



Manual: Guía de conexión a la red LAN y WLAN

**Karen Lucero Roldán Serrato
Alethia Patricia Estrella Ruiz
Emmanuel Gómez Cantoya
2022**

Financiamiento (interno)

Manual: Guía de conexión a la red LAN y WLAN

Karen Lucero Roldán Serrato, Alethia Patricia Estrella Ruiz, Emmanuel Gómez Cantoya

Instituto de Ciencias Aplicadas y Tecnología, Circuito Exterior S/N, C.P. 04510,
A.P.70- 186, Universidad Nacional Autónoma de México, CDMX, México.

Resumen

En este documento se presenta el procedimiento para la configuración de una conexión en la red local (LAN) en dispositivos Windows y la configuración de una conexión inalámbrica (WLAN) en la autenticación para modo interno (BYOD) y externo (GUEST) con el fin de lograr la conexión a internet de los usuarios hacia los equipos y dispositivos dentro del instituto. A continuación, se describe de forma detallada el procedimiento a fin de facilitar una guía de apoyo a la configuración de la tarjeta de red interna en los equipos, que requieran la conexión a internet respecto a los usuarios, el personal interno y visitantes al instituto.

Índice

Resumen	1
Nomenclatura	3
Introducción	4
Especificaciones	7
1. Guía de configuración para el protocolo de autenticación 802.11x en <i>Windows</i>	7
2. Guía de conexión <i>WiFi</i> con el protocolo 802.11x en <i>Windows</i>	13
Referencias.....	18

Nomenclatura

BYOD	<i>Bring Your Own Device, Conexión sobre traer tu propio dispositivo (Rouse, 2017).</i>
Dirección MAC	<i>es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales [8 bits]) (Rouse, 2017)</i>
GUEST	<i>Conexiones para invitados son las que tienen un tiempo limitado y es para visitantes que requieran conexión a internet (Rouse, 2017).</i>
Internet	<i>Es una conexión entre equipos para comunicación y ofrecer servicios (Rouse, 2017).</i>
Proxy	<i>Es una configuración que tiene como función autorizar las acciones controladas como límite de navegación, tráfico y tiempo en línea (CISCO, 2006).</i>
Trama	<i>Es una unidad de envío de datos que contiene una longitud máxima de tamaño de bytes (CISCO, 2006).</i>
Trunk	<i>Es una configuración de canal para puertos de switch que estén en una red Ethernet (ALEPH, 2021).</i>
VLAN	<i>Es una red virtual local la cual nos permite segmentar o distribuir el tráfico por líneas virtuales de comunicación (CISCO, 2006).</i>
WIFI	<i>Es una tecnología de red inalámbrica a través de la cual los dispositivos, como computadoras (portátiles y de escritorio), dispositivos móviles (teléfonos inteligentes y accesorios) y otros equipos (impresoras y videocámaras), pueden interactuar en Internet (CISCO, 2022).</i>
Windows	<i>Es el nombre de una familia de distribuciones de software para PC, servidores y etc.(WINDOWS, 2021).</i>

Introducción

La conexión a internet es una necesidad primordial derivada de las actividades educativas, científicas y tecnológicas, así como, la vinculación con el medio de interacción del conocimiento y las demandas del mundo actual respecto a la transformación digital y la conexión a internet de forma continua (CEPAL-UNESCO, 2020). Desde las conexiones de internet sobre los equipos de almacenamiento y publicación de sitios de internet en los centros de datos, instituciones y lugares educativos hasta las conexiones en los dispositivos móviles, ha tenido gran relevancia la protección de información en dichas conexiones. Por su alta demanda y los niveles de riesgo que circulan en Internet se han creado estrategias de seguridad informática tales como, enlaces protegidos, conexiones cifradas y otras herramientas para contener las amenazas hacia los equipos y sus sesiones al exterior. Así, las conexiones a internet a una red local (LAN) y de forma inalámbrica (WLAN) requieren mantener la seguridad de la información en su disponibilidad, integridad y confidencialidad sobre los dispositivos. Para cumplir con la conexión segura se implementó un protocolo de autenticación 802.11 (INTEL, 2021).

Control de acceso a red basada en puertos

Estándar 802.11 y seguridad de puerto

El estándar 802.11 del *Institute of Electrical and Electronics Engineers, Inc. (IEEE)* define dos tipos de autenticación a nivel de enlace: *Sistema abierto* y *Clave compartida*.

Autenticación de sistema abierto

La autenticación de sistema abierto consta de dos comunicaciones:

- a. Se envía una solicitud de autenticación desde el dispositivo móvil que contiene el ID de estación (por lo general, la dirección *MAC*).
- b. A continuación, se obtiene una respuesta de autenticación del *Ap/Router* con un mensaje de éxito o error.

