1.- NORMATIVA DE POLÍTICA DE SEGURIDAD DE LA RED DE COMUNICACIONES

(Aprobado en Consejo de Gobierno de 30 de marzo de 2006 y publicado en el BO-UCLM nº 91 de abril de 2006).

CAPÍTULO I. DISPOSICIONES GENERALES

Artículo 1. Objeto.

Esta política tiene como objeto definir la normativa de seguridad de la red de comunicaciones de la Universidad de Castilla-La Mancha que garantice la confidencialidad, integridad y disponibilidad de la información en los usos requeridos por la comunidad universitaria.

Artículo 2. Ámbito de aplicación.

La Universidad de Castilla-La Mancha dispone de una red de comunicaciones que da servicios de voz y datos a todos sus centros. En adelante, por el ámbito del documento, se hará referencia a la red de datos como «la red de comunicaciones» o simplemente como «la red».

Las medidas expuestas en este documento afectan a todo el personal docente e investigador, al personal de administración y servicios y en general, a todos los miembros de la comunidad universitaria que accedan a la red de comunicaciones.

En lo que respecta a los equipos informáticos, su ámbito de aplicación son todos los nodos (ordenadores personales, servidores, impresoras, etc.) conectados a la red de comunicaciones de la Universidad.

Las medidas expuestas en este documento referidas a la transmisión de datos afectan exclusivamente a las comunicaciones basadas en el conjunto de protocolos TCP/IP.

En cuanto a los temas abordados, se incide sobre tres aspectos:

- La infraestructura de red.

- La heterogeneidad de los colectivos de usuarios que comparten esa infraestructura, y por tanto, de sus necesidades de seguridad.

- La política de uso de la red por parte de los usuarios que, aunque su ámbito supera al de este documento, ha sido incluida por sus repercusiones directas sobre la seguridad de la red.

Por tener un alcance mayor que el de la seguridad en la red, no se ha considerado conveniente incluir en esta normativa la política de tratamiento de incidentes de seguridad y la política de formación del personal, si bien resulta un complemento imprescindible para la aplicación efectiva de las medidas aquí descritas.

Artículo 3. Definiciones.

a) Cliente: equipo informático cuyo papel habitual es el de consumir servicios ofertados por otros equipos informáticos. Es el caso de los ordenadores personales situados en los puestos de trabajo.

b) DHCP (Dynamic Host Configuration Protocol): protocolo de red que permite la asignación dinámica de direcciones IP.

c) DMZ (Demilitarized Zone): término utilizado comúnmente para designar una zona de la red donde las medidas de seguridad perimetral son menos estrictas. En el caso de la red de la UCLM coincide con la zona de servidores públicos.

d) DNS (Domain Name System): servicio de red cuya principal función es traducir nombres en direcciones IP y viceversa.

e) ICMP: protocolo de la familia TCP/IP orientado al control de las comunicaciones.

f) IPSec: conjunto de servicios de seguridad para el protocolo de red IP.

g) Mbps (Megabit por segundo): medida de ancho de banda. Un Mbps corresponde a la transmisión de un millón de bits por segundo.

h) MZ (Militarized Zone): término utilizado comúnmente para designar una zona de la red donde se extreman las medidas de seguridad perimetrales. En el caso de la red de la UCLM coincide con la zona de servidores de datos corporativos.

i) Nodo: cualquier dispositivo conectado a una red de comunicaciones.

j) NTP (Network Time Protocol): protocolo que permite la sincronización horaria de nodos a través de la red.

k) Red privada virtual: tecnología que habitualmente se utiliza para desplegar una red segura de ámbito privado sobre otra no segura de ámbito público.

l) Servidor: equipo informático cuya única función es suministrar servicios a otros equipos informáticos. Habitualmente se encuentran ubicados en salas dedicadas.

m) SNMP: protocolo de la familia TCP/IP para la administración a través de la red de equipamiento y servicios informáticos.

n) SOCKS: protocolo genérico para el uso de comunicaciones TCP/IP de cualquier tipo a través de un intermediario (*proxy*)

o) TCP/IP: conjunto de protocolos de red que constituye la tecnología de comunicaciones de la red Internet y también de la red de la Universidad de Castilla-La Mancha.

p) Usuario: cualquier persona que utilice la infraestructura de red de la Universidad.

q) Zona de seguridad: conjunto de nodos de una red que comparten finalidad, condiciones de conectividad, medidas de seguridad y modelo de asignación de ancho de banda.

CAPÍTULO II. INFRAESTRUCTURA DE RED

Artículo 4. Continuidad del servicio.

La red de la UCLM se encuentra estructurada en tres niveles:

- Red troncal o *backbone*, que cubre los enlaces entre campus y la conexión a Internet.
- Red de distribución, núcleo de las comunicaciones en cada uno de los campus.
- Red de acceso a los puestos.

