicado e independiente de la web.



Arquitectura de "Actuadores Privilegiados"

Separación física que impide que la aplicación web acceda directamente al disco o al repositorio.

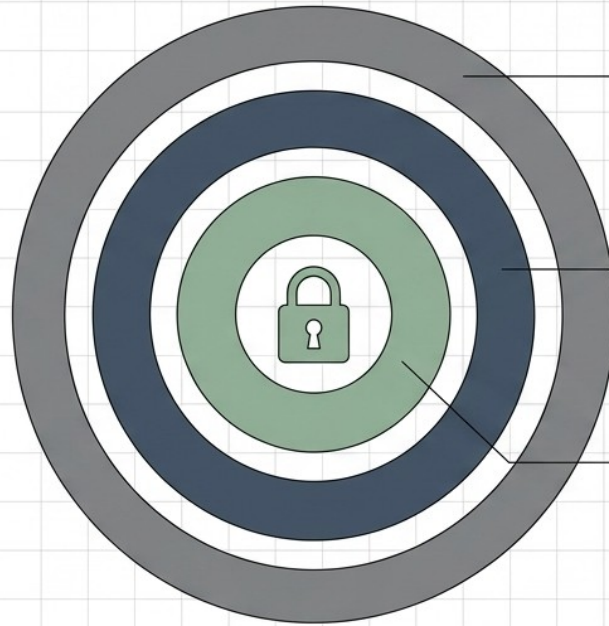


Higiene Criptográfica Automática

Rotación automática de claves privadas en cada ciclo de renovación del certificado.



Capas de protección y perímetros de seguridad



Capa Externa: Red y DNS

Acceso restringido a red interna UV. Validaciones obligatorias contra DNS institucional. Autorización explícita (whitelisting) de IPs por servidor.

Capa Intermedia: Identidad y Gobernanza

Restringido a personal UV activo. Asignación obligatoria de dominios a Entes institucionales para evitar cuentas huérfanas.

Capa Interna: Criptografía y Aislamiento

Códigos de acceso cifrados. Túneles TLS (Stunnel). Actuadores aíslan procesos root. Separación total entre BD (metadatos) y Repositorio (claves).



Garantías en la entrega de material criptográfico

- Lista blanca de servidores autorizados por nombre canónico (evita riesgos por reutilización de IP)
- Doble factor de descarga: Validación de Host + Código de acceso encriptado único por dominio
- Uso de túnel TLS dedicado (stunnel) para el transporte seguro



