DIRECCIÓN GENERAL DE MANTENIMIENTO TÉCNICO
SECRETARÍA DE ECONOMÍA, FINANZAS Y CONTROL DE GESTIÓN
MUNICIPALIDAD DE COMODORO RIVADAVIA

Para poder brindar asistencia remota a los equipos del municipio contamos con una herramienta segura y estandarizada para que el personal de soporte pueda acceder a su equipo como si estuvieran en la oficina.

PRECAUCIONES PARA REFORZAR LA SEGURIDAD

Aunque las personas corrientes no pueden blindarse a las malas intenciones de los piratas informáticos, sí existen algunos consejos prácticos que te ayudarán a proteger mejor el equipo y la información contenida en tus cuentas virtuales.

Estas son las 5 reglas de oro para evitar ser víctima de un ciberataque:

1. **Reforzar las contraseñas:** Aunque es el "abc" de la seguridad informática, uno de los errores más frecuentes entre los usuarios es el de utilizar siempre la misma contraseña en todos los accesos o contraseñas demasiado cortas y simples. Para proteger nuestra información de forma correcta y efectiva es conveniente utilizar contraseñas propias y extensas, como oraciones que sean fáciles de memorizar y distintas para cada acceso, con letras mayúsculas y minúsculas, números y símbolos. También puede resultar muy útil utilizar un administrador de contraseñas, pero nunca guardes en el ordenador un "documento de passwords".

2. **No abrir links ni archivos adjuntos ZIP:** En un gran número de casos, los hackers llevan a cabo sus ataques informáticos mediante links maliciosos y archivos ZIP que mandan a los usuarios por correo electrónico. Para ello, emplean nombres de dominio muy parecidos a los de los grandes proveedores de servicios, como compañías de gas, teléfono o banco; integran links en páginas de contenido en Internet, y mandan emails falsos con textos confusos acerca de novedades, impagos, premios y/o otros.
   Antes de proceder a descargar cualquier archivo adjunto –especialmente si es ZIP- recibido por email o hacer click en un link, es muy importante asegurar la procedencia del correo (ver, en efecto, si el dominio está bien escrito y coincide con el de la página web de la empresa) y examinar toda la información del link sin hacer click (ver, por ejemplo, si la dirección que aparece en forma de pop-up coincide con el texto del link).

3. **Instalar actualizaciones del sistema operativo:** Para mantener el equipo de casa a salvo, también es muy recomendable instalar las actualizaciones del sistema pertinentes. Todos los sistemas operativos –Windows, Mac y Linux son los más conocidos- publican de forma periódica actualizaciones de sus versiones que mejoran el producto y lo hacen más seguro, gracias al trabajo de sus desarrolladores. Lo mismo sucede con el software.

4. **Confiar en los certificados de seguridad:** Los certificados de seguridad son garantía de que sitio web que visitamos o el software que queremos descargar son seguros. Cuando visitamos una

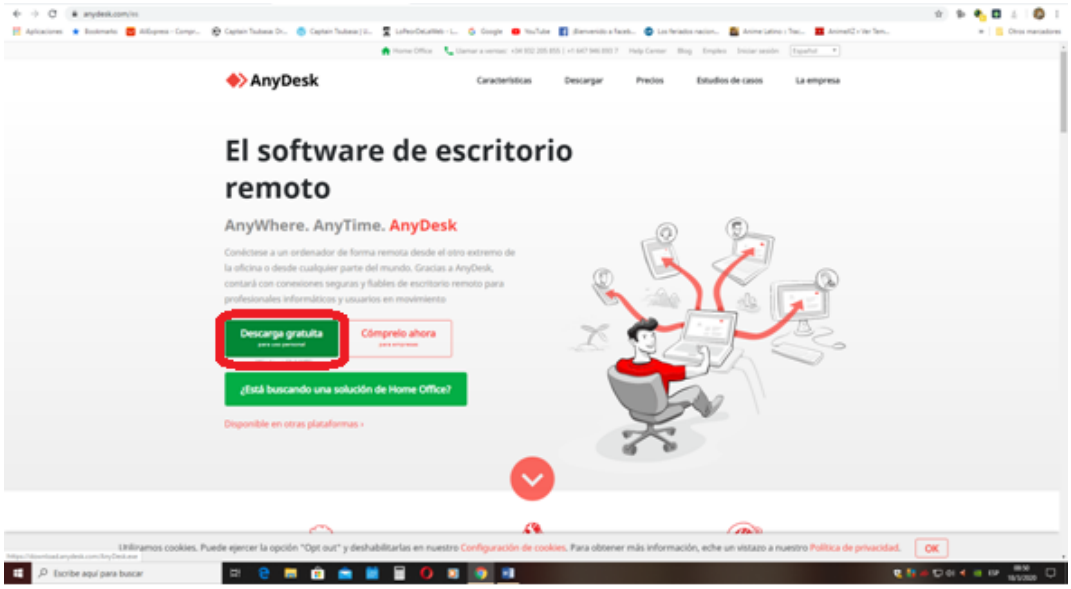
página web con certificado de seguridad, aparece un icono de candado en la barra del explorador. Este símbolo indica que la página web está certificada por un organismo regulador y es 100% segura, porque los datos de la conexión están cifrados y es casi imposible que sean interceptados por un tercero. Confiar solo en los sitios web que cuentan con certificados de seguridad es una de las medidas más efectivas para prevenirnos de acciones no deseadas y es especialmente recomendable en aquellos usuarios que navegan muy a menudo por Internet.

