

MANUAL BÁSICO DE CONEXIÓN A LA RED WIRELESS DE UMH.

MANUAL DE CONFIGURACIÓN BÁSICA DE ACCESO A LA RED WIRELESS DE UMH

UNIVERSIDAD MIGUEL HERNÁNDEZ.



1	INT	PODUCCIÓN 2
1	1191	KODUCCION.
2	REI	DES WIFI DISPONIBLES4
3	QUI	IEN PUEDE ACCEDER A IUMH5
4	SOY	Y USUARIO DE UMHNET ¿CÓMO ME CONECTO?5
5	SOY	Y ESTUDIANTE DE LA UMH. ¿CÓMO ME CONECTO?5
6	SOY	Y VISITANTE DE UMH. ¿CÓMO ME CONECTO?6
7	REG	QUISITOS PARA LA CONEXIÓN
	7.1	INSTALACIÓN DE CERTIFICADOS RAIZ E INTERMEDIOS
	7.1.	1 certificados para iumhweb7
	7.1.2	2 CERTIFICADOS PARA IUMHNET Y EDUROAM
8	CO	NEXIÓN A LA RED IUMHNET
	8.1	CONEXIÓN DESDE WINDOWS XP
	8.2	CONEXIÓN DESDE WINDOWS 7
	8.3	CONEXIÓN DESDE IPHONE
9	CO	NEXIÓN IUMHWEB
	9.1	CONEXIÓN DESDE WINDOW XP
1	0 EDU	UROAM
	10.1	DESCRIPCIÓN DE LA RED EDUROAM
	10.2 LA INIC	CONEXIÓN A EDUROAM DESDE LA UMH PARA USUARIOS DE OTRAS INSTITUCIONES ADHERIDAS A CIATIVA
	10.3	CONEXIÓN AEDUROAM DE USUARIOS DE LA UMH QUE VISITAN OTRAS INSTITUCIONES52



1 INTRODUCCIÓN.

La red de comunicaciones de la Universidad Miguel Hernández es un recurso dinámico y en continua evolución y expansión de acuerdo a las necesidades de los usuarios, a los avances tecnológicos y a la disponibilidad presupuestaria.

De acuerdo a este principio y debido a la creciente demanda de servicios de red en zonas de uso común, la UMH dispone de una red inalámbrica, llamada **lumhnet** concebida inicialmente como método de conexión alternativo a las conexiones tradicionales por cable. De esta forma se pretende cubrir las necesidades de los usuarios que requieren conexiones puntuales de manera dinámica y flexible.

La cobertura pues, es total en las zonas propias de este tipo de demanda, es decir, zonas de uso común o de permanencia temporal como son, bibliotecas, salas de reuniones, salones de actos, recibidores o distribuidores amplios, salas de lectura, o estudio, cafeterías, etc.

Así pues, la red inalámbrica de la UMH se concibe como un método alternativo de conexión a la red general de comunicaciones, no sustituye al método tradicional de acceso a través de cableado para puestos de trabajo permanentes, sino que lo complementa aportando a determinado tipo de usuarios movilidad en el acceso a los servicios de red.

Técnicamente, la **lumhnet** se basa en el estándar 802.11b/g/n para redes inalámbricas.El estándar 802.11g y el 802.11b se basa en la comunicación entre dispositivos utilizando la banda radiofrecuencia no licenciada de 2.4 GHz. La aplicación del estándar aporta a nuestra red las máximas garantías de seguridad, accesibilidad e interoperabilidad en cuanto a redes inalámbricas.





2 REDES WIFI DISPONIBLES.

La tecnología utilizada en los puntos de acceso es la del fabricante Aruba, modelo OmniAccess AP61 y AP105 gestionados mediante un controlador OmniAccess 6000 del mismo fabricante. Estos equipos cumplen con la normativa europea de limitación de potencia en emisiones radioeléctricas y al mismo tiempo cumplen con los estándares de seguridad requeridos por la UMH.

La red inalámbrica, es decir, puntos de acceso y controladores, son instalados, configurados y gestionados por los Servicios Informáticos de la Universidad como una parte más de la red de comunicaciones de la UMH.

Actualmente existen tres redes inalámbricas disponibles dentro de la Universidad Miguel Hernández: **lumhnet, lumhweb y eduroam**

lumhnet. Tiene las siguientes características:

- Encriptación WPA/TKIP
- Validación : PEAP/MS-CHAP2
- Estándares soportados: 802.11b y 802.11g
- SSID: lumhnet

lumhweb. Tiene las siguientes características:

- Encriptación: NO
- Validación: Portal Captivo
- Estándares soportados: 802.11b y 802.11g.
- SSID: lumhweb

eduroam. Tiene las siguientes características:

- Encriptación WPA/TKIP
- Validación : (Según la Institución de origen del usuario)
- Estándares soportados: 802.11b y 802.11g
- SSID: eduroam

La universidad Miguel Hernández recomienda que se utilice siempre el SSID "lumhnet" por sus mejores características en cuanto a seguridad en envío y recepción de información.



3 QUIEN PUEDE ACCEDER A IUMH

La red inalámbrica de la UMH está proyectada para dar servicio a todos los usuarios habituales de la red de comunicaciones de la UMH, los cuales podrán acceder utilizando su DNI@umh.es / PIN, en caso de estudiantes, o su usuario/password para los usuarios del dominio. El acceso diseñado para tal fin es el llamado *lumhnet* cada uno en su perfil correspondiente "estudiante UMH" o "usuarios de lumhnet"

Pero también se pretende dar servicio a todas aquellas personas que se desplazan a la UMH para desarrollar puntualmente alguna actividad, como por ejemplo, asistencia a reuniones, congresos, seminarios, etc. y requieren el servicio de conexión a Internet. El acceso diseñado para tal fin es el llamado *lumhnet* en el perfil *visitante.*

4 SOY USUARIO DE UMHNET ¿CÓMO ME CONECTO?

Si usted es usuario habitual de la red de comunicaciones de la UMH, siga los siguientes pasos:

Asegúrese de tener instalados los certificados raíz e intermedios adecuados.

Asegúrese de tener configurado el suplicante para establecer la conexión.

- 1. Seleccione la red **lumhnet**
- 2. Introduzca su usuario/password del dominio umhnet en la ventana de identificación.

Se debe establecer una conexión inalámbrica idéntica a la que realiza cuando inicia sesión en la red cableada umhnet, es decir, usted dispone de mismos servicios, unidades de red, soporte remoto, antivirus, etc. manera idéntica a la de la red cableada. El acceso es identificado y las comunicaciones son encriptadas.

Si sólo desea navegar (http o https) y no le importa que la información vaya en abierto puede seleccionar la red **lumhweb.**

La universidad Miguel Hernández recomienda que se utilice siempre el SSID "lumhnet " por sus mejores características en cuanto a seguridad en envío y recepción de información

5 SOY ESTUDIANTE DE LA UMH. ¿CÓMO ME CONECTO?

Si eres estudiante de la UMH sigue los siguientes pasos:

Asegúrese de tener instalados los certificados raíz e intermedios adecuados.

Asegúrate de tener <u>configurado el suplicante</u> para establecer una **conexión segura**.



- 1. Seleccione la red **lumhnet**
- 2. Introduce DNI@umh.es / PIN en la ventana de identificación.

