DIRECCIÓN DE INNOVACIÓN,
PLANIFICACIÓN Y
NUEVAS TECNOLOGÍAS

MANUAL DE USO PARA EL FUNCIONAMIENTO PARLAMENTARIO REMOTO

AISLAMIENTO SOCIAL, PREVENTIVO Y OBLIGATORIO
CORONAVIRUS COVID-19

ÍNDICE

1. Introducción

El presente manual de usuario describe el paso a paso del funcionamiento de sesiones plenarias y reuniones de comisión telemáticas, a partir del Protocolo de Funcionamiento Parlamentario Remoto consensuado en la Comisión Especial de Modernización Parlamentaria y aprobado por unanimidad en la Comisión de Peticiones, Poderes y Reglamento de la Honorable Cámara de Diputados de la Nación.

Tanto para el desarrollo de las reuniones de comisión como para la realización de las sesiones plenarias telemáticas se utilizarán dos plataformas:

Por un lado, **una plataforma propia de la HCDN**, que permitirá la identificación del diputado/a a través del sistema de validación de identidad de RENAPER.

- Para las **reuniones de comisión** se podrá acceder a dicha plataforma ingresando a comisiones.hcdn.gob.ar.
- Para las **sesiones plenarias** se podrá acceder a la plataforma ingresando a recinto.hcdn.gob.ar. En este caso, además de acreditar la identidad y registrar la asistencia, la plataforma permite acceder a la votación.

Por otro lado, se utilizará una **plataforma de videoconferencia llamada Webex**, a través de la cual se desarrollará la interacción telemática o debate.

Luego de haber ingresado y validado su identidad en comisiones.hcdn.gob.ar o recinto.hcdn.gob.ar, según corresponda, los diputados/as podrán acceder al link de la videoconferencia, que se encontrará en el botón "Webex" de la plataforma de la HCDN.

2. Requerimientos y recomendaciones técnicas generales

Los/as Diputados deberán:

a) Utilizar la Red Virtual Privada (VPN) de la HCDN para el envío de proyectos y la participación en sesiones y reuniones de comisión telemáticas, lo cual que garantizará que la conexión se realice de forma segura. **Ver ANEXO II sobre cómo instalar la VPN.**

b) Firmar los proyectos de ley, resolución, declaración, despachos de comisión y los documentos relacionados a los mismos, a través del sistema de firma digital, siempre que los/as diputados/as cuenten con el registro de la misma.

   Aclaración: los/as diputados/as que no cuentan con la firma digital podrán realizar las actividades referidas por las otras vías previstas, hasta que gestionen el registro de su firma digital.

   La firma digital se puede gestionar en la HCDN, autoridad de registro certificada por la Oficina Nacional de Tecnologías e Información (ONTI) o en los entes habilitados en todo el país.

   El turno de generación de la firma digital en la HCDN se debe solicitar en el siguiente link: https://turnofirmadigital.hcdn.gob.ar. Los/as diputados/as que se encuentren en otras provincias, podrán tramitar su firma digital en los organismos públicos del siguiente listado, que funcionan como autoridades de registro certificadas por la ONTI:
   https://pki.jgm.gov.ar/app/Listado_de_Autoridades_de_Registro.aspx

c) Tener conocimiento de la fuente de conexión a Internet que se usará en las sesiones (es decir, si es por cable o inalámbrica) para que, en caso de inconvenientes, se pueda proporcionar esta información a la Mesa de Ayuda para una mejor asistencia.

d) Revisar que funcionen sus dispositivos electrónicos, las cámaras de video y los micrófonos, con una antelación mínima de 24 hs. antes de la reunión telemática, a fin de contar con su correcto funcionamiento.
e) Verificar el funcionamiento de la conexión a la plataforma conectándose a las sesiones telemáticas **al menos treinta (30) minutos antes** del horario pautado y recibir asistencia en caso de que sea necesario. Para revisar el estado de la conexión ingresar en el siguiente sitio: https://mediatest.ciscospark.com/.
f) Mantener la cámara encendida para verificar la asistencia de los miembros en los momentos necesarios para contabilizar el quórum, así mismo se recomienda mantenerla encendida durante todo el debate telemático.
g) Disponer de auriculares y mantener el **micrófono apagado** mientras no se esté haciendo uso de la palabra. Esto permitirá evitar ruidos de fondo durante el transcurso de la reunión.

Se recomienda a los/as Diputados/as:

a) Ingresar a la plataforma a través de una computadora que esté conectada a internet directamente por cable. De no ser posible, hacerlo con conexión inalámbrica, procurando estar lo más cerca posible del repetidor de señal. Asimismo, se recomienda ubicarse en un ambiente silencioso y con buena iluminación.
b) Evitar la conexión a internet de otros dispositivos que afecten la disponibilidad del ancho de banda.
c) Procurar que la posición y el ángulo de la cámara web utilizada para la sesión y/o reunión telemática sea lo más frontal y centrado posible.
d) Realizar consultas y solicitar asistencia en todo momento comunicándose con la **Mesa de Ayuda** a través del chat de la plataforma o telefónicamente llamando al: 011 6075-5111.

3. Presentación de proyectos

Para la presentación de proyectos de Ley, Resolución y Declaración los/as diputados/as deberán:

a) Enviar un correo electrónico desde su casilla institucional personal a la casilla de la Mesa de Entradas de la Secretaría Parlamentaria: mentradas.dsecretaria@hcdn.gob.ar.
b) Adjuntar el proyecto en formato PDF. Los documentos en PDF deberán contar con firma digital en los casos que los/las firmantes estén registrados/as.
c) Copiar a los co-firmantes, en caso de existir, en el correo electrónico.
d) La Mesa de Entradas responderá la comunicación indicando su recepción y el número del expediente asignado, tanto al autor del correo electrónico con el proyecto adjunto, como a los/as co-firmantes expresados en el envío.
e) En caso de que se copie un/a diputado/a que no es co-firmante, dicho diputado/a debe informar el error a la Mesa de Entradas en un plazo no mayor a un (1) día hábil de haber recibido dicha notificación.

