Guía básica de trabajo remoto para trabajadores del Estado

Introducción

Ante el nuevo escenario generado por el coronavirus en el que la recomendación es procurar el aislamiento social, lo que implica que, en muchos casos los trabajadores no puedan asistir a sus puestos de trabajos físicos, y frente a la necesidad de no resentir las prestaciones que presta el Gobierno y los agentes continúen realizando su actividad, la DIC ha instrumentado una serie de pautas para facilitar el trabajo en casa.

Bajo esta línea, se han establecido mecanismos generales que debe seguir cada repartición para lograr la conectividad necesaria a los sistemas y archivos que cada trabajador requiere y utiliza a diario.

Recomendaciones

Sugerencias de lugar de trabajo en casa:

Es recomendable que el espacio destinado a las tareas de trabajo remoto reúna unas condiciones mínimas para garantizar el efectivo desempeño de la actividad en adecuadas condiciones de salud e higiene, con lo cual es recomendable establecer un espacio físico fijo de trabajo que reúna unas condiciones mínimas de iluminación, ventilación, ruido, clima, etc.

Sugerencias del desarrollo de la actividad de trabajo en casa:

Uno de los requerimientos más importante del teletrabajo es la conectividad domiciliaria. En tal sentido es indispensable hacer un uso racional de la red, dándole prioridad al trabajo durante las horas de actividad, en lugar de aplicaciones y usos domiciliarios tales como youtube, netflix, etc.

En lo posible hacer uso de una conexión cableada por sobre el WiFi

Según las actividades es importante que se establezcan horas de trabajo consensuada con el resto de los integrantes de su dependencia y siempre en concordancia con el normal horario de trabajo.

Comunicación efectiva:

Cuando se trabaja de forma remota, lo que debe hacer puede perderse en el texto y las cosas pueden no ser tan claras como si estuviera discutiendo una tarea en persona, lo que significa que se debe hacer un mayor esfuerzo en la comunicación en general.

Es beneficioso si puede complementar la comunicación por correo electrónico o mensaje de texto con frecuentes interacciones cara a cara (videollamada) y de voz (audio), según el tipo de discusión que tenga.

Equipamiento

La Dirección de Informática y Comunicaciones proveerá las autorizaciones y credenciales necesarias para realizar la actividad remota. El soporte e instalación de los recursos necesarios para el acceso remoto serán brindados por el área informática correspondiente a cada Dirección o Ministerio, con lo cual es muy importante tener el contacto de su referente informático.

Necesitará lo siguiente para poder completar funciones básicas fuera de su entorno de trabajo normal:

- Notebook o PC
- Acceso a internet
- Acceso remoto seguro a la red interna/intranet de gobierno (Usando VPN provista por la DIC)
- Celular
- WhatsApp

Para tener acceso a la Red Interna de Gobierno es necesario contar con las credenciales VPN otorgadas por la Dirección de Informática y Comunicaciones del Ministerio de Gobierno. La mismas deben ser solicitadas debidamente al referente informático de cada Área, Dirección o Ministerio, quien las elevará a la DIC para su autorización, en función de la disponibilidad y prioridades fijadas por las autoridades.

Para instalar y configurar la VPN en su Computadora, Notebook o Tablet siga la guía del Anexo 1. Ante cualquier duda, consulta o dificultad debe comunicarse con su referente informático para recibir soporte técnico. (Ver lista de referentes informáticos en Anexo 2)

Los referentes informáticos deberán solicitar las VPN de las personas que requieran acceso a través de CCOO con el formato de datos establecido en el Anexo 3.

Tener acceso por VPN a la red de gobierno es un comienzo, pero existen otras herramientas tecnológicas que pueden ayudar a construir una comunicación más sólida, utilizar de manera más eficiente los equipos y mejorar la organización general.

Herramientas sugeridas:

Acceso remoto a su computadora en su oficina:

- Windows Remote Desktop

Comunicación:

- Correo oficial: https://rcmail.mendoza.gov.ar/
- Chat y videollamada: Whatsapp
- Videoconferencia: Skype
- Derivación del interno al celular personal del empleado (ver Anexo 4)

Metodología de trabajo sugerida

Es muy importante que al momento de operar en modo teletrabajo las condiciones de conectividad permanezcan a plena disposición para tal efecto, en particular, se debe privilegiar el uso del ancho de banda para realizar la actividad de trabajo, tal como se explicó anteriormente.