Se debe establecer una conexión inalámbrica que te permite tener acceso http, ftp, chat y correo. El acceso es identificado y las comunicaciones son encriptadas.

Si sólo quieres navegar(http o https) y no te importa que la información vaya en abierto puedes seleccionar la red **lumhweb.**

La universidad Miguel Hernández recomienda que se utilice siempre el SSID "lumhnet " por sus mejores características en cuanto a seguridad en envío y recepción de información

6 SOY VISITANTE DE UMH. ¿CÓMO ME CONECTO?

Si su organización de origen dispone de la red <u>eduroam</u>, puede utilizar dicha red en la UMH para la conexión, usando las credenciales de su organización.

Si su organización no dispone de **eduroam**, puede conectarse a **lumhnet**, obteniendo en primer lugar una clave de acceso.

¿Cómo obtengo la clave de acceso?.

Para obtener dicha clave puede optar por dos posibilidades:

 1.- Envio de SMS. Si su operador de telefonía móvil es Movistar debe enviar un SMS al 215401, para otros operadores, envíe el SMS al 669 385 000 con el mensaje "iumh". Al cabo de unos instantes recibirá en su móvil un mensaje de la universidad con una clave de acceso.

2.- **Registro mediante formulario.** Siga el procedimiento de <u>Conexión</u> <u>lumhweb</u> para que el sistema le envíe un SMS automáticamente a su terminal móvil.

La clave obtenida por cualquiera de las dos opciones únicamente tiene una validez de 7 dias a partir del momento de recepción de la misma.

Asegúrese de tener instalados los certificados raíz e intermedios adecuados.

Asegúrate de tener <u>configurado el suplicante</u> para establecer una **conexión segura**.

- 1. Seleccione la red **lumhnet**
- Introduzca su número de teléfono seguido de @umh.es como usuario y la clave de acceso obtenida en la ventana de identificación. Por ejemplo, Usuario: 666999444@umh.es



Se debe establecer una conexión inalámbrica que te permite tener acceso http, ftp, chat, correo y vpn. El acceso es identificado y las comunicaciones son encriptadas.

Si sólo desea navegar (http o https) y no le importa que la información vaya en abierto puede seleccionar la red **lumhweb una vez obtenida la clave de acceso.**

La universidad Miguel Hernández recomienda que se utilice siempre el SSID "lumhnet " por sus mejores características en cuanto a seguridad en envío y recepción de información

7 REQUISITOS PARA LA CONEXIÓN.

Para conectarse a la red lumhnet será necesario disponer de:

Equipo con tarjeta inalámbrica que soporte 802.11b o 802.11g.

La tarjeta inalámbrica de dicho equipo debe ser certificada WPA.

Se puede ver información sobre la compatibilidad WPA de tarjetas en el enlace: http://www.wi-fi.org/

Para la conexión a la red **lumhweb** solamente es necesario disponer de un equipo con tarjeta inalámbrica soportando 802.11b o 802.11g.

7.1 INSTALACIÓN DE CERTIFICADOS RAIZ E INTERMEDIOS.

7.1.1 CERTIFICADOS PARA IUMHWEB

La red lumhweb utiliza para la autenticación de usuarios un certificado digital emitido por TERENA SSL CA, siendo la cadena total de certificación:

AddTrustExternalCARoot->UTN-USERFirst-Hardware->TERENA SSL CA.

Por tanto, para que nuestra autenticación sobre el sistema sea segura, deberemos instalar dicha cadena de certificación en el navegador que usemos para conectarnos a Internet, en el caso de Internet Explorer se deberá seguir el siguiente procedimiento:

Paso 0. Descargarse los certificados raíz e intermedios.

AddTrustExternalCARoot

UTN-USERFirst-Hardware

TERENA SSL CA



Paso 1. Seleccionamos Opciones de Internet.

Color	Progra	Programas Opcior			
General	Seguridad	Priva	cidad	Contenido	
ágina principal Para una lí	crear pestañas de p nea independiente. p://go.microsoft.co	ágina principa m/fwlink/?Lir	al, escriba c hkīd=6915	ada dirección en	
-				-	
Usar ac	tual Usar pr	edeterminada	usar p	agina en <u>b</u> lanco	
istorial de expl	pración				
	e archivos temporale ladas e información	es, historial, o de formulario	cookies, cor s web.	ntraseñas	
úsqueda —	e archivos temporale ladas e información minar el historial de <u>E</u>	es, historial, d de formulario exploración a liminar	cookies, cor s web. I salir	ntraseñas onfiguración	
úsqueda — Camb prede	e archivos temporale ladas e información minar el historial de <u>E</u> ie las opciones terminadas de búsq	es, historial, d de formulario exploración a iminar ueda.	cookies, cor s web. I salir	ntraseñas onfiguración onfiguración	
úsqueda — Camb prede estañas — Camb web s	e archivos temporale ladas e información minar el historial de <u>E</u> ie las opciones eterminadas de búsq ie la forma en que la se muestran en las p	es, historial, d de formulario exploración a iminar ueda. ueda. as páginas estañas.	cookies, cor s web. I salir Cc	ntraseñas onfiguración onfigu <u>r</u> ación	
éstañas — Camb prede estañas — Camb prede camb web s	e archivos temporal ladas e información minar el historial de El ie las opciones eterminadas de búsq ie la forma en que la se muestran en las p	es, historial, d de formulario exploración a iminar ueda. ueda. as páginas estañas.	cookies, cor s web. I salir Co	ntraseñas onfiguración onfigu <u>r</u> ación	
Limin guard úsqueda — Camb prede estañas — Camb web s pariencia — Colores	e archivos temporale ladas e información minar el historial de El ie las opciones eterminadas de búsq ie la forma en que la se muestran en las p	es, historial, de formulario de formulario exploración a liminar ueda. ueda. as páginas estañas.	tes	ntraseñas onfiguración onfiguración onfiguración	

Paso 2. Seleccionamos la Opción de Contenido+ Certificados.

	:			
Conexiones	Programa	s	Opciones	avanzadas
General	Seguridad	Privacida	be	Contenido
ertificados Use ce identif	rtificados para las con cación.	exiones cifrad	das y para f	fines de
Borrar	estado SSL	rtificados	E	ditores
utocompletar -				
Autoco página lo que coincio	ompletar almacena lo e s web para intentar ar escribe y sugerir posib encias.	scrito en nticiparse a oles	Con	figuración
uentes y Web Sli	ces		225	
Las fue propor	entes y las Web Slices cionan contenido actu veb, el cual puede leer et Explorer y en otros	alizado de se en programas.	Con	figuración

Paso 3. Seleccionamos "Entidades de certificación Intermedias"



Paso 4. Seleccionamos "Importar"

Deberemos seleccionar primero el fichero UTN-USERFirst-Hardware.crt y terminar la importación, luego deberemos de repetir los mismos pasos para el fichero TERENA SSL CA.crt.

IOS INFORMÁTICOS	
	Miguel Hernández
Asistente para importación de certificados	
Archivo para importar	
Especifique el archivo que desea importar.	
Nombre de archivo:	
C:\Users\umh\Desktop\UTN-USERFirst-Hardware.crt	aminar
Nota: se puede almacenar más de un certificado en un mismo archivo en los sig formatos: Intercambio de información personal: PKCS #12 (.PFX,.P12) Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7	rB)
Almacén de certificados en serie de Microsoft (.SST)	
Más información acerca de los <u>formatos de archivo de certificado</u>	
< <u>A</u> trás Siguien <u>t</u> e >	Cancelar

Paso 5. Seleccionamos "Entidades de certificación raíz de confianza"



Paso 6. Instalación certificado raíz de la cadena.