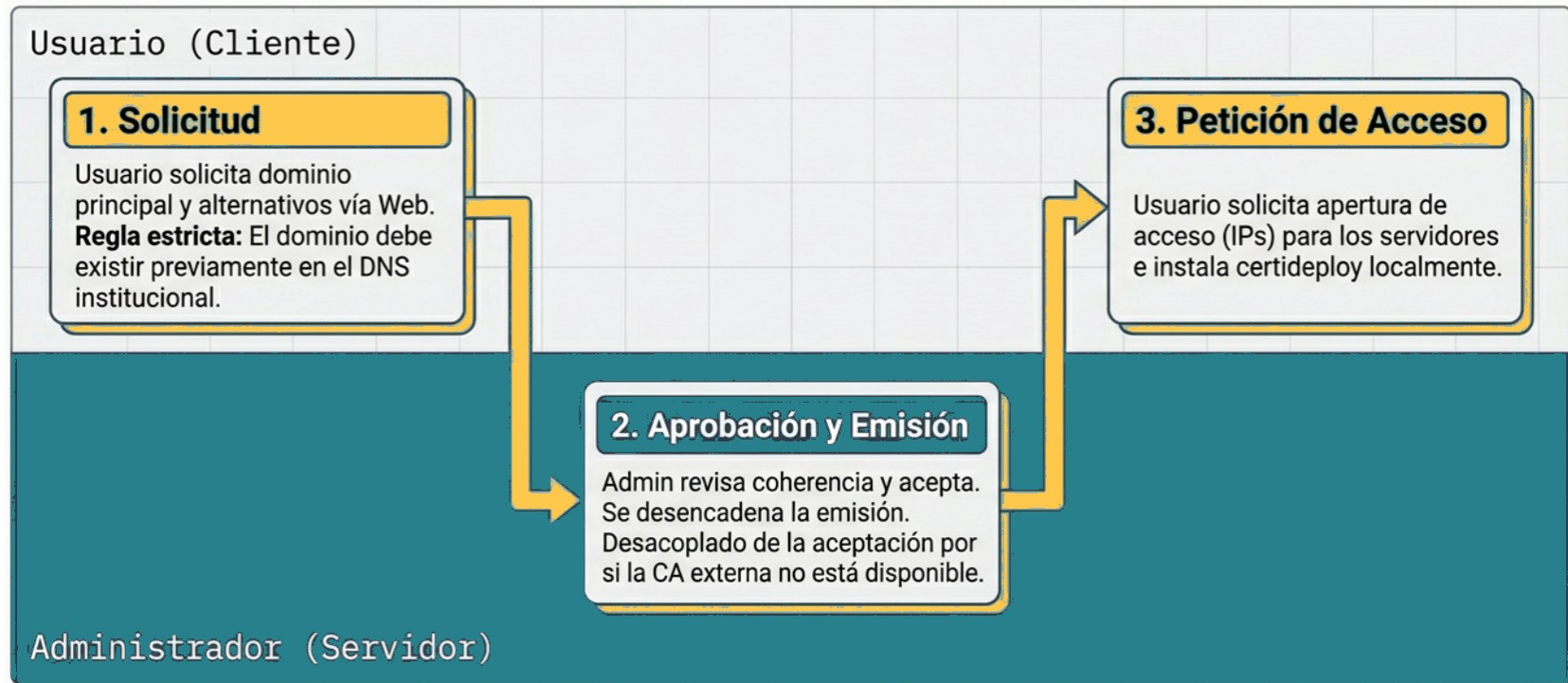
Ciclo Completo

Jt 2026
Red IRIS

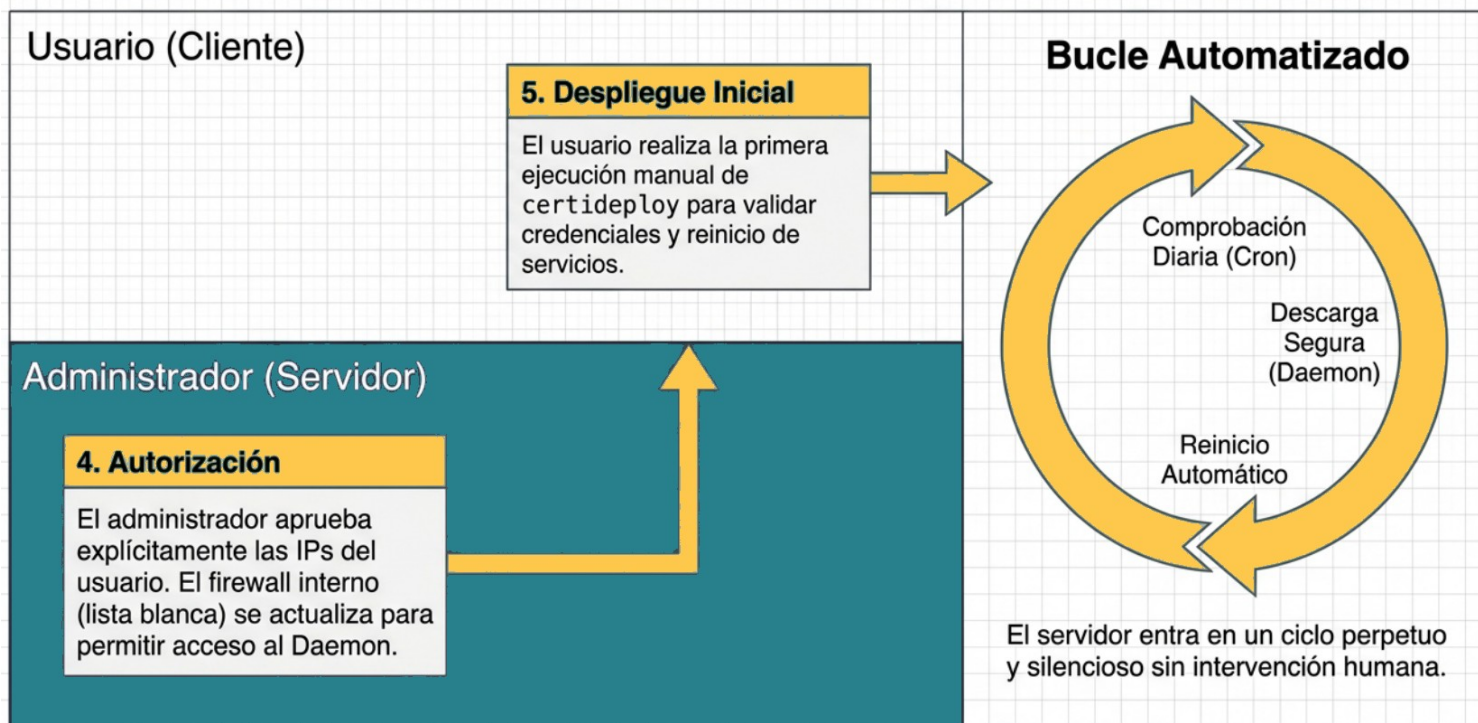

A CORUÑA
22-25 JUNIO Universidade da Coruña



Procedimiento operativo de gestión



Automatización del Ciclo de Vida



Estado Actual y Roadmap

Jt 2026
Red IRIS


A CORUÑA
22-25 JUNIO Universidade da Coruña



Balance de situación y evolución del proyecto

- Eliminación de caducidades no detectadas y auditoría completa de actividad
- Gobierno de toda la infraestructura desde la aplicación
- Evolución activa, próximos pasos
 - Adaptación para clientes Windows (PowerShell)
 - Viabilidad de Proxy ACME local



Aplicación ACMEBOT - Inicio

ACMEBOT certificados UV

Valencià | Castellano

ACMEBOT Gestión de certificados UV [ADMIN] cerrar sesión

GESTIÓN DE CERTIFICADOS UV

El sistema ACMEBOT gestiona la solicitud y renovación de los Certificados UV. La mayoría de lo aquí presentado es solo para usuarios autorizados.

¡Atención!