4. Reunión de Comisiones Permanentes y Especiales

4.1 Convocatoria y otras acciones previas a la reunión

4.1.1 Secretarios/as de Comisión

Corresponde a los/as secretarios/as de comisión:

a) Dar aviso a las Secretarías General, Parlamentaria y a la Dirección Comisiones, previo a la convocatoria a reunión telemática, con la mayor antelación posible a fin de efectuar las gestiones correspondientes.

b) Enviar por correo electrónico la siguiente información a los/as integrantes de la comisión: día de la reunión, horario, temario (con los expedientes si

correspondiera), link y contraseña para conexión vía plataforma de videoconferencia online.

c) Gestionar la grabación de las reuniones, la transmisión en vivo y la publicación del video en la sección de la página web correspondiente a su comisión.

d) Gestionar los pedidos de acceso a las reuniones telemáticas para asesores y diputados/as que no formando parte de la comisión quieran presenciarlas.

4.2 Ingreso a la reunión de comisión telemática

Para la participación en reuniones de comisión telemáticas se recomienda a los/as diputados/as el uso de dos dispositivos; un teléfono celular para ingresar a comisiones.hcdn.gob.ar con el fin de verificar la identidad, y una computadora que deberá utilizar para poder participar en el debate durante toda la sesión telemática.

Los/as Diputados/as deberán:

a) Conectar a la red VPN (Virtual Private Network) los dispositivos electrónicos que se utilizarán para realizar la reunión de la Comisión telemática.

b) Ingresar a comisiones.hcdn.gob.ar.

c) Acceder con usuario y contraseña de red (los mismos datos de ingreso a la PC de la HCDN).

d) Acceder a la solicitud de revisión biométrica instantánea requerida por el sistema y validada con el RENAPER, a través de la toma de fotografías de los/as usuarios/as con tres variantes: rostro neutral, rostro con una mueca indicada por el sistema (sonrisa, guiño, etc.) y rostro con ojos cerrados. Para más información sobre el proceso de verificación de RENAPER ver el Anexo I al presente manual.

e) Una vez que el/la diputado/a se conecte a través de la VPN, ingrese con usuario y contraseña de red y certifique identidad con el sistema de datos

biométricos de ReNaPer, podrá acceder a las credenciales para ingresar a la reunión por videoconferencia (link, ID y contraseña), que se brindará en la aplicación y, recién en ese momento, a través del correo institucional. Dicha información es privada, de uso personal y no debe ser retransmitida.

f) Ingresar a la plataforma con nombre y apellido completo y dirección de correo electrónico institucional.

g) Introducir contraseña privada.

h) Al introducir la contraseña ingresarán a la "sala de espera", donde deberán verificar el funcionamiento del audio y cámara de video. Luego de verificar, deben apretar "Entrar en la reunión".

4.3 Acreditación y registro de asistencia

a) Para contabilizar el quórum de la reunión se tomarán en cuenta los/as diputados/as conectados/as en la plataforma, con video encendido y será registrado por el/la Secretario/a de la comisión convocante.

b) Si un/a diputado/a ingresa a la reunión de comisión con posterioridad al plazo indicado en el punto a) del presente apartado, el/la Secretario/a de comisión lo hará saber a viva voz, con el fin de que todos sus integrantes se encuentren en pleno conocimiento de la cantidad de asistentes.

4.4 Uso de la palabra

a) La palabra será concedida a los/as diputados/as de conformidad con el reglamento de la HCDN.

4.5 Dictámenes y despacho de comisiones

a) Los dictámenes podrán ser firmados conforme al procedimiento previsto en el punto 3 del presente manual de uso para funcionamiento parlamentario remoto. Los/as diputados/as que aún no tengan registrada su firma digital deberán además enunciar a viva voz, durante la reunión de comisiones, su acompañamiento al despacho.
b) Hasta tanto culmine el registro de firma digital de los/as diputados/as, los/as presidentes deberán consignar los/as diputados/as adherentes a cada dictamen y deberán copiar las direcciones de correo electrónico institucionales de dichos adherentes al momento del envío.
c) Los despachos de comisión deberán ser enviados por el/la Presidente/a de la comisión, con la asistencia del/la Secretario/a, en formato PDF, a la casilla de correo institucional de la Dirección Comisiones: dcomisiones@hcdn.gob.ar.
d) Una vez visado el expediente, la Dirección Comisiones procederá a su despacho dándole ingreso a la Mesa de Entradas de la Dirección Secretaría.
e) Los despachos recibidos y registrados por Mesa de entradas de Dirección Secretaría serán numerados correlativamente en el orden de su presentación y publicados como Orden del día por la Dirección Comisiones en el sitio web de la HCDN, a los efectos previstos en el art. 113 del Reglamento de la HCDN.

5. Sesiones

5.1 Convocatoria y otras acciones previas a la sesión

Secretarías

Corresponde a las Secretarías:

a) Enviar, desde una casilla de correo oficial de la Secretaría Parlamentaria a los correos institucionales de los/as diputados/as, la convocatoria a sesión telemática indicando día de la sesión, horario, orden del día y asuntos entrados.

b) Garantizar la publicación de la orden del día y asuntos entrados en el sitio web de la HCDN.

c) Enviar por correo electrónico, dos (2) horas antes del horario pautado para sesionar, el link de la convocatoria para ingresar a la plataforma. La información deberá ser enviada desde la casilla de correo oficial de la Secretaría Parlamentaria a los correos institucionales de los/as Diputados/as.

5.2 Ingreso a la sesión telemática

Para la participación en sesiones telemáticas se recomienda a los/as diputados/as el uso de dos dispositivos; un teléfono celular para ingresar a recinto.hcdn.gob.ar con el fin de dar quórum y votar, y una computadora que deberá utilizar para poder participar en el debate durante toda la sesión telemática.

Los/as Diputados/as deberán:

a) Conectar sus dispositivos electrónicos seleccionados a la red VPN (Virtual Private Network).

b) Ingresar a recinto.hcdn.gob.ar.

c) Acceder con usuario y contraseña de red (los mismos datos de ingreso a la PC de la HCDN).

d) Acceder a la solicitud de revisión biométrica instantánea requerida por el sistema y validada con el RENAPER, a través de la toma de fotografías de los/as usuarios/as con tres variantes: rostro neutral, rostro con una mueca indicada por el sistema (sonrisa, guiño, etc.) y rostro con ojos cerrados. Para más información sobre el proceso de verificación de RENAPER ver el anexo al presente manual.

e) Una vez que se cumplan con estos pasos, en la aplicación se visualizarán los datos personales, el orden del día, el acceso a votación y el recinto virtual

donde encontrarán a los/as concurrentes a la sesión remota. Asimismo, cuando el/la diputado/a se conecte a través de la VPN, ingrese con usuario y contraseña de red y certifique identidad con el sistema de datos biométricos de ReNaPer, podrá acceder a las credenciales para ingresar a la reunión por videoconferencia (link, ID y contraseña), que se brindará en la aplicación y, recién en ese momento, a través del correo institucional. Dicha información es privada, de uso personal y no debe ser retransmitida

f) Una vez que el/la secretario/a anuncie el quórum, se dará comienzo a la sesión.