Siguiendo los pasos anteriores deberemos finalmente seleccionar el archivo AddTrustExternalCARoot.crt, que es el raíz de la cadena de certificados.

Asi

5 INFORMATICOS	
	VERS
	s (LA)ja
	Miguel Hernánd
tente para importación de certificados	x
Archivo para importar	
Especifique el archivo que desea importar.	
Nombre de archivo:	
C:\Users\umh\Desktop\AddTrustExternalCARoot.crt	Examinar
Vota: se puede almacenar más de un certificado en un mismo archivo en los formatos: Intercambio de información personal: PKCS #12 (.PFX,.P12) Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (siguientes (.P <i>7</i> B)
Almacén de certificados en serie de Microsoft (.SST)	
Más información acerca de los <u>formatos de archivo de certificado</u>	
< <u>A</u> trás Siguien <u>t</u> e	> Cancelar

S III III

7.1.2 CERTIFICADOS PARA IUMHNET Y EDUROAM.

La red lumhnet y eduroam utilizan para la autenticación de usuarios un certificado digital emitido por TERENA SSL CA, siendo la cadena total de certificación:

AddTrustExternalCARoot->UTN-USERFirst-Hardware->TERENA SSL CA.

Por tanto, para que nuestra autenticación sobre el sistema sea segura, deberemos instalar dicha cadena de certificación en el repositorio de certificados de nuestro equipo, en el caso de Windows 7 se procedería de la siguiente forma:

Paso 0. Descargarse los certificados raíz e intermedios.

AddTrustExternalCARoot

UTN-USERFirst-Hardware

TERENA SSL CA

Paso 1. Abrimos el gestor de certificados de Windows 7.



Vamos a Inicio->ejecutar y ponemos mmc



Paso 2. Agregamos el complemento de certificados.

Dentro del gestor mmc, seleccionamos Archivo->Agregar o quitar complementos.



_	-			País de concela	
Complemento	Proveedor	Â		Raiz de consola	Editar extensiones
Administración de di	Microsoft and				Ouitar
Administración de e	Microsoft Cor				
Administración de im	Microsoft Cor	111			
Administración de TPM	Microsoft Cor				Subir
Administrador de au	Microsoft Cor		Peire		
Administrador de dis	Microsoft Cor		Agregar >		
🚽 Administrador de las	Microsoft Cor		(ngi Egui >		
Carpeta	Microsoft Cor				
🖞 Carpetas compartidas	Microsoft Cor				
Certificados	Microsoft Cor				
Configuración del cli	Microsoft Cor				
Configuración y anál	Microsoft Cor				-
🕻 Conjunto resultante	Microsoft Cor	-			Opciones avanzadas.
Y =		-			
scripción:					
complemento Certificados	nermite evaminar	r el c	ontenido de los	almacanas da cartificados, un se	ervicio o un equino

Seleccionamos "Certificados" y agregamos. Nos pregunta sobre qué cuenta queremos actuar, dejamos "Mi cuenta de usuario"



Paso 3. Importar el certificado Raiz.

Seleccionamos "entidades de certificación raíz de confianza" ->"Certificados" y con el botón derecho del ratón "Todas las tareas"->"Importar"

Consola1 - [Raíz de co Archivo Acción	RMATICOS onsola\Certificados: usuario actu Ver Favoritos Ventana Ay	al\Entidades (uda	de certificación raíz de con	fianza\Certificados]	Miguel	Л Не	rnández
🔿 🔁 📅 📋	🖬 🔝 🛃						
Raíz de consola		Emitido p	ara	Emitido por	Fecha de expir		Acciones
 Certificados: usua Personal Entidades de o Certific 	rtificados: usuario actual Personal Entidades de certificación raíz de confianza	AddTrust External CA Root Autoridad Certificadora UMH	AddTrust External CA Root Autoridad Certificadora UMH Autoridad Certificadora UMH	30/05/2020 04/02/2016 19/09/2011		Certificados	
Confianza	Todas las tareas	+	Importar	Autoridad Certificadora UMH	04/02/2016		
 Entidades Objeto de Editores de 	Ver Nueva ventana desde aquí	•	ublic Primary Certificat ublic Primary Certificat	Certum CA Class 3 Public Primary Certificatio Class 3 Public Primary Certificatio	11/06/2027 02/08/2028 08/01/2004		
Certificado Entidades	Nueva vista del cuadro de tar	Nueva vista del cuadro de tareas t (c) 1997 Microsoft C Copyright (c) 1997 Microso ecure Certificate Auth Equifax Secure Certificate A	Copyright (c) 1997 Microsoft Corp. Equifax Secure Certificate Authority	rp. 31/12/1999 ity 22/08/2018	ш		
Personas d	Actualizar erTrust Global Root GTE CyberTrust Global	GTE CyberTrust Global Root	14/08/2018				
Solicitudes	Exportar lista		vw.valicert.com/	http://www.valicert.com/	26/06/2019		
Raíces de c	Ayuda		t Authenticode(tm) Ro t Root Authority	Microsoft Authenticode(tm) Root Microsoft Root Authority	01/01/2000 31/12/2020		
		Micros	oft Root Certificate Auth	Microsoft Root Certificate Authori	10/05/2021		
		NO LIA	BILITY ACCEPTED, (c)97	NO LIABILITY ACCEPTED, (c)97 V	08/01/2004		
		Thawte	Premium Server CA	Thawte Premium Server CA	02/01/2021		
		Thawte	Premium Server CA	Thawte Premium Server CA	01/01/2021		
		Thawte	e Premium Server CA	Thawte Premium Server CA	01/01/2021		
		Thawte	Timestamping CA	Thawte Timestamping CA	01/01/2021		
		UTN-U	SERFirst-Hardware	AddTrust External CA Root	30/05/2020		
		LITN-H	SERFirst-Hardware	11TN-11SERFirst-Hardware	09/07/2019	-	

Servicios Informáticos

A continuación se nos preguntará por el archivo del certificado, deberemos seleccionar "AddTrustExternalCARoot.crt "

Especifique el arc	hivo que desea importar.
N <u>o</u> mbre de archiv	o:
	Examinar
Estándar de s Almacén de ce	ntaxis de cifrado de mensajes: certificados PKCS #7 (.P7B) rtificados en serie de Microsoft (.SST)

ERSITA

Paso 4. Importar el certificado Intermedio.

