

Pon a punto tu dispositivo para trabajar con el teletrabajo



Debido a la situación que estamos viviendo en España, muchos ciudadanos están trabajando desde sus casas mientras dure este periodo y se consiga poner freno a la expansión del coronavirus Covid-19

Por esta circunstancia, ponemos a tu disposición una serie de recursos que hoy, más que nunca, toman especial relevancia debido a que el teletrabajo conlleva una serie de riesgos que deberíamos minimizar.

Si la empresa te facilita los recursos necesarios para el teletrabajo, **sigue sus instrucciones al pie de la letra** realizando un uso exclusivamente profesional de los portátiles o cualquier otro dispositivo tecnológico facilitado. No recomendamos, bajo ninguna circunstancia, manipularlos, modificar sus configuraciones, fijadas por el equipo informático de la empresa, o prestárselos a otras personas.

Por el contrario, si vas a utilizar un dispositivo personal para desempeñar tus funciones laborales, es de vital importancia que sigas los siguientes consejos:

- Separa tu área personal del área de trabajo. Mantener cierto orden en tu ordenador es fundamental, como lo harías en tu despacho. Procura no mezclar documentos y archivos personales con los de tu desempeño laboral, creando cuentas de usuario diferentes. Más información en: [Haz uso de cuentas de usuario](#). Además, puedes utilizar un disco duro externo

Pon a punto tu dispositivo para trabajar con el teletrabajo

para almacenar toda la información relativa al trabajo y no te olvides de realizar copias de seguridad.

- Actualiza el sistema y pon al día tu antivirus. Es un buen momento para dedicar unos minutos a la salud de tus dispositivos. Realiza todas las actualizaciones que tengas pendientes y haz una revisión con el antivirus, estarás creando una barrera más fuerte contra posibles amenazas.
- Extrema la precaución al usar memorias USB o descargar archivos. No te confíes, tu espacio de trabajo contiene información de clientes, proveedores, contactos..... además de tus archivos personales. Asegúrate de utilizar solo dispositivos externos de confianza y realizar descargas de páginas oficiales que garanticen tu seguridad.
- Mantén la alerta ante páginas fraudulentas, enlaces y adjuntos. Estos días las páginas engañosas y los fraudes electrónicos se están multiplicando. Antes de introducir datos en formularios web contrasta la información desde páginas oficiales. También debes tener precaución con los adjuntos y enlaces de correos electrónicos de remitentes desconocidos, no los descargues ni hagas click si sospechas o no estás seguro de su procedencia.
- Utiliza herramientas adecuadas para transferir la información más sensible. A pesar de las circunstancias, proteger la información sensible siempre debe ser una prioridad. Procura utilizar medios adecuados para transferir y gestionar estos datos. Sin olvidarte de la conexión a Internet que estás utilizando, debes revisar la configuración de tu router wifi y no utilizar wifi abiertas o públicas.
- Instala un Red Privada Virtual (VPN) para crear una conexión privada entre tu dispositivo y el servidor de la empresa o sugiere a tu empresa que lo haga.

Estas son solo unas pautas básicas, que deben convertirse en un hábito diario cuando utilicemos nuestros dispositivos e Internet.

Y de manera adicional...

- Activa tu sentido común y presta mucha atención a las noticias, mensajes, correos electrónicos o cualquier otra información que puedas recibir a través de los diferentes servicios que utilices para evitar ser víctimas de fraudes online o descargar malware aprovechándose de técnicas de engaño, como es la ingeniería social.
- Del mismo modo, no te creas cualquier noticia que recibas. Contrasta la información y no reenvíes mensajes participando en la difusión de noticias falsas (fake news) y bulos (hoax)

FUENTE: INCIBE INSTITUTO NACIONAL DE CIBERSEGURIDAD



PRODANA CONSULTORES te ayuda a cumplir con el RGPD. Dándote herramientas y servicios para poder controlar todos los aspectos de adecuación y adaptación a esta normativa.