5.4 Uso de la palabra

a) La palabra será concedida a los/as diputados/as de conformidad con el reglamento de la HCDN. Sin perjuicio de ello, la Secretaría Parlamentaria habilitará, previo a cada sesión, un registro de uso de la palabra acordado por los Jefes de Bloque, en caso de ser necesario para un mejor desarrollo de la sesión telemática.

b) El/la diputado/a que asuma la representación de cada bloque deberá informar sobre los/as diputados/as que harán uso de la palabra.

c) Al iniciar la sesión se silenciarán todos los micrófonos y el presidente dará la palabra en forma ordenada.

5.5 Votación

a) Una vez que los/as diputados/as se hayan identificado en la aplicación de recinto.hcdn.gob.ar tendrán acceso al módulo de votación.

b) Antes de votar, el/la diputado/a deberá validar nuevamente su identidad con el sistema de datos biométricos del RENAPER.

c) Se deberá hacer click en el módulo "Votación" de recinto.hcdn.gob.ar, identificarse y votar AFIRMATIVO, NEGATIVO o ABSTENCIÓN.

d) En caso de tener inconvenientes con la plataforma, el/la diputado/a tendrá la posibilidad de aclarar su voto a viva voz.

e) Los/as diputados/as que quieran abstenerse de votar solicitarán la palabra al presidente a fin de requerir al cuerpo autorización para abstenerse y, una vez autorizados, procederán a votar en dicho sentido.

5.6 Mesa de ayuda

Los jefes de bloque tendrán la posibilidad de informar desperfectos técnicos en el transcurso de la sesión y ser asistidos por la Mesa de Ayuda de la HCDN (teléfono: 011 6075-5111).

En caso de existir desperfectos técnicos generalizados, el presidente evaluará la posibilidad de llamar a cuarto intermedio hasta resuelto el inconveniente. Serán consideradas válidas las deliberaciones y decisiones que hayan tenido lugar con anterioridad a ese momento.

Anexo I: Sistemas de RENAPER y ARSAT

RENAPER

Para realizar la verificación de identidad, el Registro Nacional de las Personas (RENAPER) precisa el número de DNI, el sexo (información contenida en la base de datos de la HCDN) y la fotografía (autorretrato o selfie) del usuario, la cual debe cumplir con los siguientes requisitos:

- Expresión neutra del fotografiado
- Fondo uniforme detrás del rostro
- Ausencia de anteojos
- Un plano tal que el rostro cubra la mayor proporción posible de la captura fotográfica

Con los datos enviados, el Sistema Automatizado de Identificación Biométrica (ABIS) del RENAPER realiza la verificación de identidad y devuelve como resultado un valor entre 0 y 100, donde cualquier valor superior a 60 puntos determinará que la persona fotografiada es quien dice ser. El tiempo de verificación que efectúa el sistema es de entre 3 y 5 segundos en línea.

La fotografía selfie capturada es transmitida de manera cifrada y en formato base64, junto al DNI y el sexo al centro de datos del RENAPER a través de la Interfaz de Programación de Aplicaciones (API) expuesta para tal fin.

La API recibe la fotografía, la convierte a imagen binaria y mediante el DNI y el sexo recibido, ejecuta una consulta sobre la base de datos DNI/Pasaporte de RENAPER y recopila la mejor fotografía asociada a un trámite firmado digitalmente y emitido por dicho organismo.

Luego, la API presenta ambas fotografías al monitor biométrico. El monitor ejecuta la comparación utilizando el algoritmo específico para tal fin, devuelve el resultado a la interfaz, y la interfaz arroja el resultado al requirente.

La tecnología empleada para el reconocimiento facial es una herramienta denominada 'NeoFace Watch' de la empresa NEC, implementada e integrada en la República Argentina por personal del RENAPER y reconocida por el National Institute of Standards and Technology (NIST) en sus informes oficiales (ver en referencia: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf)

La acción de verificación cuenta con un número de transacción único llamado TCN, que identifica a esta operación con fecha y hora y el resultado. Toda esta información está trazada en el sistema por lo que se puede generar un reporte cuando sea necesario.

Con respecto a la Infraestructura el RENAPER cuenta con dos Datacenters independientes que funcionan de forma sincronizada.Existen decenas de organismos estatales, Bancos Públicos y Privados que utilizan este servicio las veinticuatro horas del día, los siete días de la semana.

ARSAT

En convenio con ARSAT se realizan tests para descartar que existan vulnerabilidades en el sistema y un sistema de cifrado para garantizar la seguridad. A su vez, los datos recabados serán alojados en un data center propio con equipamiento con componentes redundantes y conectividad redundante a internet a través de dos proveedores. Como plan de contingencia, se encuentra habilitada en un segundo Data Center ubicado en ARSAT una copia del sistema, que garantizará la continuidad del funcionamiento en caso de incidentes mayores.

ARSAT provee un esquema de hosting en su Datacenter donde el personal de la HCDN administra los sistemas. Esto significa que el acceso a los datos es exclusivo del personal de la HCDN.

Anexo II: Cómo instalar la VPN

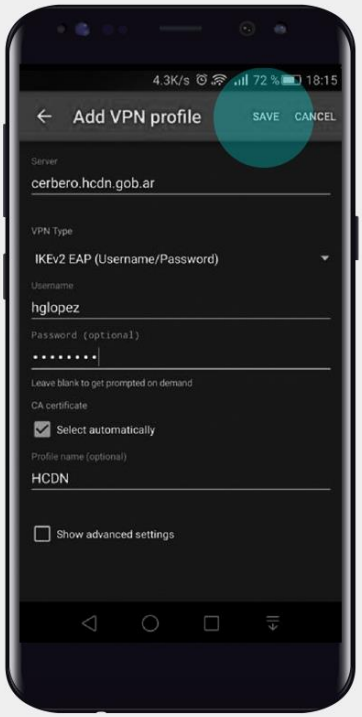
VPN | Sistema operativo ANDROID

1. Descargar StrongSwan.

•Hacer clic en el icono "**Play Store**".