Metodología:

La metodología de trabajo preferida para realizar teletrabajo es acceder remotamente a su PC de oficina mediante la herramienta de acceso remoto disponible. De esta forma su actividad cotidiana no sufrirá tantos cambios y será como si estuviese sentado en su oficina, podrá trabajar con sus archivos y sistemas a los cuales acostumbra utilizar. La computadora de la oficina deberá permanecer encendida. Dependiendo de la versión de sistema operativo que utilice es la configuración que debe realizar:

- Acceso remoto en Windows 10:
https://support.microsoft.com/es-us/help/4028379/windows-10-how-to-use-remote-desktop

- Acceso remoto en Windows 7:
https://support.microsoft.com/es-us/help/17463/windows-7-connect-to-another-computer-remote-desktop-connection

No se recomienda llevarse el equipamiento de oficina a su casa por diversos motivos de configuración e inconvenientes para su correcto funcionamiento fuera del espacio de trabajo normal, sin embargo en caso de fuerza mayor y que sea necesario llevar el equipamiento a su casa se deberá solicitar autorización formal al responsable de Área, Dirección o Ministerio según corresponda, quien evaluará cada caso en particular, realizará los trámites administrativos correspondientes y la entrega formal del equipo bajo su responsabilidad de cuidado y mantenimiento previa firma.

Para comunicarse se sugiere que cada oficina creé un grupo de Whatsapp entre los trabajadores que están remotos y los que están in-situ para poder establecer una comunicación efectiva y rápida, en la cual puedan hacer videollamadas y enviar audios.

En caso de perder conexión o no sea posible acceder a su escritorio remoto de la computadora ubicada en la oficina, deberá contactar con su referente informático para dar tratativa al problema. No obstante, se podrá seguir trabajando sin escritorio remoto a los sistemas, tales como Sídico Web, GDE, etc., que sean accesibles desde su navegador (IE, Firefox o Chrome) siempre y cuando la conexión VPN se mantenga activada. Recuerde que todo esto sistemas usan credenciales (usuario / clave) que son personales y es responsabilidad de cada usuario conocerlas y usarlas de manera estrictamente personal, sin darlas a conocer a terceros aunque fueran compañeros de trabajo.

Anexo 1 - Configuración OpenVPN

Para establecer la conexión de red privada virtual basada en OpenVPN, es necesario realizar lo siguiente:

1. Solicite el acceso VPN al referente de informática de su Área, Dirección o Ministerio, quien solicitará a la Dirección de Informática y Comunicaciones mediante Comunicación Oficial utilizando la planilla del Anexo 3 y dirigida a al Director de la DIC Maximiliano Jaime.

2. Una vez creada la VPN, recibirá 2 correos, uno con un archivo en formato OVPN que contiene las credenciales y un segundo mail que contiene la clave de la VPN.

3. Instalar el software OpenVPN en Windows. (para otro sistema operativo consulte con el referente informático)

   Para WINDOWS 7/8/8.1/SERVER 2012R2 se puede descargar en:
   https://swupdate.openvpn.org/community/releases/openvpn-install-2.4.8-I602-Win7.exe

   Para WINDOWS 10/SERVER 2016/SERVER 2019 se puede descargar en:
   https://swupdate.openvpn.org/community/releases/openvpn-install-2.4.8-I602-Win10.exe

   Se crea un icono en el escritorio "OpenVPN GUI" y un icontry cerca donde esta la fecha y la hora en la barra de tareas.

4. Guardar el archivo que contiene las credenciales que recibió por correo en el directorio:
   C:\Archivos de programa\OpenVPN\config

5. Para iniciar la conexión, hay que hacer click en el icono con el botón derecho y seleccionar conectar.
   a. Cuando la conexión se establece, el indicador de estado cambia de rojo a verde.
   b. Las claves solicitadas se envían en un correo separado al correo de credenciales VPN.

6. Por favor no intercambiar los distintos accesos, porque la política de acceso VPN no permite sesiones múltiples para una cuenta. Ante una nueva conexión exitosa se termina la sesión existente.

Ante cualquier duda, consulta o dificultad debe comunicarse con su referente informático para recibir soporte técnico.