La continuidad del servicio de red se medirá utilizando los siguientes indicadores:

a) Duración de una interrupción del servicio en la red troncal o en la red de distribución.

b) Duración de una interrupción del servicio en la red de acceso a los puestos.

c) Tiempo acumulado de interrupción del servicio durante un trimestre para cada campus (red troncal o red de distribución).

d) Tiempo acumulado de interrupción del servicio durante un trimestre para cada centro (red de acceso).

El anexo I *Parámetros para la medición de la continuidad del servicio* detalla como se computará la interrupción del servicio, así como los valores fijados inicialmente como objetivo. Es labor de la Comisión de Tecnologías de la Información, Comunicaciones y Seguridad Informática la revisión periódica y el ajuste del contenido de este anexo.

Artículo 5. Gestión de la red de comunicaciones.

El diseño de la red de comunicaciones se realizará con el apoyo del personal necesario para una correcta definición de los requerimientos técnicos y funcionales de la red.

Corresponde al personal autorizado del Área de Informática y Comunicaciones coordinar el diseño y la gestión de la red de comunicaciones de la Universidad. Entre otras actividades engloba:

- El diseño físico y lógico de la red.
- La gestión de los enlaces de comunicaciones.
- La gestión del cableado de los edificios.
- La gestión de la electrónica de red.
- La gestión de las medidas de seguridad de la red.
- La gestión de la interconexión de la red de la UCLM con otras redes, como RedIRIS.

El Gerente del Área de Informática y Comunicaciones podrá delegar la gestión del cableado y la gestión de la electrónica de un centro, aula o laboratorio en el personal autorizado del centro cuando las condiciones así lo requieran, mediante la aprobación de un acuerdo en el que se especifiquen las condiciones de la delegación.

Gestión de nombres de dominio

Con en fin de preservar la imagen externa de la Universidad, el alojamiento de dominios DNS dentro del espacio de direcciones IP de la UCLM estará sujeto a los criterios de aceptación del Vicerrectorado de Coordinación, Economía y Comunicación. De forma coordinada con el Área de Informática se mantendrá un registro en el que se especifique:

- El nombre, propósito y vigencia del dominio DNS albergado.
- Las direcciones IP correspondientes a los servidores DNS de ese dominio.
- Los datos de contacto del responsable administrativo del dominio.
- Los datos de contacto del responsable técnico del dominio.

En ningún caso se crearán registros DNS que, correspondiendo a un dominio albergado dentro de la UCLM, hagan referencia a direcciones de red externas. La finalidad de esta medida es evitar que se puedan asumir como propios contenidos ajenos a la institución.

Capítulo III. Zonas de seguridad

Artículo 6. Finalidad.

Dentro de la red de comunicaciones de la UCLM existen varios entornos que comparten una misma infraestructura, pero que debido a los requerimientos de seguridad impuestos por su finalidad, deben mantenerse claramente separados. En este apartado se describe cada uno de estos entornos, que dan origen a las diferentes zonas de seguridad de la red.

La estructuración por zonas no guarda ninguna relación con la distribución física de los nodos en campus o centros, sólo con su finalidad.

INTERNET

Pertenecen a esta zona todos los nodos ubicados fuera de la red de la Universidad, que acceden o que son accesibles desde la red Internet.

CENTROS ASOCIADOS

Pertenecen a esta zona todos los nodos ubicados en centros asociados a la Universidad.

SERVIDORES PÚBLICOS (DMZ)

Pertenecen a esta zona todos aquellos nodos que ofrecen servicios al resto de Internet, como servidores de correo, de DNS, o Web.

PDI

Esta zona alberga los nodos del personal docente e investigador de la Universidad.

PAS

Esta zona alberga los nodos del personal de administración y servicios de la Universidad.

LABORATORIOS DE INVESTIGACIÓN

Contiene todos aquellos nodos dedicados a las labores de investigación.

DOCENCIA

A esta zona pertenecen todos los nodos ubicados en aulas de la Universidad o dedicados a dar servicio a los alumnos.

SERVIDORES DE DATOS CORPORATIVOS (MZ)

Alberga los servidores corporativos con información sensible, dedicados a labores relacionadas exclusivamente con el funcionamiento interno de la Universidad, como la gestión de alumnos o la gestión económica.

SERVIDORES COMUNES

Contiene todos aquellos servidores que dan o pueden dar servicio a varias comunidades de usuarios, pero que no deben ser accedidos desde Internet. Es el caso de los controladores de dominio, servidores de almacenamiento, etc.

ZONAS ESPECIALES

Además de las ya mencionadas, existen zonas adicionales con una finalidad y requisitos de seguridad muy específicos:

1. Visitantes. Esta zona está dedicada a albergar los ordenadores de las personas que visitan la Universidad durante un periodo corto de tiempo, como los asistentes a un congreso o los convocados a una rueda de prensa.