•Buscar e instalar la aplicación "**StrongSwan VPN Client**".

VPN | Sistema operativo ANDROID

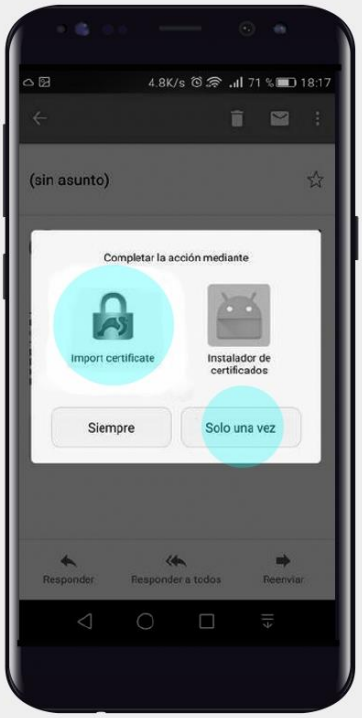


- Abrir la Aplicación **StrongSwan** y configurarla completando los siguientes campos:

- **Server**: cerbero.hcdn.gob.ar
- **VPN Type**: IKEv2 EAP
- **Username/Password**: usuario y contraseña provistos por la Dirección General de Informática y Sistemas.
- **CA certificate › Select Automatically**
- **Profile name**: HCDN
- Presionar el botón "**SAVE**"

2. Importar Certificado Digital.

- Descargar el archivo "**ca-hcdn.crt**" recibido por mail y abrirlo.
- Seleccionar la opción "**Import Certificate**".

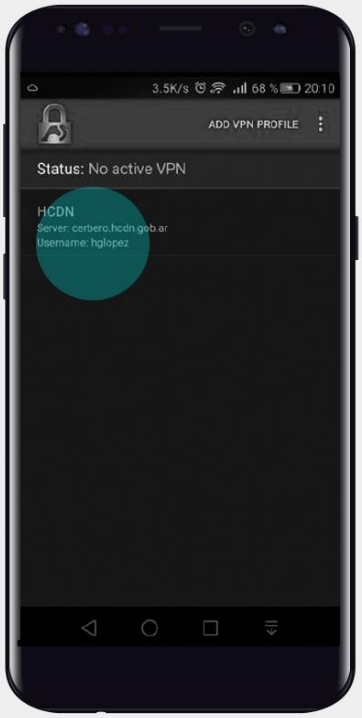


VPN | Sistema operativo ANDROID

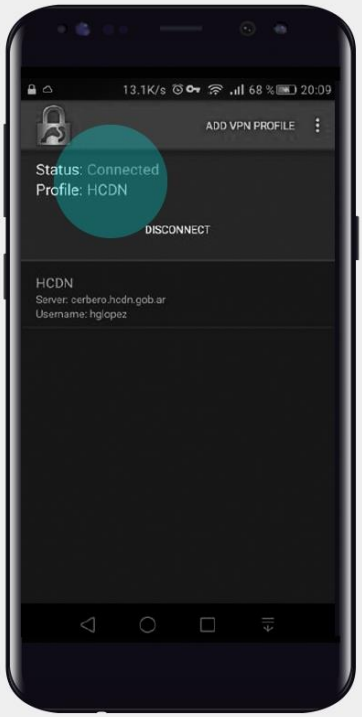
- Completar el nombre del certificado con el texto "**HCDN**" y presionar **Aceptar**.

3. Acceder a la VPN.

- Abrir la Aplicación "**StrongSwan**" y presionar la conexión "**HCDN**".



VPN | Sistema operativo ANDROID



INSTALACIÓN Y CONFIGURACIÓN DE **VPN**. ACCESO REMOTO A LA **RED DE LA HCDN**

Sistema operativo iOS

DIPUTADOS
ARGENTINA

VPN | Sistema operativo iOS

1. Configurar VPN.

Seleccionar el ícono "**Configuración**" de la pantalla principal.

- Hacer clic en "**General**"

- Hacer clic en "**VPN**"

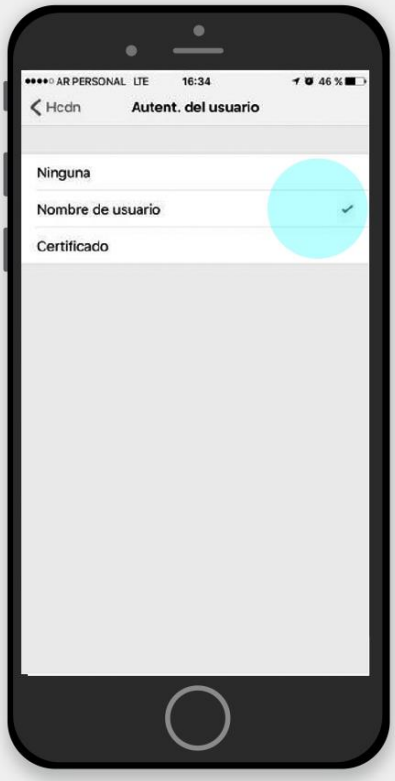
VPN | Sistema operativo iOS

- "**Agregar configuración VPN**".

- Pulsar sobre el botón **IKEv2** y completarlo con los siguientes datos:

Descripción: Hcdn
Sevidor: cerbero.hcdn.gob.ar
ID remoto: cerbero.hcdn.gob.ar
Usuario y contraseña: colocar los datos brindados por la Dirección General de Informática y Sistemas.

VPN | Sistema operativo iOS



2. Importar certificado de la HCDN.

- Descargar el archivo "**ca-hcdn.crt**" recibido por mail.
- Presionar el botón "**Permitir**".

VPN | Sistema operativo iOS

3. Activar el certificado instalado

- Seleccionar el ícono "**Configuración**" de la pantalla principal.
- Hacer clic en "**General**" › "**Perfil**" › "**186.33.210.125**" › **Instalar**.

- Volver al menú de "**Configuración**" y hacer clic en "**General**" › "**Información**" › "**Config. certificados de confianza**" y activar la opción **186.33.210.125**.

VPN | Sistema operativo iOS

- Volver al menú de "**Configuración**" y hacer clic en "**General**" › "**VPN**". **Conectar**.

