UCLM

UNIVERSIDAD DE CASTILLA-LA MANCHA

# *La Política de Seguridad de Red de la Universidad de Castilla-La Mancha*

***Evangelino Valverde Álvarez***

***Área de Informática y Comunicaciones UCLM***

**Octubre de 2005**
**XX Grupos de Trabajo: IRIS-CERT**
**JJTT 2005 - Logroño**

# Contexto: La UCLM

- **4** campus:
  - Albacete, Ciudad Real, Cuenca y Toledo
- Presencia en **8** localidades
- **30.000** estudiantes
- **48** edificios
- **10.000** nodos de red

# Contexto: El Plan de Seguridad

- 2001. Sanción por infracción del artículo 9 de la LOPD
- 2002. Dirección Académica de Seguridad Informática dependiente del Rector
- 2002. Plan de Seguridad Informática (**PSI**)
- 2003. Versión inicial de la Política de Seguridad de Red
- 2005. Aceptación de la Política de Seguridad de Red (**PSR**) por la Comisión de Tecnologías de la Información

# Contexto: Dónde encaja la PSR

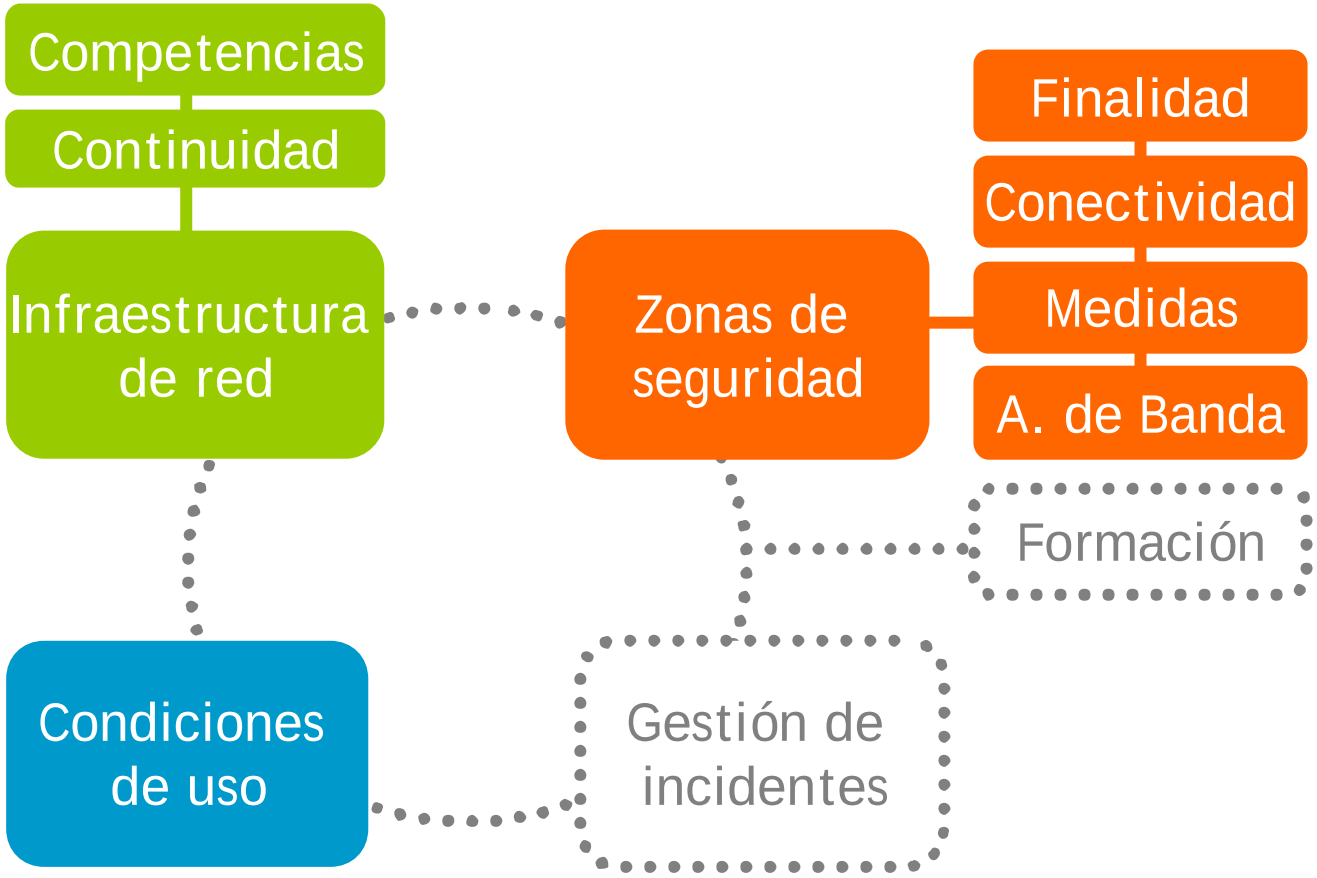
# Principios de diseño de la Política

1. Buscar servicios antes que restricciones
   - Disponibilidad, confidencialidad e integridad
2. “Tan simple como sea posible pero no más simple”
3. No pensar demasiado en cómo lo implementaremos
4. Es una herramienta de la organización, no del Área de Informática
5. Perseguir los problemas:
   - Implicar en el desarrollo a docentes de titulaciones técnicas
   - Tratar los temas delicados: responsabilidades, delegaciones, etc.