Se seguirán los mismos pasos anteriores pero seleccionando la opción "Entidades de certificación Intermedias" e importando los ficheros "UTN-USERFirst-Hardware.crt " y "TERENA SSL CA.crt"



Consola1 - [Raíz de	e consola\Certificados: usuario actua	al\Entidades	de certificación intermedia	s\Certificados]		
🖕 🔿 🖄 📰 🗄		uua				- 0 4
 Raíz de consola Certificados: u Personal Entidades Certific Confianza Entidades Lista de 	isuario actual de certificación raíz de confianza cados empresarial de certificación intermedias revocación de certificados	Emitido para Autoridad Certificadora UMH Microsoft Windows Hardware Root Agency TERENA SSL CA UTN-USERFirst-Hardware www.verisign.com/CPS Incorp		Emitido por Autoridad Certificadora UMH Microsoft Root Authority Root Agency UTN-USERFirst-Hardware AddTrust External CA Root Class 3 Public Primary Certificatio	Fecha de expir F 04/02/2016 31/12/2002 F 01/01/2040 30/05/2020 30/05/2020 25/10/2016 25/10/2016 2	F Acciones Certificados V
 Cerving Objeto Objeto Certific Certific Entidac Person Solicitu Raíces 	Todas las tareas Ver Nueva ventana desde aquí Nueva vista del cuadro de tareas. Actualizar Exportar lista Ayuda		Importar			
Agregar un certificado	en el almacén					

8 CONEXIÓN A LA RED IUMHNET.

8.1 CONEXIÓN DESDE WINDOWS XP.

Paso 1.- Comprobar si nuestro equipo Windows XP está actualizado para soportar WPA. Para ello deberemos comprobar la versión de Service Pack que tenemos instalada (botón derecho del ratón en el icono "MI PC", y seleccionar "PROPIEDADES" del menú desplegable).

• Si tenemos Windows XP SP1. Necesitamos tener instalada la "REVISIÓN DE WINDOWS XP PARA OBTENER COMPATIBILIDAD CON WPA". Para comprobar si está instalada ir a:

"Inicio" -> "Panel de Control" -> "Agregar o quitar programas"

Tiene que existir un programa instalado con nombre "REVISIÓN DE WINDOWS XP – KB826942". En caso de no tenerla instalada, la podeis obtener <u>en este enlace</u>.

• Windows XP SP2 . El equipo está listo para conectarse.



Paso 2.- Debemos seleccionar las conexión de red inalámbrica mediante "Inicio -> Panel de Control -> Conexiones de red.

Seleccionamos la conexión de red Inalmbrica y con el botón derecho del ratón pulsar "Propiedades"



Paso 3.- Debemos configurar los parámetros TCP/IP dentro de la pestaña general de las conexiones de red, marcando las opciones de "Obtener Dirección IP Automáticamente" y "Obtener DNS Automático".



onectar usanc	lo:				
B ASUS U	6B Wireless	Network Adapte	Conf	igurar	
sta conexión u	utiliza los sig	uientes elemento	is:		
Progra Progra FAEGIS Protoc	mador de pa Protocol (IE olo Internet	aquetes QoS EEE 802.1x) v2.3 (TCP/IP)	3.1.9		
٢	141				
Instalar		Desinstalar	Propie	edades	
Descripción					
Protocolo TC predetermina redes conec	:P/IP. El pro do que pern tadas entre	itocolo de red de nite la comunicad sí.	área extens; ción entre va	a rias	
Mostraricon Notificarme	o en el área cuando esta	a de notificación a conexión tenga	al conectarse conectividad	: d limitada o	

Рго

ORMÁTICOS	IIVERSITAS
	5 Miguel Hernán
ropiedades de Protocolo Interne	et (TCP/IP)
General Configuración alternativa	
Puede hacer que la configuración IP se red es compatible con este recurso. De con el administrador de la red cuál es la	e asigne automáticamente si su lo contrario, necesita consultar a configuración IP apropiada.
 Ubtener una dirección IP automát 	icamente
O Usar la siguiente dirección IP: —	
Dirección IP:	
Máscara de subred:	
Puerta de enlace predeterminada:	
Obtener la dirección del servidor E	DNS automáticamente
O Usar las siguientes direcciones de	servidor DNS:
Servidor DNS preferido:	
Servidor DNS alternativo:	
	Opciones avanzadas
	Aceptar Cancelar

Paso 4.- En estos momentos debemos configurar las redes inalámbricas, para ello pulsamos la pestaña "Redes Inalámbricas" de la ventana "Propiedades de Conexiones de Red Inalámbricas", marcamos la opción "Usar Windows para establecer mi configuración de red inalámbrica" y pulsaremos la opción "Ágregar"

G

RMÁTICOS				ITAS
				UNIVERS
Propiedades de Conex	iones de rec	l inalámbr	icas 🚺	Miguel Hernár ? 🔀
eneral Redes inalámbricas	Opciones ava	anzadas		
🛛 Usar Windows para estab	lecer mi configu	uración de rec	l inalámbrica	
Redes disponibles:				
Haga clic en el siguiente bo redes inalámbricas o para o	otón para cone obtener más info	ctarse o desc ormación acer	onectarse de ca de ellas.	
		Ver rede	es inalámbricas	
Redes preferidas:				
Conectar automáticamente	a redes dispon	ibles en el oro	len siguiente:	
24			Subir	
			Bajar	
Agregar Quita	r Propie	dades		
Obtener más información ac	erca de cómo	brica Opci	ones avanzada	as
establecer una coninquiació	n de reu indidit			
		Acenta	r Can	celar

ez

Paso 5.- En la siguiente ventana, bajo la pestaña de "Asociación" debemos introducir el nombre SSID: **lumhnet** y selección **WPA** como "Autenticación de red" y **TKIP** como "Cifrado de datos".

En caso de que la opción WPA no esté disponible puede ser porque su tarjeta inalámbrica no sea compatible WPA o si lo es, necesite actualizar los drivers de la misma.



undiendo
undiendo
ite:
amente
ioc). No se utilizan

Paso 6.- Bajo la pestaña de "Autenticación", se debe Habilitar la autenticación IEEE 802.1X y debemos escoger como "Tipo de EAP" **: PEAP**



sociacion	Autenticación	Conexión
Seleccion redes Ethe	e esta opción pa ernet inalámbrica:	ra proporcionar acceso autenticado a s.
🕑 Habilita	ar la autenticació	n IEEE 802.1X en esta red
Tipo de EAP:	EAP protegido	(PEAP)
Autenti disponi	car como equipo ble car como invitad no estén dispon	o cuando la información de equipo esté o cuando el usuario o la información de ibles

Paso 7.- Ahora se debe configurar la autenticación PEAP, para ello pulsamos sobre el botón "Propiedades". En la pantalla siguiente deberemos seleccionar la opción "Validar un certificado del servidor" y escogeremos como "Metodo de autenticación" **EAP-MSCHAPv2.**



Paso 8.- Ahora pasaremos a configurar la forma en que se pedirá usuario y contraseña para MSCHAPv2, para ello debemos pulsar el botón **Configurar** en la pantalla "Propiedades de EAP Protegido", aparecerá otra ventana donde solamente deberemos deseleccionar la opción "**Usar el nombre de inicio de sesión y la contraseña de Windows** " puesto que podemos usar credenciales diferentes.

Propieda	des de EAP M	SCHAPv2	×
Al conect	ar:		
Usa sesi exis	r automáticament ón y la contraseñ: te alguno).	e el nombre de inicio a de Windows (y do	o de minio, si
	Aceptar	Cancelar	



Paso 9.- Finalizados estos pasos, debemos seleccionar la red lumhnet y pulsamos conectar.



Paso 10.- Nos aparecerá en la barra de tareas un mensaje invitándonos proporcionar las credenciales, hemos de pulsar y nos aparece la pantalla siguiente invitándonos a introducir nuestras credenciales.