802.1X es un protocolo de acceso a puertos para proteger redes mediante autenticación. Como resultado, este tipo de método de autenticación es extremadamente útil en el entorno inalámbrico (*Wi-Fi*) debido a la naturaleza del medio. Si un usuario de *Wi-Fi* se autentica a través de 802.1X para acceder a la red, se abre un puerto virtual en el punto de acceso que permite la comunicación. Si no se autoriza correctamente, no habrá ningún puerto virtual disponible y se bloquearán las comunicaciones.

Los componentes básicos en la autenticación 802.1X (Figura 1):

*Solicitante: Un cliente de software que se ejecuta en la estación de trabajo *Wi-Fi* (Figura 1).

*Autenticador: El punto de acceso *Wi-Fi* (Figura 1).

*Servidor de autenticación: Una base de datos de autenticación, normalmente un servidor *radius* como *Cisco ACS**, *Funk Steel-Belted RADIUS** o *Microsoft IAS** (Figura 1).

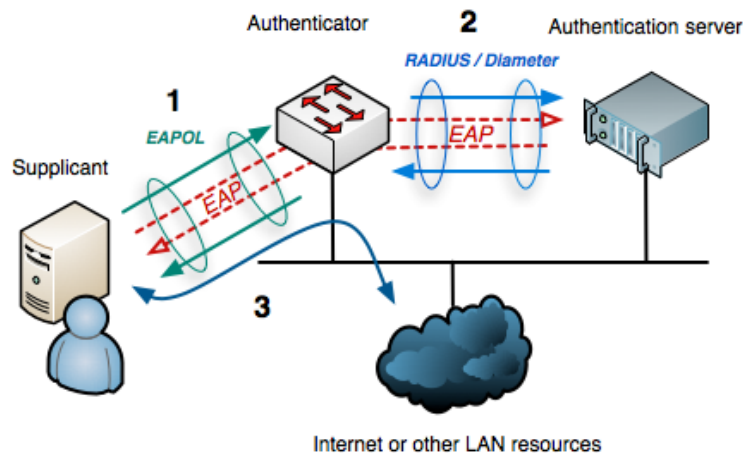


Figura 1. Conexión puerto seguro 802.11 (Perle, 2021).

Se utiliza el protocolo de autenticación ampliable (*EAP*) para pasar la información de autenticación entre el solicitante (la estación de trabajo *Wi-Fi*) y el servidor de autenticación (*Microsoft IAS* u otro). El tipo de *EAP* en realidad maneja y define la autenticación. El punto de acceso que actúa como autenticador es solo un proxy que permite la comunicación entre el solicitante y el servidor de autenticación.

Formato de Trama IEEE 802.1q

El 802.1q es el estándar IEEE para etiquetar tramas en un *trunk* y admite hasta 4096 VLAN. En 802.1q, toda conexión que requiere un medio de autenticación, en este caso alámbrico (LAN), requiere de la implementación de un dispositivo de enlace troncal que inserta una etiqueta de 4 bytes en la trama original y vuelve a calcular la secuencia de verificación de tramas (FCS) antes de que el dispositivo envíe la trama a través del enlace troncal. En el extremo de recepción, se quita la etiqueta y se reenvía la trama a la VLAN asignada. 802.1q no etiqueta tramas en la VLAN nativa, para poder lograr la conexión y la identificación de usuario hacia el sistema central de red, para otorgar la autenticación del usuario y el servicio de la red hacia internet (CISCO, 2006).

La conexión de red de área local o LAN estará asociada a una conexión 802.1q para segmentar el tráfico de datos por usuario, es por esta configuración y administración de usuarios en la red local, que se requiere contar con una guía de implementación auxiliar para la identificación de usuarios en sus conexiones a la red en un instituto, con el fin de preservar la seguridad del puerto y hacia el enlace de internet.

En este manual se establecen los procedimientos de configuración de una conexión LAN y WLAN en un equipo con sistema operativo Windows para todo usuario que requiera la conexión a internet dentro de la red local de forma correcta y segura en el instituto.

Especificaciones

1. Guía de configuración para el protocolo de autenticación 802.11x en Windows

En Windows el servicio de autenticación 802.11x esta desactivado por defecto lo que será necesario iniciarlo y configurar su ejecución automática para realizar la conexión a la red correctamente.

- a. En el equipo a configurar, mediante la combinación de teclas Windows + R abriremos una ventana como la que se muestra a continuación (Figura 2). En el cuadro de texto escribiremos el comando **services.msc** y después clic en aceptar.

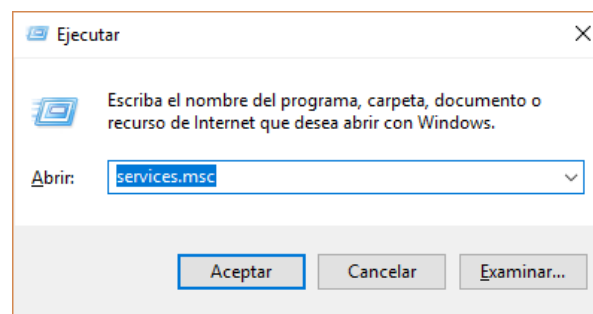


Figura 2. Servicios de Windows. Elaboración propia.

