CTU – FCEIA

PROCEDIMIENTO PARA CONECTAR A LA RED FCEIA-CTU-Segura en una maquina con Windows 7

Sobre FCEIA-CTU-Segura:

Es una de las 2 redes Wi-Fi disponibles en FCEIA. Esta red cuenta con un sistema de autenticación y cifrado de conexiones entre los más avanzados a la fecha. Quienes accedan por esta red, tendrán el mismo nivel de acceso a la red cableada, que una máquina conectada a ella. En el caso de conexiones inalámbricas es muy importante el cifrado, ya que existen multitud de programas que permiten espiar las conexiones no cifradas – desde cualquier lugar adonde llegue la señal inalámbrica.

En caso de que no le sea posible conectarse a ésta red (por falta de drivers, equipo obsoleto o no compatible), se cuenta con otra que tiene requerimientos mínimos destinada principalmente a visitantes y estudiantes. Tenga en cuenta que ésta otra red (*FCEIA-CTU-Abierta*) no cuenta con cifrado de datos y cuenta con el mismo acceso a la red de la facultad, que un usuario que accede desde Internet (lo mas notable es que, por diseño, no tiene acceso a las direcciones privadas).

Pre-requisitos para FCEIA-CTU-Segura:

- Contar con una cuenta de usuario en el servidor "eva". Se usará el mismo usuario y clave del correo.
- Antes de conectarse por primera vez, es imprescindible que cambie su clave en eva, ya que de esa forma se creará su información para conexión wifi segura. Para cambiar su clave ingrese a la página de acceso al correo y cambio de clave, o bien solicitarlo en el Laboratorio de Pellegrini.
- Tener placa Wi-Fi en su computadora :)

PASO 1:

Haga click sobre el ícono de Admistrador de Conexiones Inalámbricas en la barra de tareas, para ver las redes disponibles. Chequeamos entonces, sin hacer click, que se encuentre visible "FCEIA-CTU-Segura". Luego de esto, hacemos click en "Abrir Centro de Redes y Recursos Compartidos", donde indica la figura.



PASO 2:

Haga click sobre el texto "Administrar redes inalámbricas", donde daremos de alta manualmente la red, dado que Windows no procede como se desea, cuando intenta conectarse.



<u>*P*ASO</u> 3:

Haga click en "Agregar".



PASO 4:

Nos pregunta como deseamos agregar la red. Respondemos con la primer opción, es decir, manualmente.



PASO 5:

Completamos de la siguiente manera:

|) all Conectarse manualm | ente a una red inalámbrica | |
|--|---|--------------------------|
| Escriba la informac | ión de la red inalámbric | a que desea agregar. |
| Nombre de la red: | FCEIA-CTU-Segura | (1) |
| Tipo de seguridad: | WPA2-Enterprise | - (2) |
| Tipo de cifrado: | AES | • (3) |
| Clave de seguridad: | | Ocultar caracteres |
| Iniciar esta conexi Conectarse aunqu Advertencia: esta | ón automáticamente ie la red no difunda su nombre opción podría poner en riesgo l | a privacidad del equipo. |
| | | Siguiente Cancelar |

- 1) Nombre de la red: FCEIA-CTU-Segura
- 2) Tipo de seguridad: WPA2-Enterprise
- 3) Tipo de Cifrado: AES
- 4) Hacemos click en "Siguiente".

PASO 6:

Nos aparece la siguiente ventana, donde clickeamos en "Cambiar la configuración de la conexión".



PASO 7:

Dentro de la configuración de la conexión, tenemos 2 pestañas, (1) y (2). En (1) dejamos como viene (a) por omisión, es decir, que se conecte automáticamente si la red está en alcance. Luego pasamos a (2).

| Conexión Seguridad | |
|---------------------------------|--|
| (1) (2) Nombre: | FCEIA-CTU-Segura |
| SSID: | FCEIA-CTU-Segura |
| Tipo de red: | Punto de acceso |
| Disponibilidad de red: | Todos los usuarios |
| Conectarse automátic alcance | camente cuando esta red esté dentro del |
| Conectarse a una rec | l con mayor preferencia si está disponible |
| | |
| Conectarse aunque la | a red no difunda su nombre (SSID) |
| Conectarse aunque la | a red no difunda su nombre (SSID) |
| Conectarse aunque la | a red no difunda su nombre (SSID) |

PASO 8:

En "Seguridad", elegimos el método de autenticación de red "Microsoft: EAP protegido (PEAP)" si es que ya no se encuentra seleccionado de la lista desplegable. Luego de ésto, hacemos click en (1) "Configuración".

| Conexion Segundad | | | | |
|-------------------------|-------------------|--------|---------------|-----|
| Tipo de seguridad: | WPA2-Enter | rprise | • | |
| Tipo de cifrado: | AES | | • | |
| Elija un método de aute | nticación de red | : | | |
| Microsoft: EAP protegie | do (PEAP) | • | Configuración | (1) |
| Recordar mis creder | iciales para esta | conex | ión cada | |
| Vez que inicie sesión | iciales para esta | conex | ión cada | |
| Configuración avanz | rada (2) | conex | ión cada | |

PASO 9:

En "Configuración", nos aparece la siguiente ventana, donde tenemos que:

| Al conectar: | |
|---|---|
| 🔲 Validar un certificado de servidor (1) | |
| Conectarse a estos servidores: | |
| | 1 |
| Entidades de certificación raíz de confianza: | |
| Class 3 Public Primary Certification Authority | * |
| Equifax Secure Certificate Authority | |
| Example Certificate Authority | = |
| 🔲 GTE CyberTrust Global Root | |
| Microsoft Root Authority | |
| Microsoft Root Certificate Authority | |
| Symantec Root 2005 CA | * |
| ٠ III. | - F |
| No pedir la intervención del usuario para autori | izar nuevos |
| No pedir la intervención del usuario para autori servidores o entidades de certificación de conf Seleccione el método de autenticación: (2) | izar nuevos ianza. |
| No pedir la intervención del usuario para autori servidores o entidades de certificación de conf Seleccione el método de autenticación: (2) Contraseña segura (EAP-MSCHAP v2) | izar nuevos ianza. |
| No pedir la intervención del usuario para autori servidores o entidades de certificación de conf Seleccione el método de autenticación: (2) Contraseña segura (EAP-MSCHAP v2) ✓ Habilitar reconexión rápida | izar nuevos ianza. Configurar (3) |
| No pedir la intervención del usuario para autori servidores o entidades de certificación de conf Seleccione el método de autenticación: (2) Contraseña segura (EAP-MSCHAP v2) Habilitar reconexión rápida Aplicar Protección de acceso a redes | izar nuevos ianza. ▼ Configurar (3) |
| No pedir la intervención del usuario para autori servidores o entidades de certificación de conf Seleccione el método de autenticación: (2) Contraseña segura (EAP-MSCHAP v2) Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enla | Configurar (3) ace de cifrado |
| No pedir la intervención del usuario para autori servidores o entidades de certificación de conf Seleccione el método de autenticación: (2) Contraseña segura (EAP-MSCHAP v2) Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enla Habilitar privacidad de identidad | Configurar Configurar (3) ace de cifrado |
| No pedir la intervención del usuario para autori servidores o entidades de certificación de conf Seleccione el método de autenticación: (2) Contraseña segura (EAP-MSCHAP v2) Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enla Habilitar privacidad de identidad | Configurar (3) ace de cifrado |
| No pedir la intervención del usuario para autori servidores o entidades de certificación de conf Seleccione el método de autenticación: (2) Contraseña segura (EAP-MSCHAP v2) V Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enla Habilitar privacidad de identidad | Configurar Configurar (3) ace de cifrado ar Cancelar |
| No pedir la intervención del usuario para autori servidores o entidades de certificación de conf Seleccione el método de autenticación: (2) Contraseña segura (EAP-MSCHAP v2) Habilitar reconexión rápida Aplicar Protección de acceso a redes Desconectar si servidor no presenta TLV con enla Habilitar privacidad de identidad | Configurar Configurar (3) ace de cifrado ar Cancelar |

- 1) Destildar "Validar un certificado de servidor"
- Seleccionar método de autenticación "Contraseña segura (EAP-MSCHAP v2)
- 3) Hacer click en "Configurar"

PASO 10:

Nos aparece la siguiente ventana, donde tenemos que destildar la opción "Usar automáticamente el nombre de inicio de sesión y la contraseña de Windows (y dominio, si existe alguno)".

| Propieda | des de | EAP MS | СНАР | v2 | | × |
|--------------|---|------------------------------------|--------------------|--------------------|------------------------|-----------------|
| Al cone | ctar: | | | | | |
| U Se e | sar aut esión y ciste al <u>c</u> | omáticame la contrase guno). | nte el i rña de | nombre (Window | de inicio /s (y don | de ninio, si |
| T | C | Aceptar | | Cance | lar | |

Damos "Aceptar", volvemos a la ventana del Paso 9, donde nuevamente damos "Aceptar", volviendo a la ventana del Paso 8.

PASO 11:

En ésta ventana del **Paso 8**, hacemos click en (2), es decir, en "Configuración Avanzada", donde nos aparece la siguiente ventana:

| Config | guración de 802.1X Configuración | de 802.11 |
|--------|--|-----------------------------|
| | Especificar modo de autenticación | |
| 1) | Autenticación de usuarios o 🤅 🔻 | Guardar credenciales |
| | Eliminar credenciales de todos | los usuarios |
| -E | Habilitar inicio de sesión único en e | esta red |
| | Realizar inmediatamente antes sesión | s de que el usuario inicie |
| | Realizar inmediatamente despu inicie sesión | ués de que el usuario |
| | Retraso máximo (segundos): | 10 |
| | Permitir cuadros de diálogo ad de sesión único | icionales durante el inicio |
| | Esta red usa LAN virtuales sep autenticación de usuarios y eq | aradas para la Juipos |
| | | |
| | | |
| | | |
| | | |
| | | |

Deberemos hacer tildar la opción "Especificar modo de autenticación" y dejar la opción por omisión, es decir "Autenticación de usuarios o equipos".

Luego hacemos click en "Aceptar" para cerrar la ventana, y posteriormente en "Aceptar" nuevamente, para terminar cerrando la ventana del *Paso 7*.

PASO 12:

Nos queda la ventana del *Paso 6*, donde le damos en "Aceptar" para cerrar la misma.



PASO 13:

Una vez hecho el paso anterior, sale un mensaje en la barra de tareas indicando que "Se necesita información adicional para conectar a "FCEIA-CTU-Segura".



Hacemos click dentro del mensaje informativo, donde nos aparece una ventana para ingresar nuestros datos ((1) Usuario / (2) Contraseña) de EVA:

| utenticac | ción de red | |
|--------------|-----------------------|-----|
| criba sus cr | edenciales de usuario | |
| | | |
| 1 | Nombre de usuario | (1) |
| | Contraseña | (2) |

Una vez que completamos los mismos, y hacemos click en "Aceptar", luego de unos segundos donde intercambia datos, la conexión se establece.