Escribir creder	iciales 🛛 🕅	U
Nombre de usuario: Contraseña: Dominio de inicio de sesión:		
	Aceptar Cancelar	

En esta pantalla se deben introducir nuestras credenciales según nuestro perfil:

- **PAS y PDI:** Deberán introducir su usuario de dominio, password y el nombre del dominio.
- Alumnos: Deberán introducir como usuario su DNI@umh.es, el password es el PIN que tienen asignado y deberán dejar el domino en blanco.
- Personal Visitante: Deberán introducir como usuario su nº de Teléfono@umh.es, como password el código de 13 caracteres que habrán recibido por SMS y dejar el domino en blanco.

Una vez introducidas nuestras credenciales, habremos conectado a la red wireless con el perfil adecuado de seguridad.

8.2 CONEXIÓN DESDE WINDOWS 7.



Paso 1.- Debemos ir a Panel de Control -> Redes e Internet -> Centro de redes y recursos compartidos -> Administrar Redes Inalámbricas.

🚱 🔵 🗢 📶 🕨 Panel de control 🕨 R	Redes e Internet 🕨 Administrar redes inalámbricas	👻 😽 Buscar Administrar redes inalámbricas 👂
Administrar redes inalámbri	icas que usen (Conexión de red inalámbrica)	
Windows intenta conectarse a estas r	redes en el orden que aparece a continuación.	
Agregar Propiedades del adaptador	Tipos de perfil Centro de redes y recursos compartidos	0
0 elementos		

Paso 3.- Debemos Agregar un nuevo perfil de conexión seleccionando la opción de configuración manual e introduciendo los siguientes parámetros:

Nombre de la red:	lumhnet
Tipo de seguridad:	WPA-Enterprise
Tipo de cifrado:	TKIP

Escriba la informac	ión de la red inalámbrica que dese	a agregar.
Nombre de la red:	Iumhnet	
Tipo de segu <u>r</u> idad:	WPA-Enterprise 👻	
Tipo <u>d</u> e cifrado:	TKIP	
<u>C</u> lave de seguridad:		Ocultar caracteres
niciar esta conexi	ón automáticamente	
Con <u>e</u> ctarse aunqu	e la red no difunda su nombre	del en la c

NIVERSITAS

Seleccionamos Siguiente y finalizamos la configuración del perfil.

Paso 4.- Debemos verificar en estos momentos la configuración de seguridad del perfil lumhnet creado, para ello hacemos "Doble Click" en el perfil y nos aparecen sus propiedades, seleccionamos la pestaña de "Seguridad" y debemos comprobar los siguientes datos:

Tipo de Seguridad:	WPA-Enterprise
Tipo de cifrado:	ТКІР
Autenticación:	PEAP
Recordar mis creder	ciales: Deshabilitado.



onexión Seguridad		
Tipo de <u>s</u> eguridad:	WPA-Enterprise	•
<u>T</u> ipo de cifrado:	TKIP	•
Microsoft: EAP protegi	ido (PEAP)	Configuración
Recordar mis creder vez que inicie sesiór	nciales para esta cone: n	kión cada
Recordar mis crede vez que inicie sesiór	nciales para esta cone: n	xión cada
Configuración avan;	nciales para esta cone: n <u>z</u> ada	ción cada
Configuración avan;	nciales para esta cone: n <u>z</u> ada	ción cada

Paso 5.- Debemos cerciorarmos que hemos utilizado como "Método de Autenticación de red" la opción "PEAP", y seleccionando "Configuración" nos aparecerá la siguiente ventana:

picasacs ac i	AP protegido		1	
l conectar:				
Validar un c	ertificado de serv	/idor		
Conectars	e a estos servidor	res:		
acs.umh	.es			
Entidades de	certificación raíz c	de confianza:		
AddTrust	External CA Root	t		
Autoridad	Certificadora UM	1H		-
Autoridad	Certificadora UM	1H		-
Certum C	A			
Class 3 Pu	ublic Primary Certi	ification Authority		
Equifax S	ecure Certificate	Authority		
GTE Cybe	rTrust Global Roc	ot		-
1	11	11	•	
servidores	o entidades de co todo de <u>a</u> utentica	ertificación de confia ación:	anza.	
Contrasena seg		F V2)		rar.
Habilitar reco	nexión rápida			
There in contracts	rción de acceso a	redes		
Aplicar Prote	LUOIT DE ALLESU A			
Aplicar Prote	si servidor no pre	senta TLV con enlac	e de cifrado	
Aplicar Prote	si servidor no pre acidad	esenta <u>T</u> LV con enlac	e de cifrado	

AS

Debemos seleccionar la opción "Validar un certificado de servidor" y confiar en la CA Raiz "GTE CyberTrust Global Root" que habremos instalado previamente en caso de no estar ya instalada.

Por último en la configuración de EAP-MSCHAP v2 debemos asegurarnos de deseleccionar la opción "Usar automáticamente el nombre de inicio de sesión y contraseña de Windows".



Al conectar: Usar <u>a</u> utomáticamente el nombre de inicio de sesión y la contraseña de Windows (y dominio, s existe alguno).	Al conectar: Usar <u>a</u> utomáticamente el nombre de inicio de sesión y la contraseña de Windows (y dominio, s existe alguno).		
Usar <u>a</u> utomáticamente el nombre de inicio de essión y la contraseña de Windows (y dominio, s existe alguno).	Usar automáticamente el nombre de inicio de Essión y la contraseña de Windows (y dominio, s existe alguno).	Al conecta	r:
 sesión y la contraseña de Windows (y dominio, s existe alguno). 	sesión y la contraseña de Windows (y dominio, s existe alguno).	Üsar	automáticamente el nombre de inicio de
existe alguno).	existe alguno).	:030	automaticamente er tombre de micro de
		sesió	n y la contraseña de Windows (y dominio,
		existe	n y la contraseña de Windows (y dominio, alguno).

Paso 9.- Configuración de las propiedades de red.

En la pantalla de administración de redes inalámbricas, seleccionamos el Perfil "Iumhnet" creado previamente y vamos a "Propiedades del adaptador".

	Uso compartido
Conectar usand	o:
Conexión	de red Intel(R) PRO/Wireless 3945ABG
	Configurer
Esta conexión u	isa los siguientes elementos:
Cliente	nam melan Minmant
	para reces Microsoft mader de paquetes OoS
	itir impresoras y archivos para redes Microsoft
Protoci	olo de Internet versión 6 (TCP/IPv6)
Protoc	olo de Internet versión 4 (TCP/IPv4)
🗹 🔺 Control	ador de E/S del asignador de detección de topol
🗹 🔺 Respon	ndedor de detección de topologías de nivel de v
Inst <u>a</u> lar	Desinstalar Propiedades
Inst <u>a</u> lar Descripción	Desinstalar Desinstalar
Inst <u>a</u> lar Descripción Protocolo TC	P/IP. El protocolo de red de área extensa
Inst <u>a</u> lar Descripción Protocolo TC predetermina	Desinstalar Propiedades P/IP. El protocolo de red de área extensa do que permite la comunicación entre varias
Inst <u>a</u> lar Descripción Protocolo TC predeterminar redes conect	Desinstalar Propiedades P/IP. El protocolo de red de área extensa do que permite la comunicación entre varias adas entre sí.