A partir del **13 de marzo 2026** todos los certificados nuevos tendrán de validez máxima **199 días** (antes eran 365 días). Esto es conforme a los nuevos requisitos para certificados SSL/TLS impuestos por el CAB/Forum. Los certificados ya emitidos no se ven afectados y seguirán siendo válidos hasta su fecha de expiración. Más detalles... ¿Por qué ACMEBOT?

UTILIDADES

Existen diversas utilidades para ayudar a la gestión de certificados.

- Vida y muerte certificados UV

ADMINISTRADORES

Los administradores del ACMEBOT tienen acceso a todas las solicitudes, dominios y certificados, incluyendo muchos comandos específicos de gestión. Y además:

- Acceso directo a las tablas de la BD (solo para iniciados!)
- Entorno del Bot
- Ver Log
- Comprobar ACMEDEAMON
- Actualizar la tabla códigos del acmedaemon
- Ponerse en modo usuario

DOCUMENTACION

- Configuración automática
- Origen de la Imagen

Solicitudes

Dominios

Mis Solicitudes

Mis Dominios

Noticias

Comenariros

ACMEBOT certificados UV

Valencià | Castellano

ACMEBOT Gestión de certificados UV cerrar sesión

GESTIÓN DE CERTIFICADOS UV

El sistema ACMEBOT gestiona la solicitud y renovación de los Certificados UV. La mayoría de lo aquí presentado es solo para usuarios autorizados.