- b. Se abrirá el administrador de servicios de Windows, en la lista desplegada de servicios buscaremos: **“Configuración automática de redes cableadas”** (Figura 3).

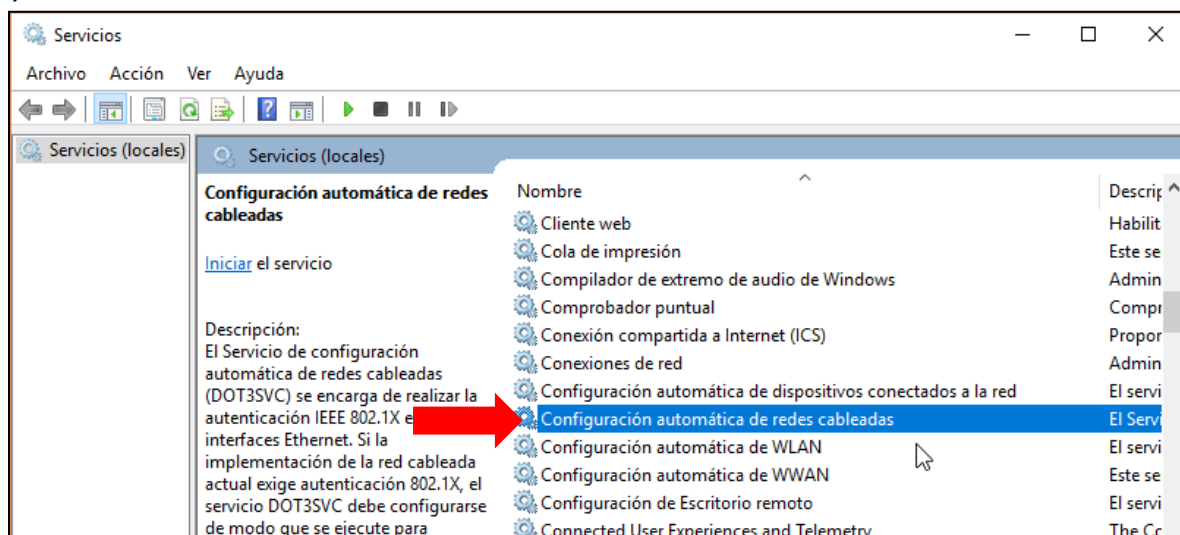


Figura 3. Servicio de redes cableadas (DOT3SCV). Elaboración propia.

- c. Daremos doble clic en él para abrir las opciones de configuración y en la sección **Tipo de inicio** seleccionaremos **Automático**.

A continuación, daremos clic en el botón **Iniciar**, después en el botón **Aplicar** y a continuación en **Aceptar** para finalizar (Figura 4).

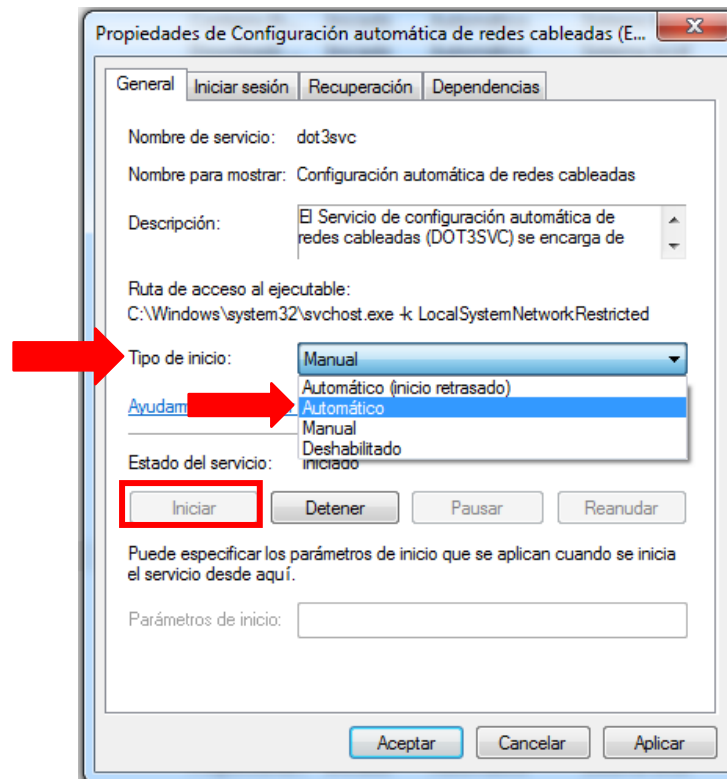


Figura 4. Propiedades de configuración automática. Elaboración propia.

- d. Ahora teclearemos nuevamente **Windows + R**, y Ejecutamos el comando **ncpa.cpl** y damos clic en Aceptar.

Se abrirá el administrador de conexiones de red, buscaremos el adaptador correspondiente a la red cableada/ethernet que estamos configurando. Daremos clic derecho sobre el ícono de **Conexión de área local/Ethernet**, y después en **Propiedades** (Figura 5).

