Procedimiento de Conexión a Red Inálambrica

Windows 7

Caso 1. Equipos registrados en dominio UAI

1) Primeramente se debe tener tarjeta de red inalámbrica encendida.

2) Ir a redes inalámbricas disponibles tal como se muestra en la imagen:



3) Se debe mostrar redes inalámbricas disponibles y luego seleccionar red deseada.

Conexión de red inalámbrica		^
UAI Funcionarios		llee
UAI Alumnos		lle.
Conectado actualmente a:		
uai.cl Acceso a Internet		
Red no identificada Sin acceso a la red		
Acceso telefónico y VPN	Ξ	
VPN-UAI		
VPN2		
Conexión de red inalámbrica		
UAI Funcionarios		
Conectar		
UAI Alumnos	~	
Abrir Centro de redes y recursos compartidos		ļ

4) Al seleccionar

<u><u>Conectar</u> se presentará un mensaje de Alerta de seguridad</u>



5) Seleccionar nuevamente la opción 💄



6) El equipo al estar dentro del dominio tiene las credenciales del usuario guardadas, estas no serán solicitadas y se conectara a internet.

7) Si la conexión no fuera exitosa, se debe borrar la conexión de red existente desde el administrador de redes inalámbricas, primero se va "Panel de Control"



8) Ya dentro de "Panel de Control" se debe acceder a:



9) Y seleccionamos "Administrar redes inalámbricas"



10) En la siguiente pantalla se muestra un ejemplo con la red "Funcionarios", pero también se aplica a la red "Alumnos"

Admi Windo	inistrar redes inalámbricas que ws intenta conectarse a estas redes en e	e usen (Conex I orden que apare	ión de red inalámbrica) ce a continuación.
gregar	Quitar Propiedades del adaptador	Tipos de perfil	Centro de redes y recursos compartidos
edes que	puede ver, modificar y reordenar (1) —		
U U	AI Funcionarios	Segu	ridad: WPA2-Enterprise
	Propiedades		
	Quitar red		
	Cambiar nombre		

11) Luego de quitar la red repita los pasos desde el punto 1 hasta el 5, es posible que se requieran credenciales para entrar a la red indicada

Autentica	ción de red
scriba sus c	redenciales de usuario
	Contrasena

Si la conexión aun así no es exitosa, puede que haya que eliminar la red y volver a crearla manualmente.

Para borra la red repita los pasos desde el punto 7 hasta el punto 10. A continuación se detalla cómo crear una red manualmente.

12) Ingrese a "Administrar redes inalámbricas", repita pasos desde el punto 7 hasta el punto 9

13) En la pantalla de Administrar redes inalámbricas, vaya a la opción "Agregar"



14) Se abrirá la siguiente pantalla, elegiremos la primera opción, "Crear un perfil de red manualmente"



15) Al elegir la opción antes mencionada se abrirá la siguiente pantalla donde se deben incluir los campos

Nombre de la red: UAI Alumnos (o UAI Funcionarios, según sea el caso)

Tipo de seguridad: WPA2-Enterprise

Tipo de Cifrado: AES

Por el momento destiquearemos la opción "iniciar esta conexión automáticamente"

Estas configuraciones se deben aplicar según se muestra en la siguiente imagen.

Escriba la informac	ión de la red inalámbrica que c	lesea agregar.
Nombre de la red:	UAI Alumnos	
Tipo de seguridad:	WPA2-Enterprise	
Tipo de cifrado:	AES	
Clave de seguridad:		Ocultar caracteres
📃 Iniciar esta conexi	ón automáticamente	
🔲 Conectarse aunqu	e la red no difunda su nombre	
Advertencia: esta	opción podría poner en riesgo la privaci	dad del equipo.

16) Al presionar la opción "siguiente" se abrirá una nueva ventana.

UAI A	umnos se agregó correctamente.	
•	Cambiar la configuración de conexión Abra las propiedades de la conexión para cambiar la configuración.	
		Cerrar

Elegiremos la única opción disponible.

17) En la siguiente ventana seleccionaremos la pestaña que dice "Seguridad"

Conexión Seguridad	
Nombre:	UAI Funcionarios
SSID:	UAI Funcionarios
Tipo de red:	Punto de acceso
Disponibilidad de red:	Todos los usuarios
Conectarse automátic alcance	amente cuando esta red esté dentro del
Conectarse a una red	con mayor preferencia si está disponible
Conectarse aunque la	red no difunda su nombre (SSID)
📰 Habilitar configuración	a de conexión de Intel
Configurar	

18) En la Pestaña de seguridad elegiremos la opción "Configuración"

Conexión Seguridad	
Tipo de seguridad:	WPA2-Enterprise
Tipo de cifrado:	AES 💌
Microsoft: EAP prot	egido (PEAP) 👻 Configuración
Microsoft: EAP prot	egido (PEAP) Configuración denciales para esta conexión cada sión
Microsoft: EAP prot	egido (PEAP) Configuración denciales para esta conexión cada sión
Microsoft: EAP prot	egido (PEAP) Configuración denciales para esta conexión cada sión anzada
Microsoft: EAP prot	egido (PEAP) Configuración denciales para esta conexión cada sión anzada
Microsoft: EAP prot	egido (PEAP) Configuración denciales para esta conexión cada sión anzada