Seleccionamos "Protocolo de Internet versión 4 (TCP/IPv4)" y vamos a "Propiedades",

eneral	Configuración alternativa				
Puede l red es consult apropia	hacer que la configuración IP se a: compatible con esta funcionalidad. ar con el administrador de red cuá ida.	signe autor . De lo contr il es la confi	iáticar ario, i guraci	nente si la deberá ón IP	
0	otener una dirección IP automática	amente			
	sar la siguiente dirección IP:				
Direc	ción IP:				
Máso	cara de subred:				
Puer	ta de enlace predeterminada:	-	-34	4	
() ()	<u>b</u> tener la <mark>d</mark> irección del servidor DN	IS automátic	amen	te	
O Us	sar las <u>s</u> iguientes direcciones de se	ervidor DNS	. —		
Serv	idor DNS preferido:			,	
Serv	idor DNS al <u>t</u> ernativo;			+	
V	alidar configuración al salir	Opc	iones	avan <u>z</u> adas	i

Deberemos comprobar que tenemos habilitado:

"Obtener una dirección ip automáticamente"

"Obtener la dirección del servidor DNS automáticamente"

Paso 10.- Conexión a la red lumhnet.

Seleccionando la red lumhnet y pulsando sobre "Conectar" nos aparecerá la pantalla de introducción de credenciales para poder acceder a la red.

Informátic	OS		
Seguridad de Wi	ndows	-	Miguel Hernández
Autenticac Escriba sus cre	ión de red edenciales de usuario		
	Nombre de usuario		
	Contraseña		
		Aceptar	Cancelar

En esta pantalla se deben introducir nuestras credenciales según nuestro perfil:

- PAS y PDI: Deberán introducir su usuario de dominio y password.
- Alumnos: Deberán introducir como usuario su DNI@umh.es, el password es el PIN que tienen asignado y deberán dejar el domino en blanco.
- Personal Visitante: Deberán introducir como usuario su nº de Teléfono@umh.es, como password el código de 13 caracteres que habrán recibido por SMS y dejar el domino en blanco.

Una vez introducidas nuestras credenciales, habremos conectado a la red wireless con el perfil adecuado de seguridad.

8.3 CONEXIÓN DESDE IPHONE

Paso 1.- Debemos seleccionar Ajustes y Wifi.

Nos aparecerá una pantalla como la siguiente:



movistar 3G 11:19	♀ 券 📼
Ajustes Redes Wi-Fi	
Wi-Fi	
Seleccione una red	314
eduroam	₽ 🗢 🕥
lumhnet	₽ 🗢 🕥
iumhnetpru	₽ 🗢 🕥
lumhweb	? ()
SpeedTouchF89	Ş ()
WLAN_11	₽\$ 📎
Otra	>

Paso 2.- Seleccionamos la red lumhnet.

Nos aparecerá la pantalla siguiente para introducir las credenciales:



movistar	3G 10:39	• * 🖚
Introdu	zca la contraseña de	e "lumhnet"
Cancelar	Contraseña	Conectarse
Nombre	de usuario	
Contras	eña	
QWE	RTYL	JIOP
AS	DFGH	JKL
	XCVB	N M 💌
.?123	espacio	intro

Paso 3.- Introducción de credenciales.

En esta pantalla introducimos nuestras credenciales y pulsamos sobre "Conectarse".

A continuación nos aparecerá el certificado de nuestro radius





Pulsamos sobre "Aceptar" y nuestra conexión wifi estará lista.

9 CONEXIÓN IUMHWEB

9.1 CONEXIÓN DESDE WINDOW XP.

Paso 1.- Debemos seleccionar las conexión de red inalámbrica mediante "Inicio -> Panel de Control -> Conexiones de red.

Seleccionamos la conexión de red Inalmbrica y con el botón derecho del ratón pulsar "Propiedades"



Paso 2.- Debemos configurar los parámetros TCP/IP dentro de la pestaña general de las conexiones de red, marcando las opciones de "Obtener Dirección IP Automáticamente" y "Obtener DNS Automático".



onectar usando	D:			
👜 ASUS US	B Wireless Network	Adapte	Configurar	
sta conexión u	iliza los siguientes e	elementos:		
 ✓ ➡ Program ✓ ➤ AEGIS ✓ ➤ Protoco 	nador de paquetes Protocol (IEEE 802 ilo Internet (TCP/IP	QoS 1x) v2.3.1.9)		
<	III			
Instalar	Desinst	alar P	ropiedades	
Descripción –				
Protocolo TCI predeterminad redes conecta	P/IP. El protocolo d lo que permite la co adas entre sí.	e red de área ext municación entre	ensa e varias	
Mostrar icono Notificarme c	en el área de notif uando esta conexió	icación al conec in tenga conecti	tarse vidad limitada o	

Pro

ORMÁT	l'ICOS		
	des de Desteur la Interne		Miguel Hernánde
ieneral	Configuración alternativa		
Puede l red es o con el a	hacer que la configuración IP se compatible con este recurso. De administrador de la red cuál es la	asigne automáticamente si su lo contrario, necesita consultar configuración IP apropiada.	
O (ا	btener una dirección IP automáti	camente	
OU:	sar la siguiente dirección IP: —		1
Direc	sción IP:	d. d. e. e	
Más	cara de subred:	+ + +	
Puer	ta de enlace predeterminada:		
O ا	btener la dirección del servidor D	INS automáticamente	
OU	sar las siguientes direcciones de	servidor DNS:	1
Serv	idor DNS preferido:		
Serv	idor DNS alternativo:		
		Opciones avanzadas)
		Aceptar Cancel	ar

Paso 3.- En estos momentos debemos configurar las redes inalámbricas, para ello pulsamos la pestaña "Redes Inalámbricas" de la ventana "Propiedades de Conexiones de Red Inalámbricas", marcamos la opción "Usar Windows para establecer mi configuración de red inalámbrica" y pulsaremos la opción "Ágregar"

edades de Conex Redes inalámbricas	Tones de red malambricas	
ı ır Windows para estab	lecer mi configuración de red inalám	ibrica
is disponibles: a clic en el siguiente bo s inalámbricas o para c	otón para conectarse o desconectar obtener más información acerca de e	rse de ellas.
	Ver redes inalár	mbricas
es preferidas:		
ectar automáticamente	a redes disponibles en el orden sigu	uiente:
50 I	Sub	ir
	Baja	Te la
vgregar Quita ener más información ac blecer una configuració	ar Propiedades cerca de cómo un de red inalámbrica. Opciones av	vanzadas

ez

Paso 4.- En la siguiente ventana, bajo la pestaña de "Asociación" debemos introducir el nombre SSID: **lumhweb** y seleccionaremos **Abierta** como "Autenticación de red" y "Cifrado de datos" **deshabilitado**



Asociación	Autenticación	Conexión	200
Nombre de	e red (SSID):	lumhweb]
Clave de	e red inalámbrica -		1
Esta red	requiere una clav	ve para lo siguiente:	173-002
Autentio	cación de red:	Abierta	~
Cifrado	de datos:	Deshabilitado	~
Clave de	e red:		
Confirme	e la clave de red:		
Índice d	e clave (avanzadi	o): 1	
🗹 La cl	ave la proporcion	o yo automáticamente	
Ésta es puntos	s una red de equip de acceso inalár	oo a equipo (ad hoc). No se Ibrico	utilizan

Paso 5.- Finalizados estos pasos, pincharemos sobre nuestro icono de red inalámbrica y seleccionaremos la red **lumhweb** y pulsamos **conectar.**





Paso 6.- Una vez conectados, debemos abrir un navegador y nos saldrá una página informativa sobre las normas de uso donde se puede seleccionar "Acceder" si ya tenemos credenciales o bien "Obtener una clave" para poder tener nuestras credenciales.