Nota: Aquellos adaptadores que no están en uso aparecerán con una X roja en la parte inferior izquierda del icono.

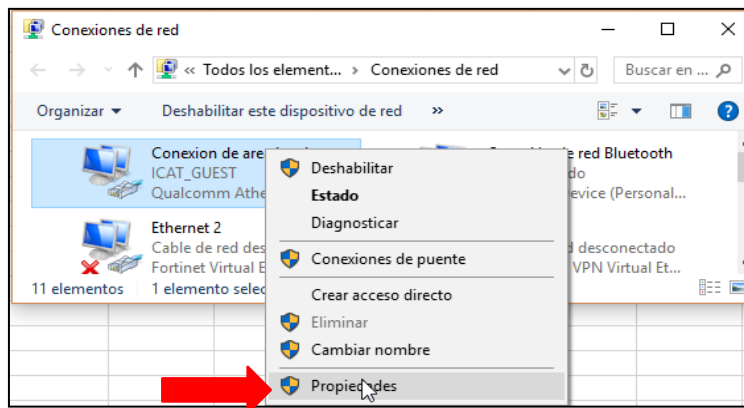


Figura 5. Adaptadores de conexión de red. Elaboración propia.

- e. En la pestaña **Funciones de red** verificaremos que este habilitado el **protocolo de internet versión 4 (TCP/IPv4)**
 Al finalizar daremos doble clic sobre **Habilitar el protocolo de internet versión 4 (TCP/IPv4)** para abrir la ventana de propiedades (Figura 5).

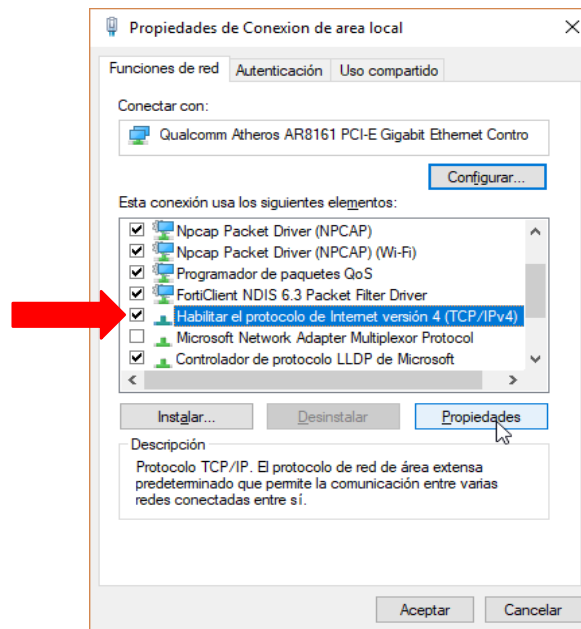


Figura 6. Propiedad de conexión Ipv4. Elaboración propia.

- f. En la pestaña **General** verificaremos que estén habilitadas las opciones **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente** como se muestra en la siguiente imagen y daremos clic en **Aceptar** (Figura 7).

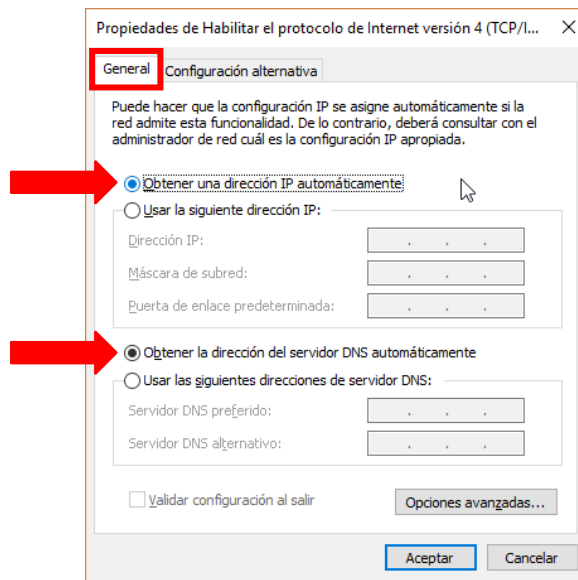


Figura 7. Configuración de protocolo de Ipv4. Elaboración propia.

- g. De nuevo en la ventana anterior, **Propiedades de Conexión de área local**, en la pestaña **Autenticación** activaremos las casillas **Habilitar la autenticación de IEEE 802.1X** y **Recordar mis credenciales para esta conexión cada vez que inicie sesión** (Figura 8).