INSTALACIÓN Y CONFIGURACIÓN DE **VPN**. ACCESO REMOTO A LA **RED DE LA HCDN**

Sistema operativo macOS

DIPUTADOS
ARGENTINA

VPN | Sistema operativo macOS

El siguiente procedimiento permite configurar la VPN en sistemas MAC.
Debe estar actualizado a la última versión (o posterior a la 10.15.1 macOS Catalina).

1. Instalar el certificado.

- Descargar el archivo **"ca-hcdn.crt"**.
- Seleccionar **"Abrir"** con **"KeyChain Access" y "Aceptar"**.

- Al solicitarse permisos ingresar **usuario y contraseña**.
- Seleccionar el certificado instalado con el nombre **186.33.210.125**, hacer clic en **"Confiar – Al utilizar este certificado..."**.
- Desplegar y seleccionar **"Confiar siempre" - "Aceptar"**.

VPN | Sistema operativo macOS

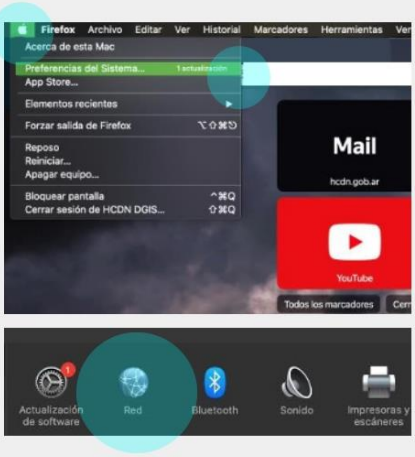
El siguiente procedimiento permite configurar la VPN en sistemas MAC.
Debe estar actualizado a la última versión (o posterior a la 10.15.1 macOS Catalina).

1. Instalar el certificado.

- Descargar el archivo **“ca-hcdn.crt”**.
- Seleccionar **“Abrir”** con **“KeyChain Access” y “Aceptar”**.

- Al solicitarse permisos ingresar **usuario y contraseña**.
- Seleccionar el certificado instalado con el nombre **186.33.210.125**, hacer clic en **“Confiar – Al utilizar este certificado...”**.
- Desplegar y seleccionar **“Confiar siempre” - “Aceptar”**.

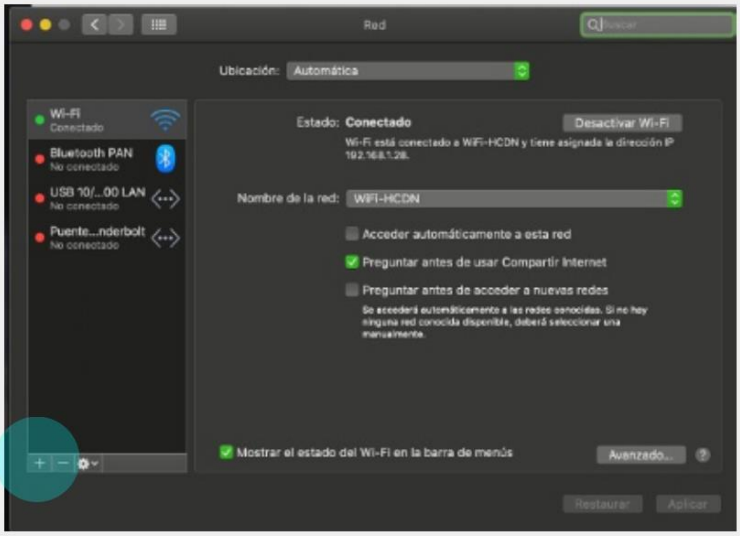
VPN | Sistema operativo macOS



2. Crear la conexión VPN.

• Seleccionar menú Apple - **"Preferencias del Sistema" – "Red".**

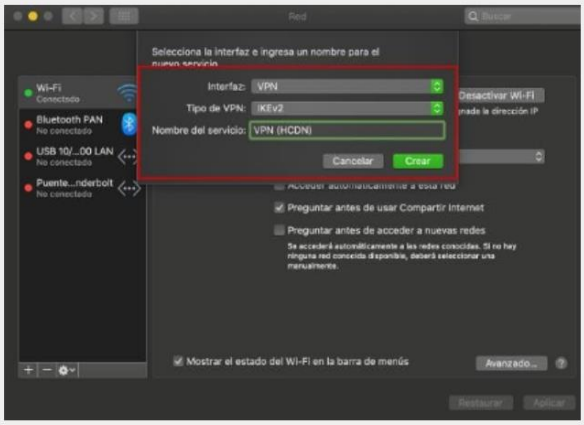
• Presionar **"+"** para agregar una conexión.



VPN | Sistema operativo macOS

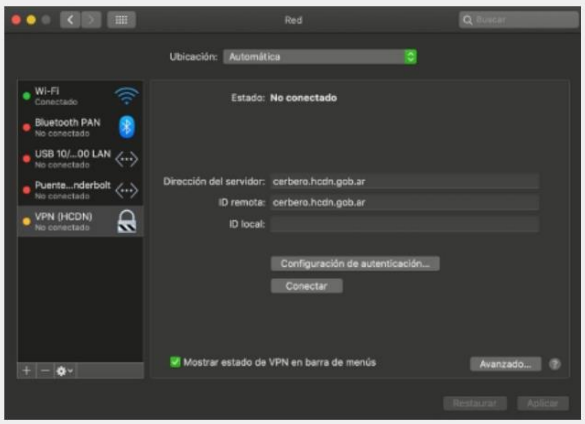
• Configurar la VPN con los siguientes datos:

INTERFAZ: **VPN**
TIPO DE VPN: **IKEV2**
NOMBRE DEL SERVICIO: **VPN (HCDN)**

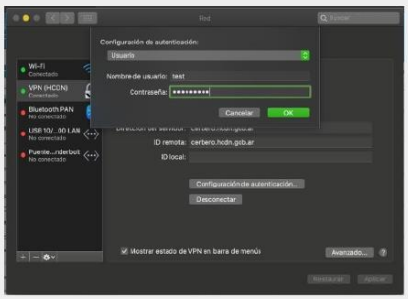


• Completar los datos como indica la imagen:

DIRECCIÓN DEL SERVIDOR: **“cerbero.hcdn.gob.ar”**
ID REMOTA: **“cerbero.hcdn.gob.ar”**