2. Videoconferencia. Esta zona alberga los equipos de videoconferencia de sala.

3. Televisión. Esta zona alberga los equipos dedicados a la emisión y recepción del canal de televisión de la UCLM.

4. Telefonía IP. Esta zona alberga los equipos de telefonía IP de la Universidad.

5. Gestión de la red. Esta zona está dedicada a la gestión de los dispositivos de red de la Universidad.

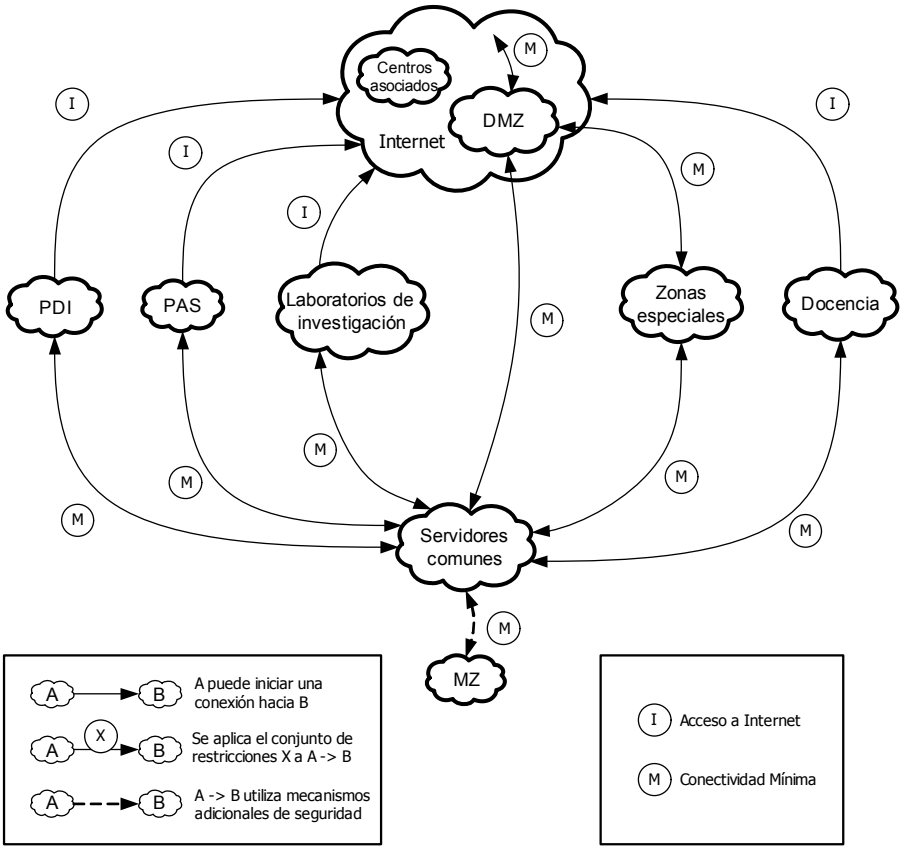
6. Mantenimiento y seguridad de los edificios. Esta red alberga los sistemas de telemetría y control de los edificios, las cámaras digitales de vigilancia, los sistemas de control de presencia, alarmas, etc.

7. Puntos de información universitarios. Esta zona alberga los puntos de información para los alumnos de la UCLM. Por su finalidad se considera una zona diferenciada de la de docencia.

Artículo 7. Conectividad entre zonas.

La estructuración por zonas permite, entre otras funcionalidades, aplicar mecanismos que ayuden a hacer efectivos los objetivos de seguridad de cada entorno. Uno de estos mecanismos consiste en establecer filtros de tráfico de red entre zonas, orientados a reducir el riesgo de que se produzca un incidente de seguridad.

El diagrama 1 representa los máximos de conectividad entre nodos de diferentes zonas. Los arcos simbolizan la conectividad entre zonas y las puntas de las flechas, quién puede recibir una conexión entrante. Las etiquetas de los arcos indican el filtro de tráfico a aplicar, mientras que los arcos de trazo discontinuo simbolizan que sólo existe conectividad a través de mecanismos de seguridad adicionales como IPSec o redes privadas virtuales.



Dentro de cada zona, si así se requiere, podrán establecerse filtros adicionales hasta el nivel centro, grupo de investigación, aula o unidad. En los casos en los que sea necesario extremar las medidas de seguridad, se limitará la conectividad a los nodos y servicios imprescindibles para la prestación del servicio.

A continuación se describen los conjuntos de restricciones que aparecen en la figura: Acceso a Internet, Conectividad Total y Conectividad Mínima.