19) En esta ventana buscaremos el certificado "Digicert High Assurance EV Root CA" y le pondremos un ticket, si este no aparece, buscar el certificado "Entrust.net Certification Authority (2048)"

 Validar un certificado de servidor Conectarse a estos servidores: Entidades de certificación raíz de confianza: Certum CA Class 3 Public Primary Certification Authority DigiCert High Assurance EV Root CA Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority Equifax Secure Certificate Authority Generic Root Trust CA III No pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. deccione el método de autenticación: ontraseña segura (EAP-MSCHAP v2) Configurar. Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad 	conectar:				
Conectarse a estos servidores: Entidades de certificación raíz de confianza: Certum CA Class 3 Public Primary Certification Authority DigiCert High Assurance EV Root CA Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority Equifax Secure Certificate Authority Generic Root Trust CA Monopedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. No pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. deccione el método de autenticación: ontrasefía segura (EAP-MSCHAP v2) Configurar. Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad	Validar un	certificado de servi	dor		
Conectarse a estos servidores: Entidades de certificación raíz de confianza: Certum CA Class 3 Public Primary Certification Authority DigiCert High Assurance EV Root CA Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority Equifax Secure Certificate Authority Generic Root Trust CA Configuration No pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. Heccione el método de autenticación: contraseña segura (EAP-MSCHAP v2) Configurar. Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad					
Entidades de certificación raíz de confianza: Certum CA Class 3 Public Primary Certification Authority DigiCert High Assurance EV Root CA Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority Equifax Secure Certificate Authority Generic Root Trust CA III No pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. leccione el método de autenticación: ontraseña segura (EAP-MSCHAP v2) Configurar. Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad	Conecta	se a estos servidore	es:		
Certum CA Class 3 Public Primary Certification Authority DigiCert High Assurance EV Root CA Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority Equifax Secure Certificate Authority Generic Root Trust CA Monopedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. Meccione el método de autenticación: Iontrasefia segura (EAP-MSCHAP v2) Configurar. Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad	Entidades de	e certificación raíz de	e confianza:		
Class 3 Public Primary Certification Authority DigiCert High Assurance EV Root CA Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority Equifax Secure Certificate Authority Generic Root Trust CA Mo pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. No pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. Intraseña segura (EAP-MSCHAP v2) Configurar. Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad Aceptar Cancelar	Certum	CA			
DigiCert High Assurance EV Root CA Entrust.net Certification Authority (2048) Entrust.net Secure Server Certification Authority Equifax Secure Certificate Authority Generic Root Trust CA Image: Constraint of the second sec	Class 3	Public Primary Certifi	ication Authority		-
	☑ DigiCert	High Assurance EV	Root CA		-
Entrust.net Secure Server Certification Authority Equifax Secure Certificate Authority Generic Root Trust CA No pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. Aeccione el método de autenticación: iontraseña segura (EAP-MSCHAP v2) Configurar. Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad Acceptar Cancelar	Entrust.	net Certification Au	thority (2048)		
Equifax Secure Certificate Authority Generic Root Trust CA No pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. eleccione el método de autenticación: iontraseña segura (EAP-MSCHAP v2) (Configurar.] Habilitar reconexión rápida] Aplicar Protección de acceso a redes] Desconectar si servidor no presenta TLV con enlace de cifrado] Habilitar privacidad de identidad Acceptar Cancelar	Entrust.	net Secure Server C	Certification Authority		
Generic Root Trust CA No pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. Geccione el método de autenticación: iontraseña segura (EAP-MSCHAP v2) (Configurar. Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad Aceptar Cancelar	Equifax	Secure Certificate A	uthority		
III No pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. deccione el método de autenticación: contraseña segura (EAP-MSCHAP v2) Configurar. Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad Aceptar Cancelar	Concrie	Deet Trust CA			100
No pedir la intervención del usuario para autorizar nuevos servidores o entidades de certificación de confianza. Seccione el método de autenticación: Configurar. Intervención rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad Aceptar Cancelar	Generic	ROOLITUSECA			1.21
Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad Aceptar Cancelar	No pedir	la intervención del u	suario para autorizar	nuevos	
Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad Aceptar Cancelar	No pedir servidore leccione el m	la intervención del u es o entidades de ce étodo de autenticac egura (EAP-MSCHAP	suario para autorizar rtificación de confianz ión: v 2) v2)	nuevos a. Config	urar.
Desconectar si servidor no presenta TLV con enlace de cifrado Habilitar privacidad de identidad	No pedir servidore leccione el m ontraseña se	la intervención del u es o entidades de ce étodo de autenticac egura (EAP-MSCHAP conexión rápida	suario para autorizar rtificación de confianz ión: v v2) v2	nuevos a.	urar.
Habilitar privacidad de identidad Aceptar Cancelar	Generic Generic No pedir servidore leccione el m ontraseña su Habilitar reu Aplicar Prot	la intervención del u so entidades de ce létodo de autenticac egura (EAP-MSCHAP conexión rápida ección de acceso a l	suario para autorizar rtificación de confianz ión: v v2) • redes	nuevos a.	urar.
Aceptar Cancelar	 Generic No pedir servidore leccione el montraseña su Habilitar reu Aplicar Prot Desconecta 	la intervención del u so entidades de ce étodo de autenticac egura (EAP-MSCHAP conexión rápida ección de acceso a la si servidor no pres	suario para autorizar rtificación de confianz ión: v v2) • redes senta TLV con enlace o	nuevos a. Config de cifrado	urar.
F The second s	 Verience No pedir servidore No pedir servidore Ideccione el montraseña se Habilitar rei Desconecta Habilitar pri de identida 	la intervención del u es o entidades de ce étodo de autenticac egura (EAP-MSCHAP conexión rápida ección de acceso a u rr si servidor no pres vacidad d	suario para autorizar rtificación de confianz ión: v2) v redes senta TLV con enlace o	nuevos a. Config de cifrado	urar.