VPN | Sistema operativo macOS



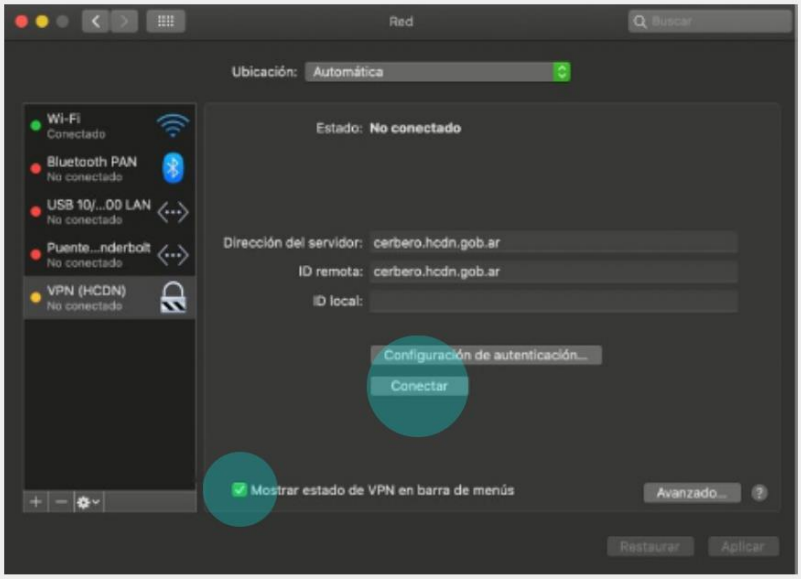
3. Configurar autenticación.

• Seleccionar **"Usuario"**.

NOMBRE DE USUARIO: completar con el usuario otorgado por la Dirección General de Informática y Sistemas, sin dominio (@hcdn.gob.ar).

CONTRASEÑA: completar con la contraseña asignada por la DGIS.

• Seleccionar **"Mostrar estado de VPN en Barra de menús"** y **"Conectar"**.



• Para verificar la correcta configuración acceder a la **intranet.hcdn.gob.ar** o aplicativos web de la Cámara.

INSTALACIÓN Y CONFIGURACIÓN DE **VPN EN WINDOWS**

Acceso remoto a la red de la HCDN

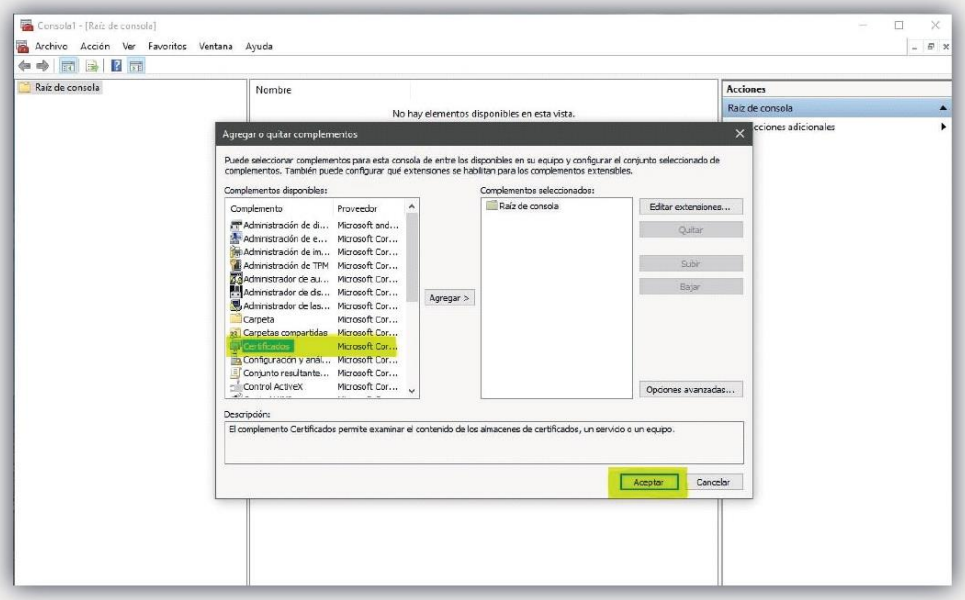
DIPUTADOS
ARGENTINA

Instalación del certificado de la CA de la HCDN

Una vez descargado el archivo "**ca-hcdn.crt**", no hacer clic en el mismo. Por favor seguir las siguientes indicaciones.

PROCEDIMIENTO:

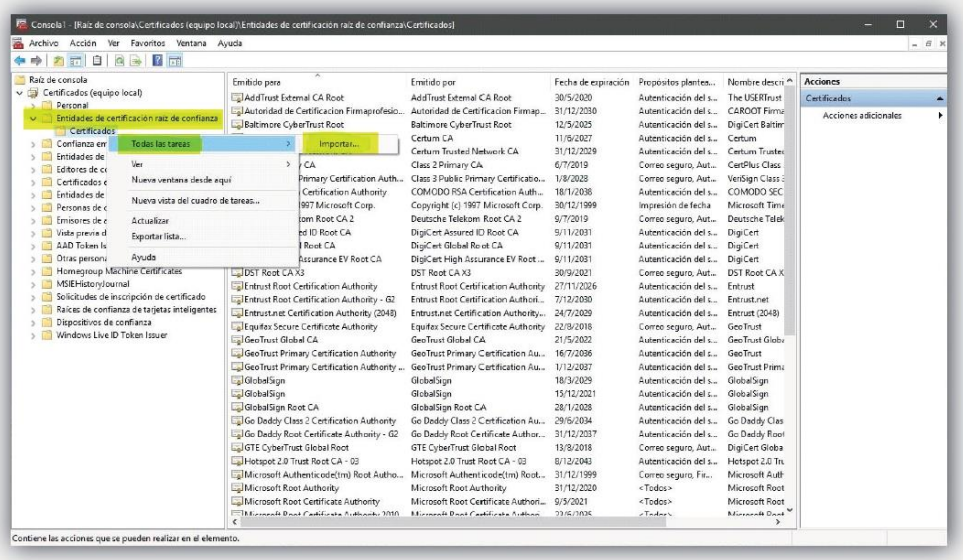
- En el teclado, pulsar el botón y la **R** al mismo tiempo.
- En la ventana emergente, ingresar "mmc" y pulsar enter.
- En la consola de Windows, seleccionar:
  - "**Archivo**" - "**Agregar o quitar complementos**" y seleccionar el complemento "**Certificados**",
  - Pulsar el botón "**Agregar**" - "**Cuenta de equipo**" - "**Siguiente**" - "**Aceptar**".