Acceso a Internet (I)

La finalidad de este conjunto de restricciones es limitar la cantidad de incidentes de seguridad que puedan ser originados, de forma intencionada o accidental, por nodos pertenecientes a la red de la UCLM. Debido al cambio frecuente de las técnicas de ataque en materia de seguridad informática, este filtro deberá ser actualizado en cada revisión de la política de seguridad en red.

Se permite todo el tráfico excepto el que se lista a continuación:

- El tráfico IP con origen en direcciones no pertenecientes al rango de direcciones públicas de la Universidad o en direcciones reservadas.
- El tráfico de correo electrónico.
- Las comunicaciones específicas de los sistemas operativos corporativos (compartición de carpetas, impresión, etc.)
- El tráfico de gestión del equipamiento de red (SNMP, etc.)
- Las comunicaciones de servidores de bases de datos (Microsoft SQL-Server, Oracle, etc.)
- El tráfico orientado a saltar las medidas de seguridad de este conjunto de restricciones (SOCKS, etc.)

Conectividad Total (T)

Por defecto, se permite todo el tráfico entre los nodos involucrados en la comunicación.

Conectividad Mínima (M)

Se permite la conectividad mínima necesaria para la prestación de los servicios.

Directrices generales

Además de los filtros anteriormente descritos, que afectan sólo a parte de los nodos, existen dos directrices generales:

- El tráfico de correo electrónico sólo puede ser manejado por servidores registrados y autorizados por el gerente del Área de Informática y Comunicaciones. Adicionalmente, existe un único punto redundado de entrada y salida de mensajes de la Universidad, donde se aplican las directrices de seguridad dictadas por RedIRIS.
- No se permitirá la entrada o salida de tráfico cuya dirección de origen no sea coherente con la subred de la que procede.

Artículo 8. Medidas de seguridad en los nodos.

En este apartado se enumeran las medidas de seguridad con las que deben contar los nodos de la red de comunicaciones. La zona en la que esté instalado el nodo determinará el conjunto de medidas a aplicar, teniendo cada una de ellas carácter optativo, recomendado o necesario. Las medidas de seguridad aplicables son:

1. **Persona de contacto por nodo.** El nodo cuenta con un responsable, que mantiene una relación contractual con la Universidad, del que se tienen registrados los siguiente datos:

- Nombre y apellidos.
- El DNI.
- La dirección de correo electrónico.
- El teléfono de contacto, fijo y/o móvil.

En el caso de los equipos cliente, la persona de contacto debe ser el usuario habitual del ordenador.

En el caso de servidores, puede existir más de una persona de contacto, distinguiéndose entre contactos técnicos y administrativos.

2. Persona de contacto por subred. La subred en la que está ubicado el nodo cuenta con un responsable, que mantiene una relación contractual con la Universidad, del que se tienen registrados los siguientes datos:

- Nombre y apellidos.
- El DNI.
- La dirección de correo electrónico.
- El teléfono de contacto, fijo y/o móvil.

El responsable de la subred asume la responsabilidad sobre el nodo cuando no existe un responsable del nodo o cuando éste no puede ser localizado.

3. **Nodo administrado por los servicios informáticos.** El nodo es administrado por el personal del Área de Informática y Comunicaciones de la Universidad.

4. **Nodo administrado por el usuario.** El nodo es administrado por la persona que figura como persona de contacto de ese nodo o de la subred en la que está ubicado.

5. **Declaración de servicios y puertos.** La persona responsable del nodo o de la subred debe declarar la relación de servicios y protocolos que pretende ofertar desde un determinado nodo, indicando:

- La denominación y finalidad de servicio.
- El tipo de transporte y puerto utilizado para ofertar dicho servicio.

6. **Autorización para la instalación de nodos.** La conexión a la red en la zona requiere una autorización previa. Se debe indicar que figura llevará a cabo dicha autorización.

7. **Gestión de parches de seguridad.** Los parches que solventan vulnerabilidades de seguridad conocidas y que afecten a la configuración software del nodo deben ser aplicados en un plazo máximo de un mes.

8. **Antivirus actualizado.** El nodo dispone de software de antivirus actualizado al menos una vez al día.

9. **Ubicación dedicada.** El nodo está situado en una ubicación dedicada exclusivamente al alojamiento de equipamiento informático en explotación, en condiciones ambientales adecuadas y sometido a un control de acceso físico estricto.

10. **Autenticación individual.** El nodo dispone de medidas de seguridad que permiten autenticar de forma unívoca a los usuarios en sus sesiones de trabajo y en el acceso a sus recursos y éstas medidas son aplicadas permanentemente.

11. **Control de acceso.** El nodo dispone de medidas de seguridad que permiten conceder o denegar el acceso a un usuario o a un grupo de usuarios y éstas son aplicadas permanentemente.