# Proceso de elaboración

1. Estudio de la situación en la UCLM
2. Evaluación de otras políticas de seguridad
3. Elaboración de un borrador (Área de Informática + Director Académico de Seguridad Informática)
4. Evaluación del borrador con pequeños grupos de los colectivos más afectados
5. Adaptación de los puntos de conflicto del borrador
6. Aceptación del borrador por parte de la Comisión de Tecnologías de la Información
7. Aprobación de la Política de Seguridad de Red en Consejo de Gobierno

# Contenido de la política



# Infraestructura de red: Continuidad

- Indicadores y objetivos
  - Tiempos **máximos** de parada:
    - En la red troncal: **4 h**
    - En la red de acceso a los puestos: **8 h**
  - Tiempos de parada **acumulados** durante un trimestre:
    - Para cada campus: **12 h**
    - Para cada centro: **24 h**
  - Dos jornadas:
    - Diurna: laborables de 9:00 a 21:00
    - Nocturna: resto
  - El tiempo en la jornada nocturna computa como 1/2
- Incluye servicios de infraestructura: DNS y DHCP
- Constituye el SLA con nuestros usuarios, expresado en términos muy simples

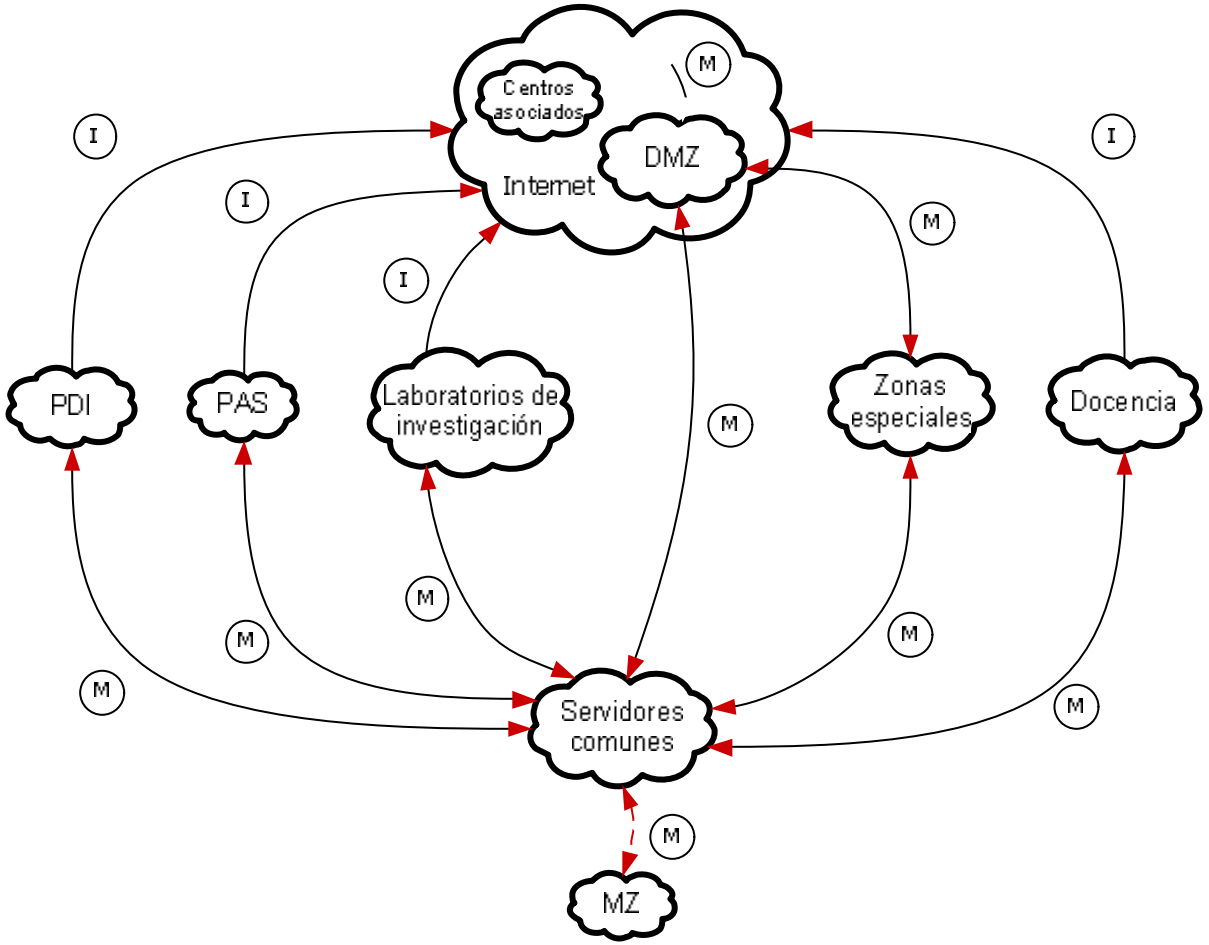
# Infraestructura de red: Competencias

- **Responsabilidad** del Área de Inf. y Comunicaciones
- Las **delegaciones** de la red de comunicaciones deben estar previamente acordadas y documentadas
- Gestión de **dominios DNS** a través del Vicerrectorado de Coordinación, Economía y Comunicación
- Los dominios DNS locales no harán referencia a direcciones de red externas

# Zonas: Finalidad

- **PDI, PAS, Investigación, Docencia**
- Servidores públicos (**DMZ**): Web, correo, etc.
- Servidores comunes: DHCP, DNS, NTP, etc.
- Servidores de datos corporativos (**MZ**): SGDB
- Centros asociados: fundaciones, etc.
- Zonas especiales:
  - Videoconferencia, Visitantes, Telefonía IP, Televisión, PIU, etc.

# Zonas: Conectividad



# Zonas: Medidas de seguridad por nodo

- 15 medidas:
  - 7 de carácter técnico
  - 8 de carácter administrativo
- Dependiendo de la zona, su cumplimiento es:
  - Necesario
  - Recomendado
  - Opcional
  - No aplicable
- Inspirado en el DRAFT NIST 800-53, *Recommended Security Controls for Federal Information Systems*

# Ejemplo: Medidas en la DMZ (I)

| Medida | Grado |
|---|---|
| Persona de contacto por nodo | Necesario |
| Persona de contacto por subred | Necesario |
| Nodo administrado por los servicios informáticos | Opcional |