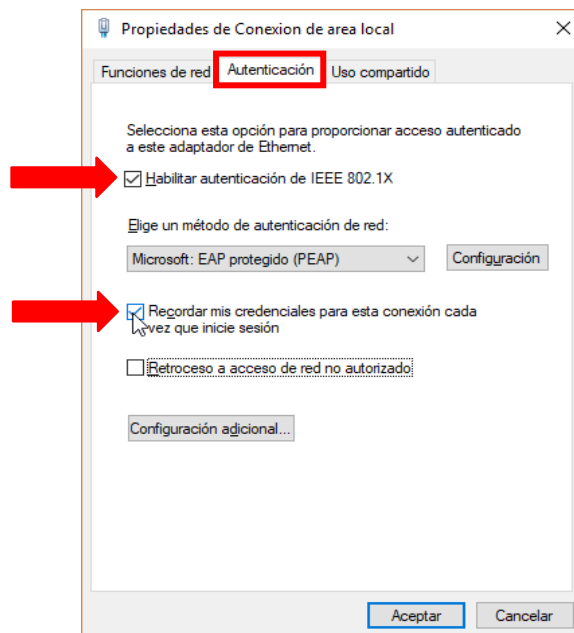


Figura 8. Configuración de la autenticación IEE 802.1x. Elaboración propia.

- h. A continuación, daremos clic en el botón **Configuración**, donde desactivaremos la casilla **Verificar la identidad del servidor validando el certificado**. En la opción **Seleccione el método de autenticación** seleccionaremos **Contraseña segura (EAP-MSCHAP v2)** y activaremos la casilla **Habilitar reconexión rápida**.

Después daremos clic en el botón **Configurar** (Figura 9).

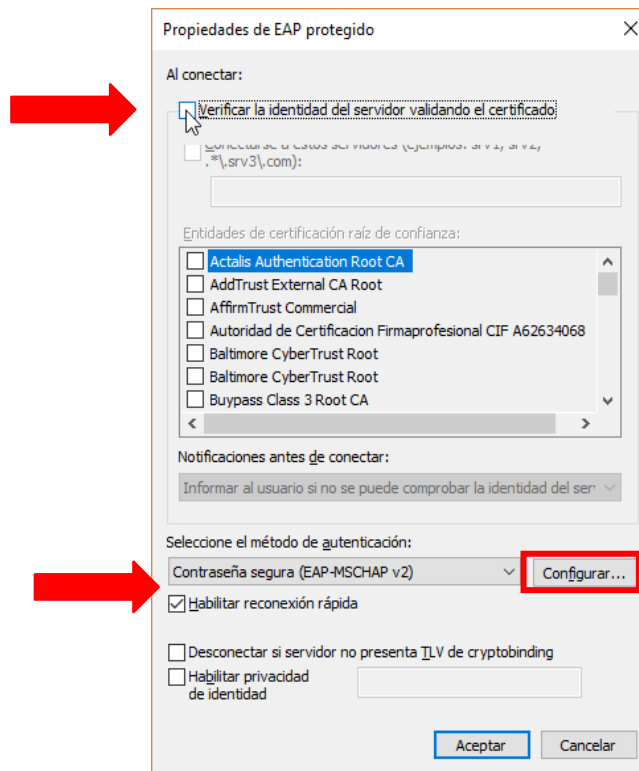


Figura 9. Configuración de protección de autenticación. Elaboración propia.

- i. En la siguiente ventana validaremos que esté desactivada la opción **Usar automáticamente mi nombre de inicio de sesión y contraseña de Windows (y dominio, si lo hay)** y Aceptar (Figura 10).

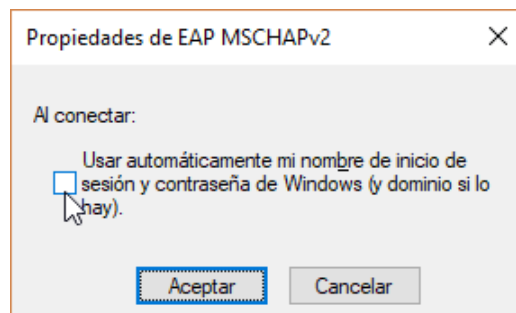


Figura 10. Inicio de sesión deshabilitado. Elaboración propia.

- j. Aparecerá una ventana de inicio de sesión donde ingresaremos el **usuario** y la **contraseña de red** personales asignados por la Unidad de Cómputo y daremos clic en **Aceptar** (Figura 11).

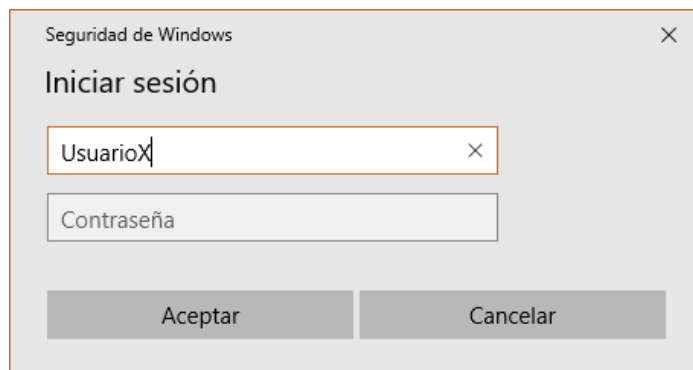


Figura 11. Autenticación de red. Elaboración propia.