Anexo 2 - Lista Referentes Informáticos

Área, Dirección o Ministerio	Referente Informático
Administración Tributaria Mendoza	Orlando Irrazabal <oirraza@mendoza.gov.ar>
	Diego Andres Garay <dagaray@mendoza.gov.ar>
	Sergio Javier Martin <sjmartin@mendoza.gov.ar>
Contaduría General de la Provincia	Gustavo Ariel Molina <gamolina@mendoza.gov.ar>
	Pablo Daniel Giraldo <pgiraldo@mendoza.gov.ar>
Dir. de Agricultura y Contingencia Climática	Leonardo Walter Insegna <linsegna@mendoza.gov.ar>
	Carlos Andres Odiard <aodiard@mendoza.gov.ar>
Dir. de Estadísticas e Investigaciones Económicas	Daniel Campeglia <dcamp@mendoza.gov.ar>
Dir. de Industria y Comercio	Ruben Achimon <rachimon@mendoza.gov.ar>
Dir. de Niñez, Adolescencia y Familia	Laura Cecilia Guinazu <lguinazu@mendoza.gov.ar>
Dir. General de Escuelas	Pablo Parola <pparola@mendoza.gov.ar>
	Javier Ibarzabal <jibarzabal@mendoza.gov.ar>
Dir. General de Informática y Comunicaciones	Maximiliano Jaime <maximilianojaime@mendoza.gov.ar>
Dir. Provincial de Ganadería	Gustavo Freire <gfreire@mendoza.gov.ar>
Dir. Transporte	Luis Alberto Gomez <luisgomez@mendoza.gov.ar>
Ente Provincial del Agua y Saneamiento	Anibal Catapano <acatapano@mendoza.gov.ar>
Ente Provincial Regulador Eléctrico	Alejandro Perissa <aperissa@epremendoza.gov.ar>
Instituto de Sanidad y Calidad Agropecuaria	Alberto Tobares <albertotobares@iscamen.com.ar>
Instituto Provincial de Juegos y Casinos	Raul Gil <raul_gil@mendoza.gov.ar>
Instituto Provincial de la Vivienda	Matías Grintal <matias@ipvmendoza.gov.ar>
Investigaciones Administrativas y Ética Pública	Alejandro Lamicela <alamicela@mendoza.gov.ar>
Min. de Cultura y Turismo	Gustavo Gabriel Almonacid <ggalmonacid@mendoza.gov.ar>
Min. de Economía y Energía	Sergio Carrizo <scarrizo@mendoza.gov.ar>
Min. de Gobierno	Rodrigo Quinteros <raquinteros@mendoza.gov.ar>
	Sebastian Nebot <snebot@mendoza.gov.ar>
Min. de Hacienda y Finanzas	Alejandro Daniel Gassull <agassull@mendoza.gov.ar>
	Dario Ruben Pais <dpais@mendoza.gov.ar>
Min. de Salud	Ricardo Federico Baigorria <rbaigorria@mendoza.gov.ar>
	Andres Torres <atorres@mendoza.gov.ar>
	Juan Alejandro Bracco <abracco@mendoza.gov.ar>
	Gerardo Fuentes <gafuentes@mendoza.gov.ar>
	Sergio E Carrion <scarrion@mendoza.gov.ar>

Min. de Seguridad	Daniel Lillo <dlillo@mendoza.gov.ar>
	Jorge Riveros <jariveros@mendoza.gov.ar>
Min. de Tierras, Ambiente y Recursos Naturales	Gustavo Acosta <gacosta@mendoza.gov.ar>
	Pablo Daniel Gandolfo <pgandolfo@mendoza.gov.ar>
Min. Desarrollo Social y Derechos Humanos	Mariano Afronti <maffronti@mendoza.gov.ar>
	Norberto Leonardo Llopiz <nllopiz@mendoza.gov.ar>
	Maria Herminia Garro <mgarro@mendoza.gov.ar>
Min. Infraestructura	Rolando Rafael Fernandez <rfernandez@mendoza.gov.ar>
	Ricardo Alejandro Yarke <ryarke@mendoza.gov.ar>
Ofic. Técnica Previsional	Jorge Ruben Fernandez <jrfernandez@mendoza.gov.ar>
Registro Civil	Diego Germán Gomez <dggomez@mendoza.gov.ar>
Servicio Penitenciario	Ruben Eduardo Dip <rubendip@mendoza.gov.ar>

Anexo 3 - Planilla Modelo para Solicitud de VPNs (uso solo de Referentes Informáticos)

Los referentes informáticos deberán solicitar las VPN de las personas que lo requieran, enviando una CCOO adjuntando la planilla modelo que debe contener los siguientes campos, en la planilla pueden agregar el listado completo de usuarios que solicitaron acceso VPN para que la solicitud sea más ágil.

Usuario: Mismo usuario de correo oficial
Nombre y Apellido: Nombres y Apellidos
CUIL: Solo los 11 dígitos sin caracteres especiales
Correo: Correo oficial
Ministerio: al cual pertenece el usuario
Oficina: a la cual pertenece el usuario
Teléfono: Interno o Celular del usuario
Responsable Pedido: responsable informático que realiza el pedido
Correo responsable del pedido: del responsable informático que realiza el pedido
Sistemas, servidores o IPs a acceder: IP de LAN del Usuario y Accesos Especiales
Observaciones: Indicar prioridad **URGENTE - ALTA - BAJA**

Planilla Modelo: http://www.mendoza.gov.ar/dic/Lista_VPNs.xls

Anexo 4 - Derivación del interno al celular personal del empleado

Para redirigir la llamadas de un teléfono fijo interno a un número de celular, debe ingresar en el teléfono fijo el siguiente código:

***22#0 seguido del número celular sin 261 y con el 15 y finalmente #**

Ejemplo para el celular 151234567 el código a ingresar en el teléfono interno será:

*22#0151234568#

Para anular el cambio realizado, solo se debe ingresar el código **#22#**