¡Atención!
A partir del **13 de marzo 2026** todos los certificados nuevos tendrán de validez máxima **199 días** (antes eran 365 días). Esto es conforme a los nuevos requisitos para certificados SSL/TLS impuestos por el CAB/Forum. Los certificados ya emitidos no se ven afectados y seguirán siendo válidos hasta su fecha de expiración. Más detalles... ¿Por qué ACMEBOT?

UTILIDADES

Existen diversas utilidades para ayudar a la gestión de certificados.

- Vida y muerte de mis certificados
- (Eres admin) Ponerse en modo admin

DOCUMENTACION

- Configuración automática
- Origen de la Imagen

Mis Solicitudes

Mis Dominios

Noticias

Comenariros



Aplicación ACMEBOT - Admin

ACMEBOT certificados UV

Valencià | Castellano

Listado de Solicitudes [ADMIN] cerrar sesión

+ Nueva Solicitud Todas Mostrar

| ID | Estado | Tipo | Fecha | Ente | Manual CSR | Fecha Exp. |
|-----|--------|-----------|---------------------|------|------------|------------|
| 323 | ND | resuelta | 16-06-2026 11:05:27 | | S | 2026-10-27 |
| 322 | ND | resuelta | 16-06-2026 11:04:53 | | S | 2026-10-24 |
| 321 | ND | resuelta | 16-06-2026 11:04:15 | | S | 2026-11-19 |
| 320 | ND | resuelta | 16-06-2026 11:03:10 | | S | 2026-10-21 |
| 319 | ND | resuelta | 15-06-2026 11:28:08 | | S | 2027-01-26 |
| 317 | ED | resuelta | 12-06-2026 09:49:55 | | S | 2026-10-03 |
| 316 | ND | resuelta | 11-06-2026 18:05:33 | | S | 2026-10-27 |
| 313 | GE | resuelta | 10-06-2026 13:17:37 | | S | 2026-10-27 |
| 312 | ED | resuelta | 10-06-2026 09:49:56 | | S | 2026-10-27 |
| 311 | MN | resuelta | 10-06-2026 09:06:40 | | S | 2026-10-27 |
| 310 | ED | resuelta | 08-06-2026 12:17:31 | | S | 2027-02-02 |
| 309 | ND | resuelta | 08-06-2026 11:18:23 | | S | 2026-10-27 |
| 308 | ND | resuelta | 08-06-2026 08:38:06 | | S | 2026-10-21 |
| 307 | ED | resuelta | 05-06-2026 14:05:37 | | S | 2026-10-24 |
| 306 | GE | resuelta | 05-06-2026 13:28:26 | | S | 2026-10-23 |
| 305 | ND | rechazada | 05-06-2026 12:01:23 | | S | 2026-11-20 |
| 303 | ND | resuelta | 04-06-2026 13:19:48 | | S | 2026-10-24 |
| 302 | ND | resuelta | 04-06-2026 11:59:28 | | S | 2027-01-01 |
| 301 | ND | resuelta | 01-06-2026 09:47:53 | | S | 2027-01-01 |
| 299 | GE | resuelta | 28-05-2026 09:54:58 | | S | 2026-10-24 |
| 298 | ND | resuelta | 27-05-2026 14:26:10 | | S | 2026-10-17 |