Finalmente, si los datos fueron ingresados correctamente podremos observar que la conexión a la red **Conectado** (Figura 12) se ha realizado de manera exitosa.

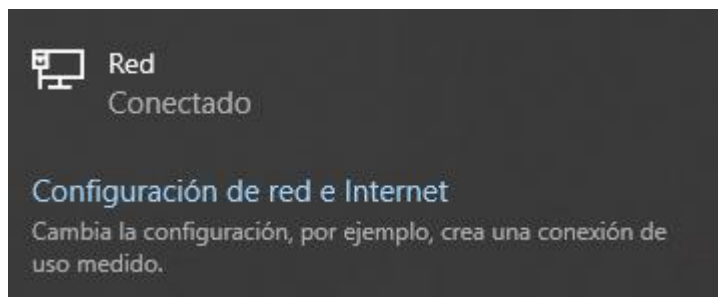


Figura 12. Equipo en conexión. Elaboración propia.

Nota: Para poder navegar de manera segura e ininterrumpida por internet, será necesario instalar el certificado de navegación segura, vea la **Guía de instalación del certificado web en Windows**.

2. Guía de conexión WiFi con el protocolo 802.11x en Windows

A continuación, se presenta el procedimiento a seguir para la implementación de los procesos para la instalación y configuración de la conexión WiFi sobre equipos con sistema operativo Windows.

- a. En la barra de tareas del sistema operativo. Localizar el icono de red (Figura 13), dar clic derecho para ver el listado de redes inalámbricas disponibles.

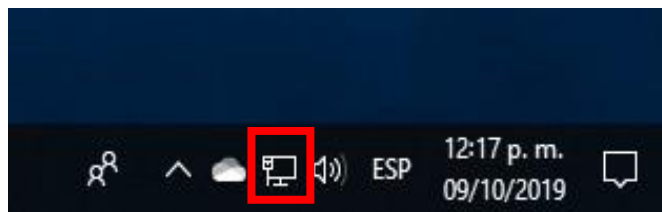


Figura 13. Icono de red. Elaboración propia.

- b. Conectarse a la red inalámbrica con el nombre SSID: ICAT, dar clic en la opción **Conectar automáticamente** y a continuación en el botón **Conectar** (Figura 14).

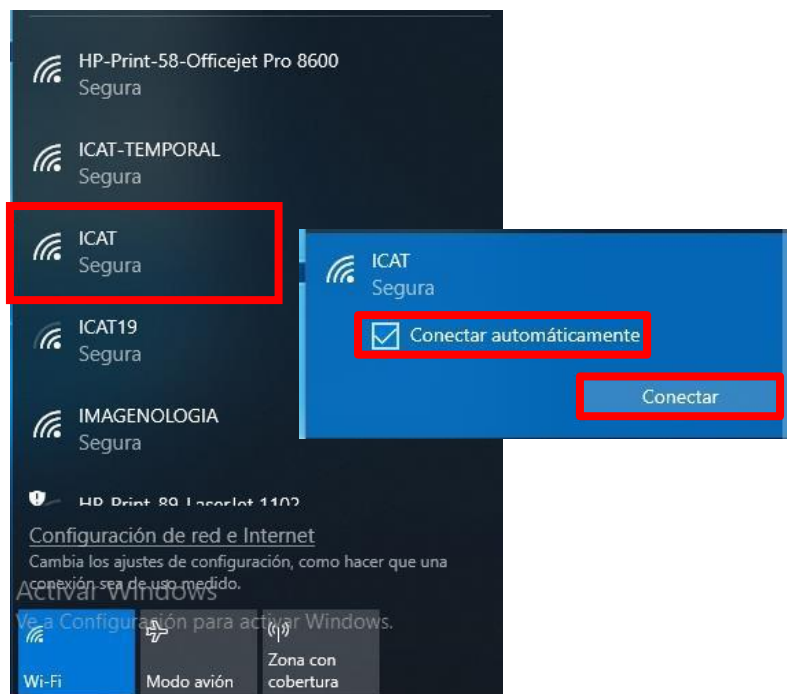


Figura 14. Conexión con SSID ICAT. Elaboración propia.

- c. Ingrese la siguiente clave de seguridad: **A5*#1UeqT8** y de clic en siguiente (Figura 15).



Figura 15. Clave de autenticación en ICAT. Elaboración propia.

- d. La conexión invocará un navegador de internet con un portal de autenticación, el cual se muestra en la siguiente imagen (Figura 16).
A continuación, se deberá ingresar su nombre de **usuario y contraseña**, de clic en las opciones **Acepto las condiciones de Uso** y **Recuérdame**, finalmente de clic en **Conectar**.