5. **Utilizar un software de escritorio remoto seguro:** Cuando se accede de forma remota a otros dispositivos (el ordenador del trabajo, por ejemplo), la cuestión de la seguridad tiene una importancia, si cabe, mayor. Para incrementar los niveles de seguridad, es necesario comprobar detalladamente las cuestiones técnicas en cuanto a seguridad descritas por el proveedor de tu herramienta de escritorio remoto y no hacer caso de falsas promesas publicitarias. Una encriptación permanente, basada en un protocolo estándar como, por ejemplo, el TLS -que se utiliza también para la banca online- o un procedimiento de autenticación -como el que emplea AnyDesk- que inhiba el acceso de terceros son imprescindibles para realizar una conexión remota segura.

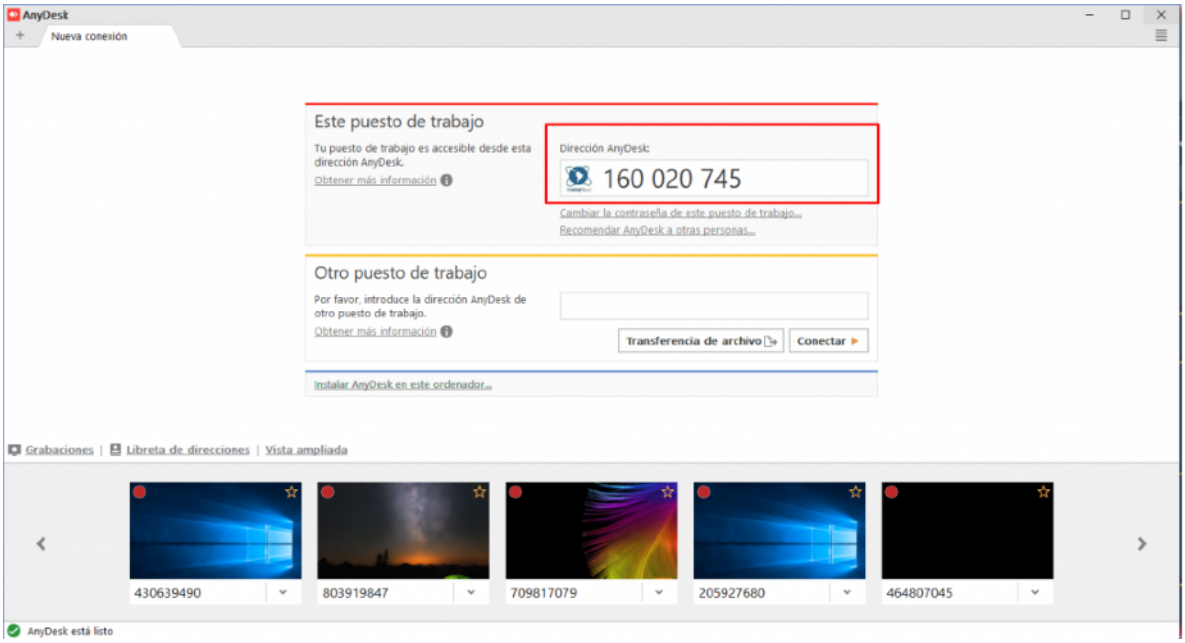
INSTRUCTIVO DE INSTALACIÓN DE ANYDESK

Tan sólo debemos descargar e instalar el programa AnyDesk en el dispositivo remoto (Oficina).

El enlace de descarga es este: **https://anydesk.com/es**



Una vez instalado se deberá se obtendrá la dirección AnyDeskAddress generada automáticamente por el equipo remoto (Oficina). En este caso el 160 020 745 es el número que arroja en pantalla el sistema que está instalado en la PC de la Oficina dentro del municipio.


AnyDesk
Nueva conexión
Este puesto de trabajo
Tu puesto de trabajo es accesible desde esta dirección AnyDesk.
Obtener más información
Dirección AnyDesk:
160 020 745
Cambiar la contraseña de este puesto de trabajo...
Recomendar AnyDesk a otras personas...
Otro puesto de trabajo
Por favor, introduce la dirección AnyDesk de otro puesto de trabajo.
Obtener más información
Transferencia de archivo
Conectar
Instalar AnyDesk en este ordenador...
Grabaciones | Libreta de direcciones | Vista ampliada
430639490
803919847
709817079
205927680
464807045
AnyDesk está listo