ACMEBOT certificados UV

Valencià | Castellano

Lista de los dominios [ADMIN] cerrar sesión

ver también alts Filtro Dominio Buscar Todos

| Dominio ↓ | Solicitante | Ente | Manual CSR | Fecha Exp. |
|-----------|-------------------|----------------|------------|------------|
| uv.es | @uv.es | | S | 2026-10-27 |
| uv.es | | | S | 2026-10-24 |
| uv.es | | Serv.Informat. | - | 2026-11-19 |
| uv.es | | Serv.Informat. | - | 2026-10-21 |
| uv.es | | Serv.Informat. | - | 2027-01-26 |
| uv.es | | Adeit | S S | 2026-10-03 |
| uv.es | @fundacions.uv.es | | S | 2026-10-27 |
| uv.es | @uv.es | | S | 2026-10-27 |
| uv.es | | Ilic | - | 2027-02-02 |
| uv.es | | Astron-Astrof. | S | 2026-10-27 |
| uv.es | | Astron-Astrof. | S | 2026-10-15 |
| uv.es | | Serv.Informat. | - | 2026-10-31 |
| uv.es | @uv.es | | S | 2026-10-24 |
| uv.es | | Serv.Informat. | - | 2026-10-21 |
| uv.es | | Eng. Electron. | S | 2026-10-24 |
| uv.es | | Serv.Informat. | - | 2026-10-23 |
| uv.es | | B.Cel I Paras. | S | 2026-11-20 |
| uv.es | @uv.es | | S | 2026-10-24 |
| uv.es | | Fac. Filologia | - | 2027-01-01 |
| uv.es | | Fac. Filologia | - | 2027-01-01 |
| uv.es | @uv.es | | S | 2026-10-24 |
| uv.es | @uv.es | | S | 2026-10-27 |
| uv.es | @uv.es | | S | 2026-10-17 |
| uv.es | | I2sysbio | - | 2026-12-24 |
| uv.es | @uv.es | | - | 2026-11-13 |



Aplicación ACMEBOT - Solicitud

UNIVERSITAT ID VALÈNCIA | ACMEBOT certificados UV | Valencia | Castellano

Solicitud de nuevo Dominio y Certificado [ADMIN] cerrar sesión

Solicitante
HECTOR MIGUEL RULOT SEGOVIA (hmr)

Dominios del certificado
Dominio:
Dominios adicionales:

Instalación del certificado: **Manual**
CSR (Opcional. Si se proporciona la CSR no es posible la renovación automática):

¿Certificado IGTF? (sólo si es para Grid)

Información del dominio
Aplicación o servicio que se alojará en el dominio:
Ente universitario asociado:
Responsable del dominio (Director, jefe grupo...)(nombre de usuario UV):
E-mail de contacto para notificaciones:
Información adicional (opcional):

[Solicitar Nuevo Certificado](#)

Solicitudes
Dominios
Mis Solicitudes
Mis Dominios
Noticias
Comentarios

UNIVERSITAT ID VALÈNCIA | ACMEBOT certificados UV | Valencia | Castellano

Ver Solicitud [ADMIN] cerrar sesión

Solicitud de certificado [resuelta]

Solicitud: #87 Tipo: ND realizada por: hmr el día: 21-11-2025 23:08:13

Dominio: .uv.es
Dominios alternativos: .uv.es
Instalación del certificado: Manual
Aporta CSR: Sí ver ver decodificada
IGTF: No

Aplicación o servicio que se alojará en el dominio: **La mas importante**
Ente universitario asociado: **Servei d'informatica -**
Responsable del dominio (usuario UV):
E-mail de contacto para notificaciones: @uv.es
Información adicional: **Nada que destacar**

Admin: Solicitud resuelta
Mensaje:
Notas:

[Borrar solicitud](#)

[Volver](#) [Ver .uv.es](#)