12. **Permisos y servicios mínimos.** El nodo dispone de los permisos y servicios mínimos necesarios para llevar a cabo sus funciones.

13. **Trazabilidad.** El nodo recopila información de traza que permite, al menos, conocer:

- Los intentos de inicio de una sesión de trabajo en el nodo y si estos han tenido o no éxito.
- Los cambios sobre la configuración de usuarios y grupos del sistema.
- Los cambios sobre la configuración de trazabilidad.

La información de trazabilidad debe conservarse, en cada caso, durante el tiempo estipulado por la legislación aplicable [1][2][3], siendo el mínimo, si no esta sujeto a ninguna norma, de un mes. Adicionalmente el reloj del nodo debe estar sincronizado con una fuente de tiempo fiable.

Se debe poner especial cuidado en mantener la confidencialidad e integridad de estos datos.

14. **Monitorización.** La actividad en red del nodo y su información de auditoría podrá ser monitorizada por el personal designado del Área de Informática y Comunicaciones o por el responsable de la subred con objeto de:

- Comprobar la efectividad de las medidas de seguridad aplicadas sobre el nodo.
- Recabar información relacionada con un incidente de seguridad.

15. **Comunicaciones cifradas.** El nodo utiliza cifrado en sus comunicaciones.

Las tablas 1 a 8 muestran el perfil de seguridad aplicable a los nodos de cada una de las zonas.

SERVIDORES PÚBLICOS (DMZ)

Tabla 1: Medidas de seguridad para los nodos de la zona DMZ

Medidas	Grado	Datos adicionales
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	Contacto técnico
Declaración de servicios y puertos	Necesario	
Autorización para la instalación de nodos	Necesario	Ver tabla 2
Gestión de parches de seguridad	Necesario	
Antivirus actualizado	Recomendado	
Ubicación dedicada	Necesario	
Autenticación individual	Necesario	
Medidas de autorización	Necesario	
Permisos y servicios mínimos	Necesario	
Trazabilidad	Necesario	
Monitorización	Necesario	
Comunicaciones cifradas	Opcional	

Tabla 2: Autorización para la instalación de nodos en la zona DMZ

Propósito del nodo	Persona que autoriza
Docencia e Investigación	Decano/director de Centro o Departamento
Servicios corporativos	Director del Área de Tecnología y Comunicaciones

En caso de que el nodo sea administrado por el usuario debe existir una persona de contacto técnico, que puede ser diferente del contacto del nodo, que actúa como administrador del equipo.

PDI

Tabla 1: Medidas de seguridad para los nodos de la zona PDI

Medidas	Grado	Datos adicionales
Persona de contacto por nodo	Necesario	
Persona de contacto por subred	Necesario	
Nodo administrado por los servicios informáticos	Recomendado	
Nodo administrado por el usuario	Opcional	
Declaración de servicios y puertos	No aplicable	
Autorización para la instalación de nodos	Necesario	Autoriza el decano/director del centro
Gestión de parches de seguridad	Necesario	
Antivirus actualizado	Necesario	Actualización recomendada cada 90 mín.
Ubicación dedicada	No aplicable	
Autenticación individual	Necesario	
Medidas de autorización	Necesario	
Permisos y servicios mínimos	Necesario	
Trazabilidad	Necesario	
Monitorización	Necesario	
Comunicaciones cifradas	Opcional	

En el caso de los nodos de la zona de PDI el nodo será administrador por los servicios informáticos, por el usuario o por ambos de forma compartida.

PAS

Tabla 1: Medidas de seguridad para los nodos de la zona PAS

Medidas	Grado	Datos adicionales
Persona de contacto por nodo	Necesario	
Persona de contacto por subred	Necesario	
Nodo administrado por los servicios informáticos	Necesario	
Nodo administrado por el usuario	No aplicable	
Declaración de servicios y puertos	No aplicable	
Autorización para la instalación de nodos	Necesario	Autoriza el director de la unidad
Gestión de parches de seguridad	Necesario	Actualización diaria
Antivirus actualizado	Necesario	Actualización máxima cada 90 mín.
Ubicación dedicada	No aplicable	
Autenticación individual	Necesario	
Medidas de autorización	Necesario	
Permisos y servicios mínimos	Necesario	
Trazabilidad	Necesario	
Monitorización	Necesario	
Comunicaciones cifradas	Opcional	

LABORATORIOS DE INVESTIGACIÓN

Tabla 1: Medidas de seguridad para los nodos de la zona Laboratorios de Investigación