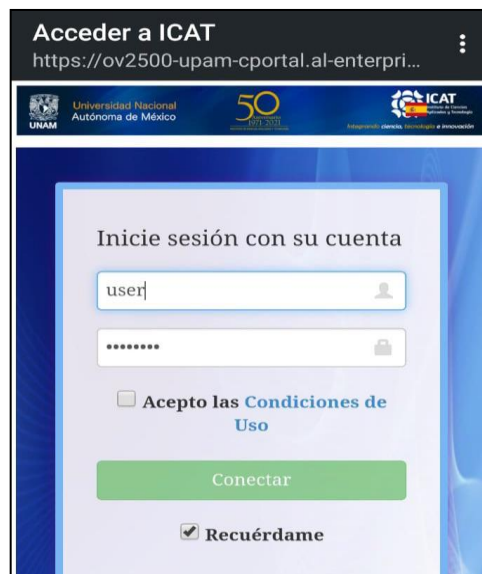


Figura 16. Acceso a la red por usuario y contraseña. Elaboración propia.

- e. Si los datos fueron ingresados correctamente, se mostrará un mensaje de **Login correcto** indicando que ya se dispone de acceso a la red (Figura 17).

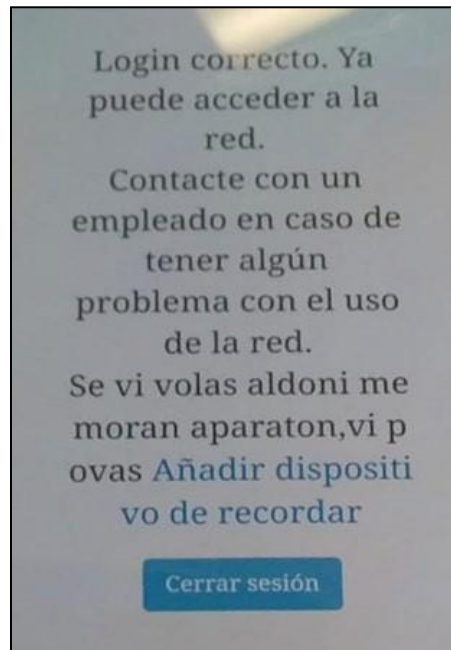


Figura 17. Autenticación exitosa. Elaboración propia.

Finalmente, si los datos fueron ingresados correctamente podremos observar que la conexión a la red se ha realizado exitosa y con estatus de **Conectada** (Figura 18).

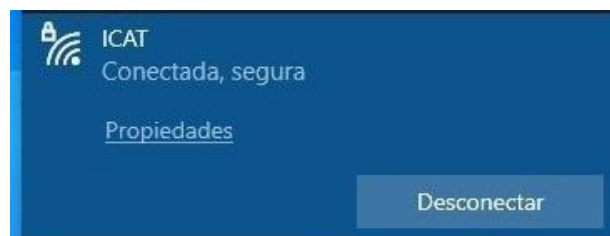


Figura 18. Conexión ICAT. Elaboración propia.

Nota: Para poder navegar de manera segura e ininterrumpida por internet, será necesario instalar el certificado de navegación segura, vea la **Guía de instalación del certificado web**.

3. Guía de conexión *WiFi* usuario Visitante con el protocolo 802.11x en *Windows*

A continuación, se presenta el procedimiento a seguir para la implementación de los procesos para la instalación y configuración de la conexión *WiFi* usuario Visitante sobre equipos con sistema operativo *Windows*.

- a. En la barra de tareas del sistema operativo. Localizar el icono de red (Figura 19), dar clic derecho para ver el listado de redes inalámbricas disponibles.

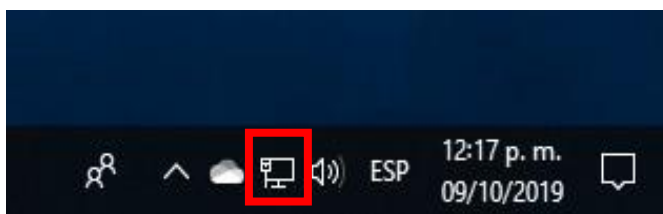


Figura 19. Icono de acceso a red. Elaboración propia.

- b. Conectarse a la red inalámbrica con el nombre SSID: ICAT-Visitante, dar clic en la opción **Conectar automáticamente** y no pedirá ningún dato, a continuación de clic en el botón **Conectar** (Figura 20).

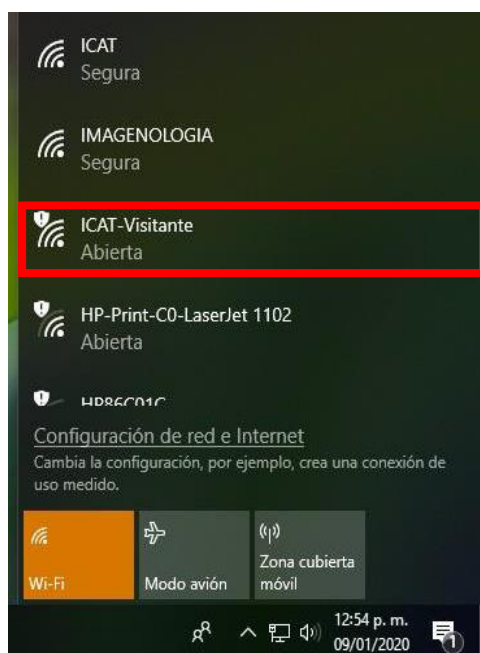


Figura 20. Conexión tipo Visitante. Elaboración propia.