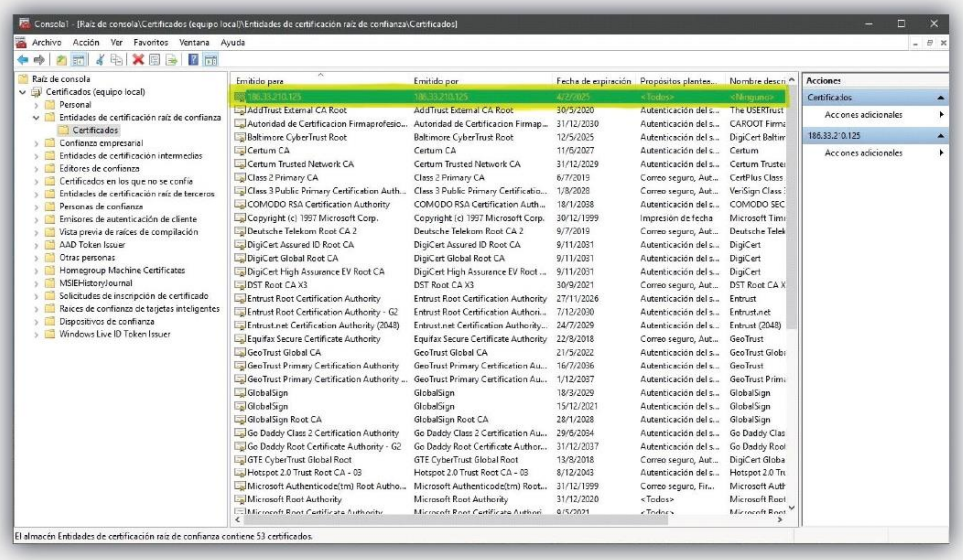
- A la izquierda de la ventana, desplegar (>), la opción "Certificados (equipo local)" y la opción "Entidades de certificación raíz de confianza".
- Hacer clic con el botón derecho en "**Certificados**" - "**Todas las tareas**" - "**Importar**".

Instalación del certificado de la CA de la HCDN

- Seleccionar el certificado ca-hcdn.crt y luego continuar con las opciones por default.



- Para verificar la instalación del certificado corroborar que se visualice el archivo con el nombre 186.33.210.125 al principio de la lista.



Configuración de la VPN en Windows

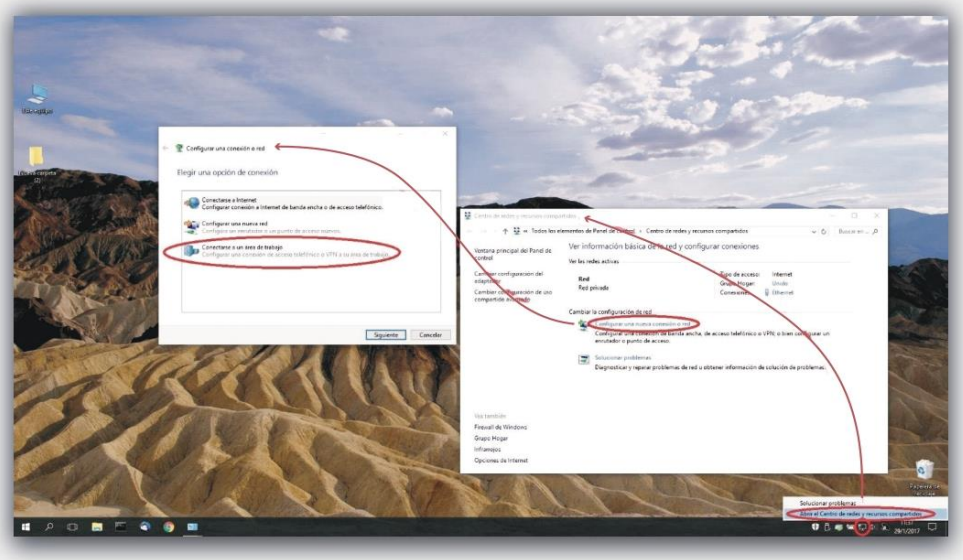
- Seleccionar el certificado ca-hcdn.crt y luego continuar con las opciones por default.

PROCEDIMIENTO:

• Hacer clic con el botón derecho de mouse en el icono de red (antena o computadora) que se encuentra en la barra inferior del escritorio, del lado derecho.

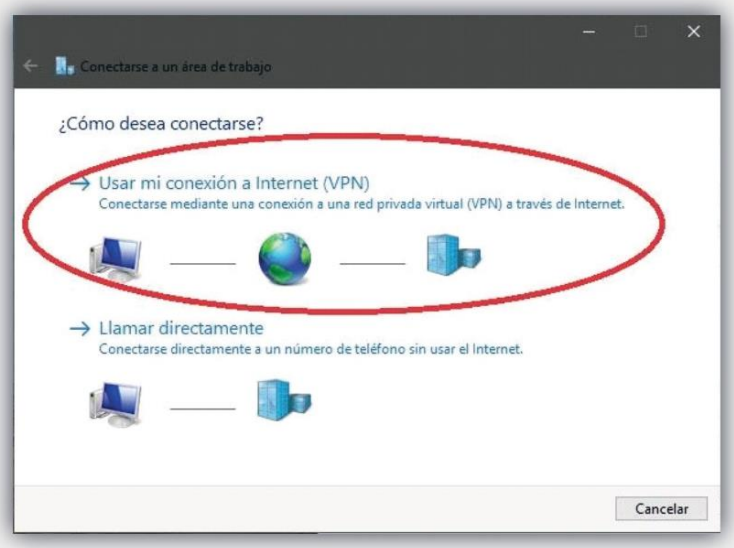
Seleccionar las siguientes opciones:

- "**Centro de redes y recursos compartidos**".
- "**Centro de redes y recursos compartidos**".
- "**Configurar una nueva conexión o red**".
- "**Conectarse a un área de trabajo**".