Medidas	Grado	Datos adicionales
Persona de contacto por nodo	Recomendado	
Persona de contacto por subred	Necesario	
Administrado por los servicios informáticos	No aplicable	
Administrado por el usuario	Opcional	
Declaración de servicios y puertos	No aplicable	
Autorización para la instalación de nodos	Necesario	Autoriza el director del grupo de investigación
Gestión de parches de seguridad	Recomendado	
Antivirus actualizado	Recomendado	Actualización máxima cada 90 mín.
Ubicación dedicada	No aplicable	
Autenticación individual	Recomendado	
Medidas de autorización	Recomendado	
Permisos y servicios mínimos	Recomendado	
Trazabilidad	Recomendado	
Monitorización	Recomendado	
Comunicaciones cifradas	Opcional	

DOCENCIA

Tabla 1: Medidas de seguridad para los nodos de la zona Docencia

Medidas	Grado	Datos adicionales
Persona de contacto por nodo	No aplicable	
Persona de contacto por subred	Necesario	
Administrado por los servicios informáticos	Opcional	
Administrado por el usuario	Opcional	
Declaración de servicios y puertos	No aplicable	
Autorización para la instalación de nodos	Necesario	Autoriza el decano/director del centro
Gestión de parches de seguridad	Necesario	
Antivirus actualizado	Necesario	Actualización máxima cada 90 mín.
Ubicación dedicada	No aplicable	
Autenticación individual	Necesario	
Medidas de autorización	Necesario	
Permisos y servicios mínimos	Necesario	
Trazabilidad	Necesario	
Monitorización	Necesario	
Comunicaciones cifradas	Opcional	

SERVIDORES DE DATOS CORPORATIVOS (MZ)

Tabla 1: Medidas de seguridad para los nodos de la zona MZ

Medidas	Grado	Datos adicionales
Persona de contacto por nodo	Necesario	
Persona de contacto por subred	Necesario	
Administrado por los servicios informáticos	Necesario	
Administrado por el usuario	No aplicable	
Declaración de servicios y puertos	Necesario	
Autorización para la instalación de nodos	Necesario	Autoriza el Gerente del Área de Informática y Comunicaciones.
Gestión de parches de seguridad	Necesario	
Antivirus actualizado	Recomendado	
Ubicación dedicada	Necesario	
Autenticación individual	Necesario	
Medidas de autorización	Necesario	
Permisos y servicios mínimos	Necesario	
Trazabilidad	Necesario	
Monitorización	Necesario	
Comunicaciones cifradas	Necesario	

SERVIDORES COMUNES

Tabla 1: Medidas de seguridad para los nodos de la zona Servidores Comunes

Medidas	Grado	Datos adicionales
Persona de contacto por nodo	Necesario	
Persona de contacto por subred	Necesario	
Administrado por los servicios informáticos	Recomendado	
Administrado por el usuario	No aplicable	
Declaración de servicios y puertos	Necesario	
Autorización para la instalación de nodos	Necesario	Ver tabla 9
Gestión de parches de seguridad	Necesario	
Antivirus actualizado	Recomendado	
Ubicación dedicada	Necesario	
Autenticación individual	Necesario	
Medidas de autorización	Necesario	
Permisos y servicios mínimos	Necesario	
Trazabilidad	Necesario	
Monitorización	Necesario	
Comunicaciones cifradas	Opcional	

Tabla 2: Autorización para la instalación de nodos en la zona Servidores Comunes

Propósito del nodo	Persona que autoriza
Docencia e Investigación	Decano/Director de Centro o Departamento
Servicios corporativos	Director del Área de Tecnología y Comunicaciones

Zonas especiales

Dentro del conjunto de zonas especiales se pueden distinguir dos casos:

- La zona de visitantes, en la que por su finalidad resulta imposible controlar las medidas de seguridad incorporadas por los nodos. En este caso todos los mecanismos utilizados por la Universidad son de tipo perimetral.

- El resto de zonas especiales, donde se aplicará como principio general mantener los privilegios mínimos necesarios para la prestación y mantenimiento de los servicios.

Artículo 9. Gestión del ancho de banda.

Las medidas de gestión del ancho de banda en la red de la Universidad están orientadas a garantizar la disponibilidad de los recursos necesarios para:

- Desarrollar la actividad docente e investigadora.

- Llevar a cabo los procesos de gestión interna que dan soporte a la actividad docente e investigadora.

Se distingue entre las medidas a aplicar en el acceso a Internet y las medidas a aplicar en el acceso a los recursos internos.

Acceso a Internet

El ancho de banda total disponible para el acceso a Internet es asignado siguiendo estos criterios:

- Cada nodo dispone de un ancho de banda mínimo garantizado, que será idéntico para todos los nodos de una misma zona.

- Los servidores ubicados en las zonas DMZ, MZ y de servidores comunes disponen del ancho de banda mínimo garantizado que se estime oportuno para la prestación de cada servicio.

- Existe un ancho de banda máximo por nodo, que será idéntico para todos los nodos de una zona. Esta cota tiene por objeto minimizar la posibilidad de que un nodo sea utilizado para saturar la capacidad de la red o para llevar a cabo un ataque de denegación de servicio.