Paso 7.- Si seleccionamos "Obtener una clave", nos aparecerá la página siguiente:

http://sms4wi	ifi. umh.es :8484/registrar.asp		×5≊ + Q	🙆 Portal Login	×			1
on 🗸 🚳 -	- Q + C) DAEMON Tools Lite	🕶 🥥 Astroburn Lite Weat	her 🔻 🕞 🛛 Radio player	💼 🌒 🍓 Tran:	ilate 🔻 🚹 Face	book 🔻 🚮 Calendar 👻 [👔 Map 🔻 »
TIPOS DE CO	NEXIÓN							
Opción 1: Le	enviamos un SMS con su	clave						
Indíquenos su (válida para 7	número de teléfono ⁽¹⁾ para días).	que le enviemos u	in SMS con la contraseña	a de acceso a la red W	IFI			
(1) Para números inte	ernacionales indique el prefijo correcto de	su país (España: +34)						
		REGISTRO DE	USUARIO					
		Pref. País	Teléfono Móvil					
	Nº Teléfono móvil	+34						
	¿Cuanto es 8 + 7?							
		Canada una a	entressão					
		Concrar and co						
Opción 2: En	víenos un SMS y le enviar Ina clave (válida para 7 día	remos su clave	IS ⁽²⁾ con el texto jumb. Si	su operador de telefor	lía móvil	e acceso		
es Movistar er	nvie el mensaje al 215401, e	en otro caso enviel	o al 669 385 000.			0		
(2) Coste del envío: tr	arifa ordinaria mensaje SMS					unt	umin	
Si ya ha recibi	do la clave Acceder					d	wireless	
						Centro de	Atención al Usuari	0

En esta pantalla podemos optar por enviar un SMS directamente desde nuestro móvil para recibir una clave o bien introducir nuestro teléfono en un formulario y recibir un SMS en el móvil con la clave.



Paso 8.- Una vez obtenida la clave, con la opción "Acceder" nos aparecerá la pantalla de validación y podremos acceder a la red.

🔶 🛞 http://192168.12.3/upload/custom/perfil_portal_captivo/siguiente.htm 🖉 + 🗟 C 🗙 🎯 Portal Login x	
x DAEMON v 🐼 v 🔍 🕂 🕑 DAEMON Tools Lite v 🖉 Astroburn Lite 🏦 Weather v 🛞 Radiio player v 🕢 👻 Translate v 🚯 Facebook v سیالیت کارکان کارک	🖬 Calendar 🕶 🞑 Map 👻 » 🥮
VALIDACIÓN Usuarios de umhnet : Utilizar usuario@umh es y la contraseña del dominio. Estudiantes: Utilizar DNI@umh.es y como contraseña el PIN del acceso identificado. Visitantes: Utilizar n⁰telefono@umh.es y como contraseña la recibida por SMS (válida para 7 días).	Formulario usado para validarse los usuarios
ACCESO DE USUARIO	
Usuario Contraseña Conectar	, mh
Centro de Aten 96 662	ción al Usuario 5 8582

En esta pantalla se deben introducir nuestras credenciales según nuestro perfil:

- **PAS y PDI:** Deberán introducir su usuario de dominio y password.
- Alumnos: Deberán introducir como usuario su DNI@umh.es, el password es el PIN que tienen asignado y deberán dejar el domino en blanco.
- Personal Visitante: Deberán introducir como usuario su nº de Teléfono@umh.es, como password el código de que habrán recibido por SMS y dejar el domino en blanco.

Una vez identificados, tendremos acceso no seguro desde la red lumhweb a Internet.



10 EDUROAM

10.1 DESCRIPCIÓN DE LA RED EDUROAM

El objetivo del Proyecto Eduroam (*Educational Roaming*) es tener conectividad y movilidad entre las distintas redes inalámbricas de investigación mundiales que estén adheridas a dicho proyecto. De esta forma, un usuario de otra institución que esté adscrita a este proyecto, podría conectarse, sin realizar cambios en la configuración de su equipo, desde nuestra universidad con su identificador y clave, e igualmente, un usuario de nuestra universidad podría conectarse, desde cualquiera de las redes incluidas en Eduroam, a Internet.

Eduroam.es es una iniciativa de <u>RedIRIS</u> que se encarga de coordinar en el ámbito nacional las iniciativas de diversas organizaciones con el fin de conseguir un espacio único de movilidad. Este espacio único de movilidad consiste en un amplio grupo de organizaciones, que en base a una política de uso y una serie de requerimientos tecnológicos y funcionales, permiten que sus usuarios puedan desplazarse entre ellas, disponiendo en todo momento de los servicios móviles que pudieran necesitar. El objetivo último sería que estos usuarios al llegar a otra organización dispusieran, de la manera más transparente posible, de un entorno de trabajo virtual con conexión a Internet y acceso a los servicios y recursos de su organización origen, así como acceso a los servicios y recursos de la organización que en ese momento les acoge.

La iniciativa eduroam también tiene su <u>extensión internacional</u> que engloba a distintas organizaciones NREN (National Research and Education Network) en Europa y a lo largo del mundo.

Para mas información sobre eduroam, puede visitar los sitios oficiales de eduroam en Internet:

www.eduroam.es

www.eduroam.org

10.2 CONEXIÓN A EDUROAM DESDE LA UMH PARA USUARIOS DE OTRAS INSTITUCIONES ADHERIDAS A LA INICIATIVA.

Eduroam permite a los usuarios de otras instituciones adheridas al proyecto conectarse a la red inalámbrica de la UMH utilizando las credenciales de su institución de origen. Para ello, el usuario visitante deberá conocer previamente los parámetros de autenticación de su institución ya que se validará contra ella. Los pasos a seguir para conectarse a eduroam son los siguientes:

Comprobar si nuestro equipo Windows XP está actualizado para soportar WPA. Para ello deberemos comprobar la versión de Service Pack que tenemos instalada (



botón derecho del ratón en el icono "Mi PC", y seleccionar "Propiedades" del menú desplegable).

• Si tenemos Windows XP SP1. Necesitamos tener instalada la "REVISIÓN DE WINDOWS XP PARA OBTENER COMPATIBILIDAD CON WPA". Para comprobar si está instalada ir a:

"Inicio" -> "Panel de Control" -> "Agregar o quitar programas"

Tiene que existir un programa instalado con nombre "REVISIÓN DE WINDOWS XP – KB826942". En caso de no tenerla instalada, la podéis obtener <u>en este enlace.</u>

• Windows XP SP2. El equipo está listo para conectarse.

Debemos seleccionar las conexión de red inalámbrica mediante "Inicio -> Panel de Control -> Conexiones de red.

Seleccionamos la conexión de red Inalmbrica y con el botón derecho del ratón pulsar "Propiedades"





Debemos configurar los parámetros TCP/IP dentro de la pestaña general de las conexiones de red, marcando las opciones de "Obtener Dirección IP Automáticamente" y "Obtener DNS Automático".