- c. Enseguida la aplicación lanzará el portal que se muestra en la siguiente imagen (Figura 21).

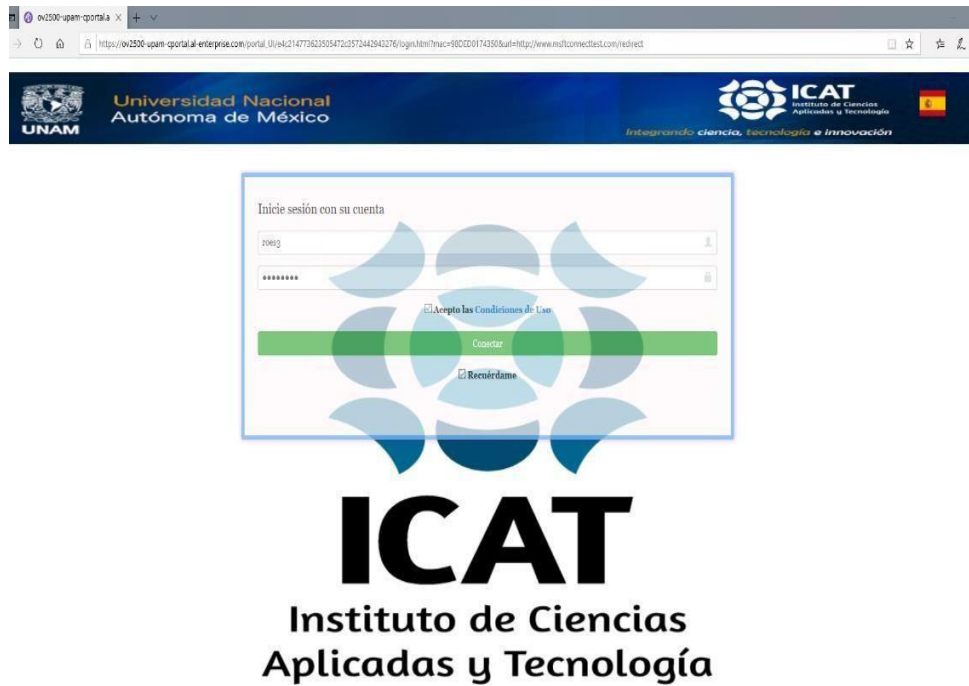


Figura 21. Portal de autenticación. Elaboración propia.

- d. Ingrese su **nombre de usuario y contraseña**, de clic en las opciones **Acepto las condiciones de Uso** (Figura 22).



Figura 22. Configuración de usuario y contraseña. Elaboración propia.

Referencias

- ALEPH, 2021. ¿Qué es un *trunk* de red?. [En línea]. Disponible desde <https://aleph.org.mx/que-es-un-trunk-en-red#:~:text=Trunk%20es%20una%20configuraci%C3%B3n%20de,m%C3%A1s%20de%20una%20VLAN.%3B%20as%C3%AD> [Fecha de recuperación 19 de enero de 2022].
- CEPAL-UNESCO, 2020. La educación en tiempos de la pandemia de COVID-19. Publicado en agosto de 2020. [En línea]. Disponible desde https://repositorio.cepal.org/bitstream/handle/11362/45904/1/S2000510_es.pdf [Fecha de recuperación 12 de enero de 2022].
- CISCO, 2006. Inter-Switch Link y Formato de Trama IEEE 802.1Q. [En línea]. Disponible desde https://www.cisco.com/c/es_mx/support/docs/lan-switching/8021q/17056-741-4.html [Fecha de recuperación 13 de enero de 2022].
- CISCO, 2022. ¿What is WIFI?. [En línea]. Disponible desde https://www.cisco.com/c/es_mx/products/wireless/what-is-wifi.html [Fecha de recuperación 19 de enero de 2022].
- INTEL, 2021. Comprender la asociación y autenticación de IEEE* 802.11. [En línea]. Disponible desde <https://www.intel.la/content/www/xl/es/support/articles/000006508/wireless/legacy-intel-wireless-products.html> [Fecha de recuperación 12 de enero de 2021].
- Perle, 2021. Control de acceso a red basada en puertos. IEEE 802.1X y seguridad de puerto. [En línea]. Disponible desde <https://www.perlesystems.es/supportfiles/port-based-network-access.shtml> [Fecha de recuperación 13 de enero de 2022].
- Rouse M., 2017. BYOD traiga su propio dispositivo. [En línea]. Disponible desde <https://www.computerweekly.com/es/definicion/BYOD-traiga-supropiodispositivo> [Fecha de recuperación 13 de enero de 2022].