20) En la ventana anterior si presionamos el botón "Configurar" se desplegara la siguiente información



Esta ventana es importante ya que si el equipo pertenece al dominio, y se encuentra con ticket la opción, usara las credenciales de Windows para acceder a la red creada, si su equipo no pertenece a la red, retire este ticket.

21) Al elegir la opción "Aceptar", volveremos a la ventana que se muestra en el punto 18, ahora elegiremos la opción "Configuración avanzada", esta nos mostrara la siguiente información, debemos tickear la opción "Especificar modo de autenticación" y selecciónamos " Autenticacion de usuarios o equipos". Presionar Aceptar.

 Especificar modo de autenticación: Autenticación de usuarios o (Guardar credenciales Eliminar credenciales de todos los usuarios Habilitar inicio de sesión único en esta red Realizar inmediatamente antes de que el usuario inicie sesión Realizar inmediatamente después de que el usuario inicie sesión Retraso máximo (segundos): Permitir cuadros de diálogo adicionales durante el inicio de sesión único 	onfiguración de 802.1X Configuración o	de 802.11
Autenticación de usuarios o € Guardar credenciales Eliminar credenciales de todos los usuarios Habilitar inicio de sesión único en esta red	Especificar modo de autenticación:	
 Eliminar credenciales de todos los usuarios Habilitar inicio de sesión único en esta red Realizar inmediatamente antes de que el usuario inicie sesión Realizar inmediatamente después de que el usuario inicie sesión Retraso máximo (segundos): 10 * Permitir cuadros de diálogo adicionales durante el inicio de sesión único 	Autenticación de usuarios o e 🔻	Guardar credenciales
 Habilitar inicio de sesión único en esta red Realizar inmediatamente antes de que el usuario inicie sesión Realizar inmediatamente después de que el usuario inicie sesión Retraso máximo (segundos): 10 Permitir cuadros de diálogo adicionales durante el inicio de sesión único 	Eliminar credenciales de todos l	os usuarios
 Realizar inmediatamente antes de que el usuario inicie sesión Realizar inmediatamente después de que el usuario inicie sesión Retraso máximo (segundos): 10 1	Habilitar inicio de sesión único en e	sta red
 Realizar inmediatamente después de que el usuario inicie sesión Retraso máximo (segundos): 10 Permitir cuadros de diálogo adicionales durante el inicio de sesión único 	Realizar inmediatamente antes sesión	de que el usuario inicie
Retraso máximo (segundos): 10 💌	Realizar inmediatamente despu inicie sesión	és de que el usuario
Permitir cuadros de diálogo adicionales durante el inicio de sesión único	Retraso máximo (segundos):	10
The state and some 1. ANI state to be a supervised as a same lar.	Permitir cuadros de diálogo adio de sesión único	cionales durante el inicio
autenticación de usuarios y equipos	Esta red usa LAN virtuales sepa autenticación de usuarios y equ	aradas para la Jipos
	ſ	

22) Cerramos la ventana que se muestra en el punto 16 y accedemos a la red requerida, repetimos los pasos desde el punto 1 hasta el 5

Caso 2. Equipos personales.

23) La conexión de equipos que están fuera del dominio UAI debiera solo mostrar el mensaje:

No se pudo co	mpletar el intento de conexión
No se pudieron validar las cred que finalice la conexión y que c detalles. Aún puede conectarse a un riesgo de seguridad d	enciales proporcionadas por el servidor. Es recomendable omunique al administrador la información suministrada en los e, pero si lo hace, se expone ebido a un posible servidor no autorizado.

24) Para acceder a esta ventana repita pasos desde los puntos 1 al punto 4

25) Haga click en el botón

26) Si la conexión no fuera exitosa revisar pasos desde los puntos 6 hasta el punto 22

*Estos dos casos se debiera aplicar también para el sistema operativo WINDOWS VISTA.