Solicitudes
Dominios
Mis Solicitudes
Mis Dominios
Noticias
Comentarios



Aplicación ACMEBOT - Dominio

The screenshot shows the ACMEBOT interface for domain #412 - acmeproxy.uv.es. The header includes the logo of the Universitat de València and the text 'ACMEBOT certificados UV' with language options for 'Valencià' and 'Castellano'. The main content area displays the domain name and a list of AITDoms. The 'Lugar' is 'S033 - Servei D'informatica' and the 'App' is 'App ACME Proxy'. The 'Propiedad de' is 'Resp.' and the 'desde' date is '26-01-2026 21:13:53'. The 'Contactos' are listed as '@uv.es'. The 'Info' section shows 'CSR: f', 'MANUAL: f', 'Tipo Clave: ecc', and 'IGTF: f'. Below this, there are buttons for 'Modificar', 'Probar Dominio:443', 'Ver código', 'Cambiar código', and 'Actualizar código'. A 'SOLICITUDES' section shows a single entry: '159 ND (26-01-2026 21:13:53 por [redacted]) resuelta'. A 'HISTORICO DE CERTIFICADOS' section shows one entry with ID: 638, SERIAL: S1449988FA09A5B7C7D2D18FB517DECC, Alt: acmeproxy.uv.es, KEY: ec-256 (id-ecPublicKey/256), IGTF: f, and an expiration date of 'Expira /Tue Jan 26 21:04:15 2027/'. The interface also features a sidebar with navigation options like 'Solicitudes', 'Dominios', 'Mis Solicitudes', 'Mis Dominios', 'Noticias', and 'Comentarios'.

The screenshot shows the ACMEBOT interface for domain #455. The header is identical to the first screenshot. The main content area displays the domain name and a list of AITDoms. The 'Lugar' is 'S033 - Servei D'informatica' and the 'App' is 'App Servidor de NTP'. The 'Propiedad de' is 'Resp.' and the 'desde' date is '16-04-2026 08:07:18'. The 'Contactos' are listed as '@uv.es'. The 'Info' section shows 'CSR: f', 'MANUAL: t', 'Tipo Clave: ecc', and 'IGTF: f'. Below this, there are buttons for 'Modificar', 'Certificado', 'Cadena de CA's', 'Clave privada', and 'PEM key+cert+ca's'. A 'SOLICITUDES' section shows a single entry: '272 ND (16-04-2026 08:07:18 por [redacted]) resuelta'. A 'HISTORICO DE CERTIFICADOS' section shows one entry with ID: 705, SERIAL: 6E5C28695D50A179D582D3A1163D73B9, Alt: [redacted].uv.es [redacted].uv.es [redacted].valencia.edu [redacted].red.valencia.edu [redacted], KEY: ec-256 (id-ecPublicKey/256), IGTF: f, and an expiration date of 'Expira /Sun Nov 01 07:28:37 2026/'. The interface also features a sidebar with navigation options like 'Solicitudes', 'Dominios', 'Mis Solicitudes', 'Mis Dominios', 'Noticias', and 'Comentarios'.



Conclusiones



¿Qué nos aporta ACMEBOT?

Eficiencia y Gestión Centralizada



Gestión Integral del Ciclo de Vida

Control total automatizado: desde la solicitud inicial y emisión hasta la renovación y baja.



Centralización Estratégica

Uso de cuenta única de CA que simplifica migraciones y la gestión institucional masiva.



Simplicidad Absoluta para el Cliente

Automatización real sin dependencias externas ni necesidad de conocimientos técnicos del protocolo ACME.

Seguridad y Éxito Operativo



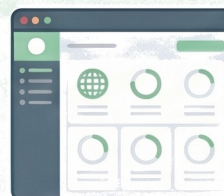
Seguridad Robusta por Diseño

Múltiples capas de protección integradas, incluyendo canales cifrados y códigos de acceso únicos.



Éxito Operativo Contrastado

Plataforma estable en evolución activa que gestiona cientos de dominios con éxito rotundo.



Resumen del Alcance y Escala Actual

354

Dominios gestionados

26

Entes universitarios

122

Servidores automatizados



¿Qué podemos aportar?

Si en vuestra institución estáis planteando un reto similar, estamos disponibles para **compartir** nuestra experiencia: **criterios de diseño, decisiones** que tomamos por el camino y los **problemas** con los que nos hemos ido encontrando.