| Nodo administrado por el usuario | Opcional |
| Declaración de servicios y puertos | Necesario |
| Autorización para la instalación de nodos | Necesario |
| Gestión de parches de seguridad | Necesario |
| Antivirus actualizado | Recomendado |

# Ejemplo: Medidas en la DMZ (II)

| Medida | Grado |
|---|---|
| Ubicación dedicada | Necesario |
| Autenticación individual | Necesario |
| Medidas de autorización | Necesario |
| Permisos y servicios mínimos | Necesario |
| Trazabilidad | Necesario |
| Monitorización | Necesario |
| Comunicaciones cifradas | Opcional |

# Zonas: Ancho de banda asignado (I)

- Orientado a mejorar la disponibilidad
- En el acceso a **Internet**
  - Ancho de banda **mínimo y máximo** por nodo, asimétrico, diferente para cada zona de clientes
  - El mínimo se obtiene por reparto ponderado por nodo
  - El máximo está fijado inicialmente en:
    - **10 Mbps** de bajada
    - **5 Mbps** de subida
  - Para los servidores, en función de las necesidades
  - Beneficios
    - Evitamos "juzgar" los contenidos/protocolos
    - Prevenimos las denegaciones de servicio

# Zonas: Ancho de banda asignado (II)

- En el acceso a **recursos internos**
  - Reserva de ancho de banda estricta para servicios críticos de red, aplicaciones corporativas y correo
- En situaciones de **congestión**
  1. Resto de tráfico UCLM
  2. Navegación en Internet
  3. Resto de tráfico Internet

# Condiciones de uso de la red

- Es una adaptación de las condiciones de uso del Documento de Afiliación a **RedIRIS**:
  1. **Legalidad** de las prácticas llevadas a cabo sobre la red
  2. **Uso correcto de los recursos** (respetar la finalidad, no congestionar la red, etc.)
  3. **Confidencialidad** de la actividad de los usuarios
  4. Respeto de la **propiedad intelectual** e industrial
  5. Responsabilidad de la UCLM de **velar por el cumplimiento** de esta política

# Pasos siguientes

- Elaboración de la Guía de Aplicación de la Política de Seguridad de Red
  - Cubre el salto entre el qué y el cómo
  - Adapta permanentemente los cambios tecnológicos
- Elaboración de los procedimientos de soporte
- Implantación, centro por centro
- Paralelamente:
  - Formación de usuarios en materia de seguridad
  - Procedimiento de gestión de incidentes de seguridad
- En el papel funciona todo: ya os contaremos en los XXI Grupos de Trabajo …


# Plan de Seguridad Informática