Para la asignación de ancho de banda por nodo se utilizarán los valores de la tabla 10, *Ponderación de nodos por zonas*, del anexo II *Parámetros para la gestión del ancho de banda*.

La finalidad de asignar un ancho de banda asimétrico en las zonas destinadas a albergar nodos cliente, menor de salida que de entrada, es la de evitar que estos nodos ejerzan como servidores encubiertos, desvirtuando la estructuración por zonas de la red de comunicaciones.

Las unidades de referencia para la asignación del ancho de banda mínimo entrante o saliente será se obtendrá aplicando las fórmulas 1 y 2.

$$U_e = \frac{B_{te} - B_{re}}{\sum_{I=0}^{n} (N_i \cdot P_{ei})}$$

Fórmula 1: Unidad de referencia para la asignación de ancho de banda entrante

$$U_s = \frac{B_{ts} - B_{rs}}{\sum_{I=0}^{n} (N_i \cdot P_{si})}$$

Fórmula 2: Unidad de referencia para la asignación de ancho de banda saliente

Donde:

- U_e es la unidad de referencia para la asignación del ancho de banda entrante.
- B_{te} es el ancho de banda total entrante.
- B_{re} es el ancho de banda entrante reservado para servicios corporativos.
- N_i es el número de nodos en la zona *i*.
- P_{ei} es la ponderación para tráfico entrante de la zona *i*.
- U_s es la unidad de referencia para la asignación del ancho de banda saliente.
- B_{ts} es el ancho de banda total saliente.
- B_{rs} es el ancho de banda saliente reservado para servicios corporativos.
- P_{si} es la ponderación para tráfico saliente de la zona *i*.

El ancho de banda mínimo entrante asignado a un nodo (B_{ei}) se obtendrá multiplicando el valor de U_e obtenido por el valor de ponderación entrante que corresponda a su zona (fórmula 3).

$$B_{ei} = U_e \cdot P_{ei}$$

Fórmula 3: Ancho de banda entrante mínimo por nodo

El ancho de banda mínimo saliente asignado a un nodo (B_{si}) se obtendrá multiplicando el valor de U_s obtenido por el valor de ponderación saliente que corresponda a su zona (fórmula 4):

$$B_{si} = U_s \cdot P_{si}$$

Fórmula 4: Ancho de banda saliente mínimo por nodo

El máximo ancho de banda entrante por nodo (B_{emax}) y el máximo ancho de banda saliente por nodo (B_{smax}) están fijados a los valores iniciales que aparecen en la tabla 11 *Anchos de banda máximos* del anexo II *Parámetros para la gestión del ancho de banda*. En el caso de los servidores, el ancho de banda máximo se determinará en cada caso.

Adicionalmente, se limitará el ancho de banda global asignado a determinados protocolos cuando estos puedan ser utilizados para provocar ataques de denegación de servicio con origen o destino en la red de la Universidad (como es el caso del ICMP).

Es labor de la Comisión de Tecnologías de la Información, Comunicaciones y Seguridad Informática la revisión periódica y el ajuste de los parámetros utilizados en las fórmulas de cálculo del ancho de banda, así como los anchos de banda máximos y mínimos (anexo II).

Acceso a recursos internos

Dentro de la red de la UCLM existirá una reserva de ancho de banda estricta para los siguientes servicios:

- Servicios de soporte básico de red: DNS, DHCP y NTP.
- Correo electrónico, tanto en los protocolos de envío como en los de consulta.
- Aplicaciones corporativas.

Tratamiento en situaciones de congestión

En caso de congestión de los enlaces de la red de la Universidad, el ancho de banda sobrante se prioriza siguiendo este orden:

1. Resto del tráfico interno.
2. Tráfico Internet de navegación.
3. Resto del tráfico Internet.

Capítulo IV. Política de uso de la red

Artículo 10. Condiciones de uso de la red.

Los principios que deben guiar la utilización de la red por parte de los miembros de la comunidad universitaria derivan tanto de la filosofía de utilización de las nuevas tecnologías de la UCLM como de los derechos y obligaciones adquiridos como integrantes de la red telemática española de I+D+I, RedIRIS [4].

Las pautas de conducta que marca esta política de uso deben ser conocidas y respetadas por cualquier persona que utilice la red de la Universidad, especialmente por aquellas que mantengan una relación contractual o académica con la UCLM.