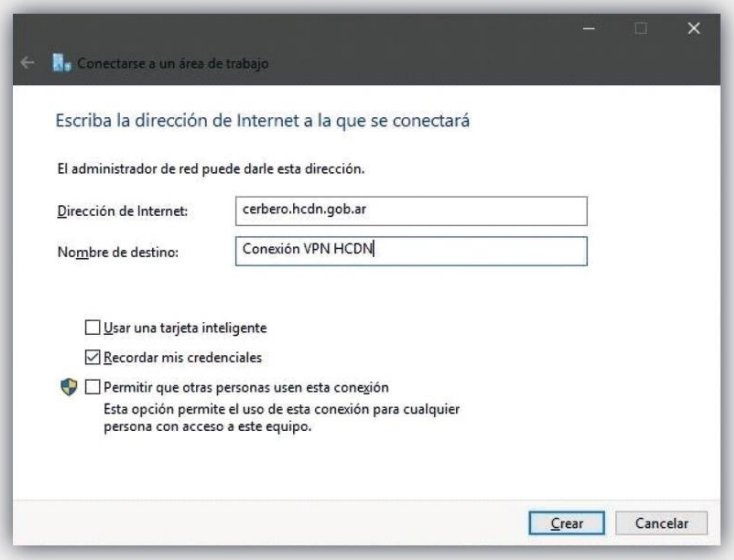


Configuración de la VPN en Windows

- "**Usar mi conexión a Internet**".



- Completar la "**Dirección de Internet**" con el nombre "**CERBERO.HCDN.GOB.AR**".
- Completar "**Nombre de destino**" con el nombre "**Conexión VPN HCDN**".
- Hacer clic en "**Crear**".



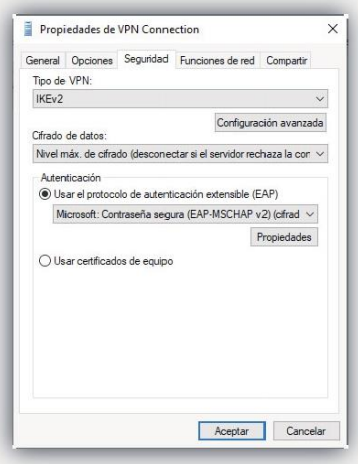
Configuración de la VPN en Windows

- Presionar el botón de inicio (primer botón en la barra inferior del escritorio a la izquierda) - "**Panel de Control**" - "**Redes e Internet**" - "**Centro de redes y recursos compartidos**" - "**Cambiar configuración del Adaptador**".

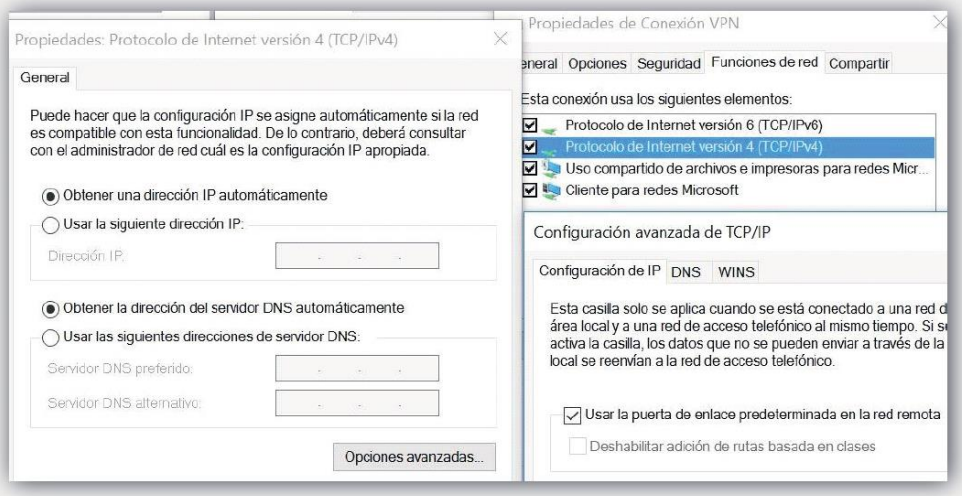
- Hacer clic con el botón derecho del mouse en "**Conexión VPN" y "Propiedades**".

Configuración de la VPN en Windows

- En la sección "**Seguridad**" configurar las opciones exactamente como se visualizan en la siguiente captura. No hacer clic en "**Aceptar**".



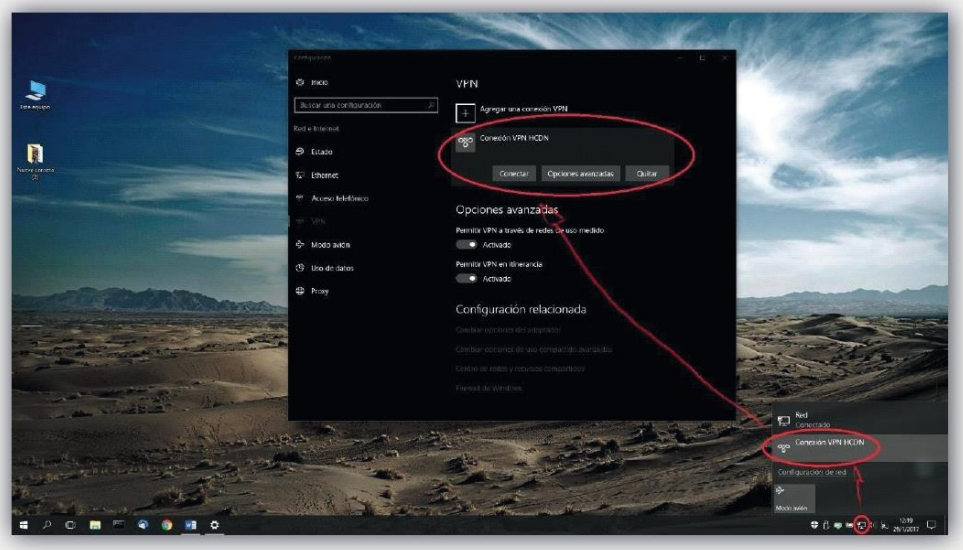
- En la solapa "**Funciones de red**", seleccionar "**Protocolo de Internet versión 4** (TCP/Ipv4)" y hacer clic en "**Propiedades**".
- En la ventana emergente, hacer clic en "**Opciones Avanzadas**".
- En la nueva ventana emergente con título "**Configuración Avanzada de TCP/IP**", seleccionar la sección "**Configuración de IP**" y tildar "**Usar la puerta de enlace predeterminada en la red remota**".
- Hacer clic en "**Aceptar**".



Configuración de la VPN en Windows

La conexión ha sido creada, solo resta conectarse.

- Hacer clic sobre el icono "**Red**" y allí seleccionar "**Conexión VPN HCDN**".



- Ingresar el usuario y contraseña brindado por la Dirección General de Informática y Sistemas. Los datos quedarán guardados, de manera tal que en las subsiguientes conexiones no serán solicitados.