- Propi	edades de Conex	xiones de red	inalámbricas	?
General	Redes inalámbricas	Dpciones ava	nzadas	
Conect	ar usando:			
B A	SUS USB Wireless I	Network Adapte	Configurar	
Esta co	nexión utiliza los sigu	ientes elementos		
	Programador de pa AEGIS Protocol (IE Protocolo Internet)	quetes QoS EE 802.1x) v2.3. TCP/IP)	1.9	
<		100		
lr	istalar	Desinstalar	Propiedades	
Desci	ipción			
Proto prede rede	icolo TCP/IP. El prot eterminado que perm s conectadas entre s	iocolo de red de a ite la comunicaci ií.	área extensa ón entre varias	
I Mos I Moti Moti nula	trar icono en el área ficarme cuando esta	de notificación a conexión tenga (l conectarse conectividad limitada o	
			Aceptar	Cancelar

eral Configuración alternativa	
ede hacer que la configuración l l es compatible con este recurso n el administrador de la red cuál d Obtener una dirección IP auto	P se asigne automáticamente si su . De lo contrario, necesita consultar es la configuración IP apropiada. máticamente
Usar la siguiente dirección IP:	
Dirección IP;	the the test
Máscara de subred:	
Puerta de enlace predeterminad	an in in in in
Obtener la dirección del servic	dor DNS automáticamente
🔿 Usar las siguientes direccione	s de servidor DNS:
Servidor DNS preferido:	

FRSITAS

En estos momentos debemos configurar las redes inalámbricas, para ello pulsamos la pestaña "Redes Inalámbricas" de la ventana "Propiedades de Conexiones de Red Inalámbricas", marcamos la opción "Usar Windows para establecer mi configuración de red inalámbrica" y pulsaremos la opción "Agregar".

piedades de Conexion	nes de red inalámbricas 🛛 ?
	polones avanzauas
usar windows para establec	er mi conriguración de red inalambrica
edes disponibles:	
ja clic en el siguiente botó	n para conectarse o desconectarse de
es inalambricas o para obte	ener mas informacion acerca de ellas.
	Ver redes inalámbricas
lea crafaridaa:	
nectar automáticamente a i	redes disponibles en el orden siguiente:
	Subir
	Deter
	Bajar
	[bajar
Agregar	Propiedades

En la siguiente ventana, bajo la pestaña de "Asociación" debemos introducir el nombre SSID: **eduroam** y selección **WPA** como "Autenticación de red" y **TKIP** como "Cifrado de datos".

En caso de que la opción WPA no esté disponible puede ser porque su tarjeta inalámbrica no sea compatible WPA o si lo es, necesite actualizar los drivers de la misma.



sociación	Autenticación	Conexión
Nombre de	e red (SSID):	eduroam
Clave de	red inalámbrica	
Esta red	requiere una cla	ve para lo siguiente:
Autentic	ación de red:	WPA 💌
Cifrado	de datos:	TKIP
Clave de	e red:	
Confirme	i la clave de red:	
Índice d	e clave (avanzad	lo). 1
🗹 La cl	ave la proporcior	no yo automáticamente
Ésta es puntos	: una red de equi de acceso inalár	po a equipo (ad hoc). No se utilizan nbrico

Bajo la pestaña "Autenticación", se debe habilitar la autenticación IEEE 802.1x y como tipo de EAP, escogemos el método de autenticación proporcionado por nuestra universidad de origen.

10.3 CONEXIÓN AEDUROAM DE USUARIOS DE LA UMH QUE VISITAN OTRAS INSTITUCIONES.

Los usuarios de la UMH que visiten otras instituciones adheridas a eduroam podrán beneficiarse de la infraestructura inalámbrica de esta institución utilizando sus credenciales de la UMH. Para ello el usuario deberá conectarse al SSID eduroam según indica la institución donde se encuentra y utilizar como método de autenticación PEAP para poder validar sus credenciales contra el servidor de la UMH tal y como se indica a continuación. A la hora de validar el usuario deberá utilizar su nombre de usuario seguido de @umh.es y su contraseña.

Bajo la pestaña de "Autenticación" en las propiedades de red inalambrica, se debe habilitar la autenticación IEEE 802.1X y debemos escoger como "Tipo de EAP" : **PEAP**



sociacion	Autenticación	Conexión
Seleccion redes Ethe	e esta opción pa met inalámbrica:	ra proporcionar acceso autenticado a s.
🔽 Habilita	ar la autenticació	n IEEE 802.1X en esta red
Tipo de EAP:	EAP protegido	o (PEAP)
Autenti	car como equípo) cuando la información de equipo esté
Autenti disponi Autenti equipo	car como equipo ble car como invitad no estén disponi	o cuando la información de equipo esté lo cuando el usuario o la información de ibles

Ahora se debe configurar la autenticación PEAP, para ello pulsamos sobre el botón "Propiedades". En la pantalla siguiente deberemos deseleccionar la opción "Validar un certificado del servidor" y escogeremos como "Método de autenticación" **EAP-MSCHAPv2**.



	£		
Validar un certificado	de servidor		
Conectar a estos se	rvidores:		
tidades emisoras de (certificados raíz de co	nfianza:	
ABA.ECOM Root C	A		~
Autoridad Certifica	idora de la Asociacion	Nacional del N	otaria 🦰
Autoridad Certifica	idora del Colegio Naci	onal de Corred	uria P
Baltimore EZ by DS	т		
Belgacom E-Trust F	Primary CA		
C&W HKT SecureN	et CA Class A		
			~
C&W HKT SecureN	et CA Class B		1.000
C&W HKT SecureN	et CA Class B		<u>></u>
C&W HKT SecureN No pedir la intervent servidores o entidad cione el método de a	et CA Class B tim tión del usuario para a les emisoras de certifi utenticación:	autorizar nuevo cados de confi	is anza.
C&W HKT SecureN No pedir la intervenc servidores o entidad cione el método de a traseña segura (EAP-	et CA Class B ini ión del usuario para a les emisoras de certifi utenticación: ·MSCHAP v2)	autorizar nuevo cados de confi	nfigurar

Ahora pasaremos a configurar la forma en que se pedirá usuario y contraseña para MSCHAPv2, para ello debemos pulsar el botón **Configurar** en la pantalla "Propiedades de EAP Protegido", aparecerá otra ventana donde solamente deberemos deseleccionar la opción **"Usar el nombre de inicio de sesión y la contraseña de Windows"** puesto que podemos usar credenciales diferentes.

Propied	lades de EAP M	SCHAPv2	×
Al cone	ctar: sar automáticament	e el nombre de inicio	de
e:	esión y la contraseñ kiste alguno).	a de Windows (y dom	inio, si
	Aceptar	Cancelar	

Finalizados estos pasos, debemos seleccionar la red eduroam y pulsamos conectar.





Nos aparecerá en la barra de tareas un mensaje invitándonos proporcionar las credenciales, hemos de pulsar y nos aparece la pantalla siguiente invitándonos a introducir nuestras credenciales.



scribir credei	nciales	
6		
Nombre de		
usuario;		
usuario: Contraseña:		
usuario: Contraseña: Dominio de inicio de sesión:		
usuario: Contraseña: Dominio de inicio de sesión:		
usuario: Contraseña: Dominio de inicio de sesión:		

En esta pantalla se deben introducir nuestras credenciales según nuestro perfil:

• Usuarios de la UMH (PAS y PDI): Deberán introducir su usuario de dominio seguido de @umh.es. y su password. Por ejemplo:

Nombre de usuario: usuario@umh.es

Password: xxxxxxxxx