No es un camino que haya que recorrer en solitario.



¿Preguntas?

Jt 2026
Red IRIS

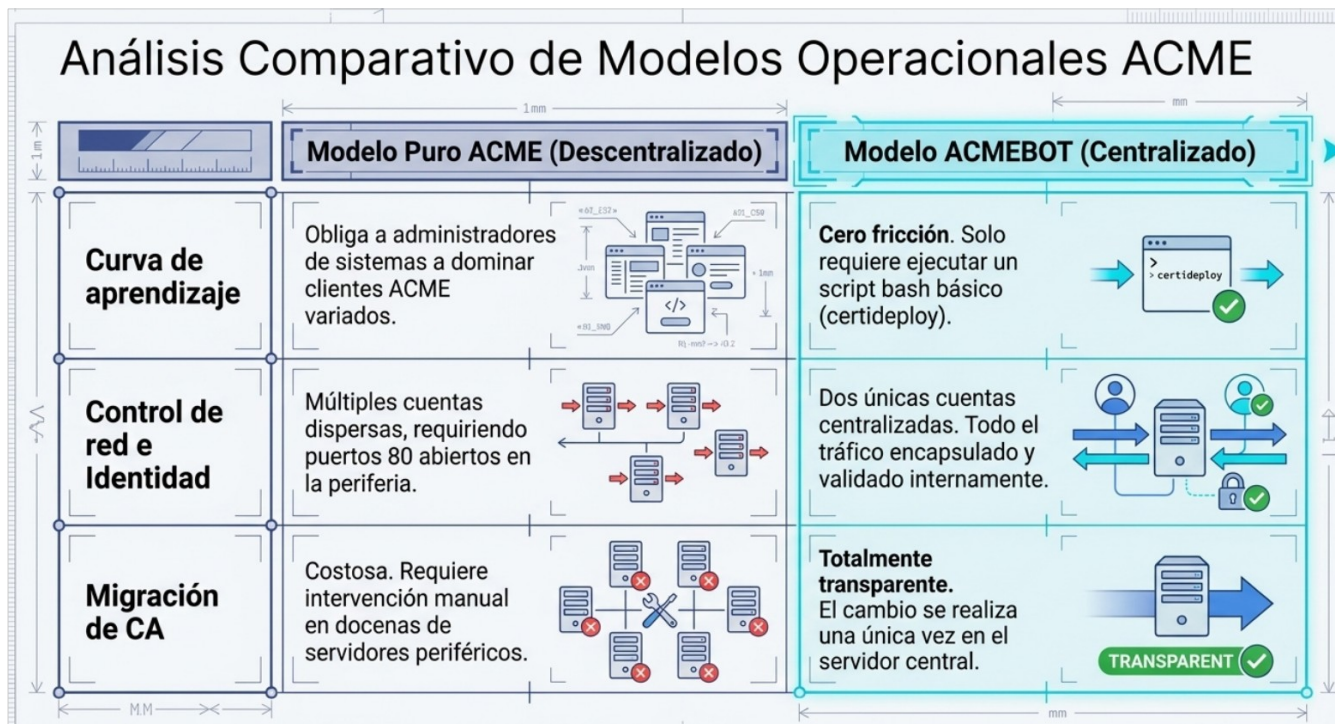

A CORUÑA
22-25 JUNIO Universidade da Coruña

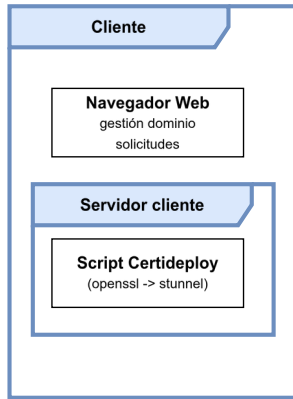


Anexos



Modelo Puro vs Centralizado





- Cliente
- Servidor
- Externo