1. Legalidad

La UCLM no estimulará ni aceptará prácticas ilegales. Se velará especialmente para proteger:

a) El orden público: para evitar que la red de la UCLM sea un vehículo de mensajes que inciten al uso de la violencia o a la participación en actividades delictivas.

b) La dignidad humana: para impedir cualquier clase de discriminación social, religiosa, étnica, cultural, política, sexual o por discapacidad física o psíquica.

c) La vida privada: para preservar los derechos y las libertades fundamentales, tutelando la vida privada, los datos personales y el secreto epistolar.

d) Los menores: para rechazar su utilización, especialmente con objetivos sexuales, y para mantener una actitud de cautela en la difusión de contenidos potencialmente nocivos para la infancia.

e) El consumidor: para respetar los principios de transparencia y accesibilidad, sometiéndose a las normativas de protección del consumidor.

2. Honradez

La UCLM utilizará correctamente los recursos públicos suministrados por RedIRIS, facilitando el acceso a su infraestructura de red al personal autorizado y denegándolo a personas u organizaciones ajenas a la institución.

Los usuarios de la UCLM utilizarán la infraestructura y los servicios de la red para las actividades académicas y de investigación, desarrollo e innovación tecnológica, incluyendo las tareas administrativas asociadas.

Los usuarios también deberán utilizar eficientemente la red, con el fin de evitar en la medida de lo posible, la congestión de la misma. En ningún caso se considera aceptable desarrollar actividades que persigan o tengan como consecuencia:

a) La creación o transmisión de material que perjudique la dinámica habitual de los usuarios de la UCLM o de RedIRIS.

b) La congestión de los enlaces de comunicaciones o sistemas informáticos.

c) La alteración de la infraestructura o de las condiciones de seguridad de la red.

d) La destrucción o modificación premeditada de la información de otros usuarios.

e) La violación de la privacidad e intimidad de otros usuarios.

f) El deterioro del trabajo de otros usuarios.

Tampoco deberán, bajo ningún concepto, usar la red de la UCLM para fines privados o personales, fines lúdicos y fines comerciales, ajenos a las actividades propias de la Universidad.

3. Confidencialidad

En su actividad ordinaria en la red, los usuarios tendrán derecho a preservar su anonimato. No obstante, la Universidad podrá establecer los mecanismos para poder identificar, en caso de incidente, los nodos o las personas que están actuando a través de la red.

4. Propiedad intelectual e industrial

Los usuarios de la UCLM deberán reconocer, respetar y defender el derecho de los autores a sus creaciones intelectuales e industriales, de acuerdo con la normativa vigente.

5. Responsabilidad

La UCLM se compromete a dar a conocer a sus usuarios los objetivos derivados de estos principios y a velar por el cumplimiento de los mismos.

Disposición final

Entrada en vigor

La presenta normativa entrará en vigor el día siguiente a su aprobación en Consejo de Gobierno, existiendo un plazo de dos años a partir de ese día para la adaptación de todos los sistemas existentes.

ANEXO I
PARÁMETROS PARA LA MEDICIÓN DE LA CONTINUIDAD DEL SERVICIO

A efectos de cálculo de la duración de las interrupciones de servicio, se establecerán dos jornadas: diurna y nocturna, computando el tiempo en jornada nocturna como la mitad que en la jornada diurna. La jornada diurna comprende los días laborables de 9 de la mañana a 9 de la noche. Se considera jornada nocturna el resto.

No se contabilizará como tiempo de avería el invertido en desplazamientos fuera de las capitales de provincia.

Se deberán tomar las medidas técnicas y organizativas necesarias para garantizar que estos indicadores no superan los valores límite, fijados inicialmente en:

a) 4 horas para una interrupción del servicio en la red troncal o en la red de distribución.

b) 8 horas para una interrupción del servicio en la red de acceso a los puestos.

c) 12 horas de tiempo acumulado de interrupción del servicio durante un trimestre en cada campus.

d) 24 horas de tiempo acumulado de interrupción del servicio durante un trimestre en cada centro.

Anexo II
Parámetros para la gestión del ancho de banda

Tabla 1: Ponderación de nodos por zonas

Zona del nodo	Ponderación tráfico entrante (P_e)	Ponderación tráfico saliente (P_s)
PDI	1	0.5
Lab. de Investigación	1	0.5
PAS	0.6	0.3
Alumnos	0.2	0.1
DMZ	A determinar por nodo	A determinar por nodo
Serv. Comunes	A determinar por nodo	A determinar por nodo

Tabla 21: Anchos de banda máximos

Variable	Valor
Máximo ancho de banda entrante por nodo (B_{emax})	10 Mbps
Máximo ancho de banda saliente por nodo (B_{smax})	5 Mbps

Anexo III
Referencias

1. Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.

2. Real decreto 994/1999, de 11 de Junio, por el que se aprueba el Reglamento de Medidas de Seguridad de ficheros automatizados que contengan datos de carácter personal.

3. Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

4. Documento de afiliación a RedIRIS,

   http://www.rediris.es/rediris/PERs/rediris_afiliacion.es.html