

Teletrabajo seguro

CONSEJOS

PARA EMPLEADOS



Acceda a los datos de la empresa con el equipo corporativo

Solo use dispositivos y software proporcionados por su empresa. Cree contraseñas robustas (use administradores de contraseñas confiables/aprobados, si están disponibles), no la anote y procure no ser visto cuando las está tecleando. Evite soluciones temporales, incluso si parece que le proporcionan justo lo que necesita.



Pare. Piense. Conéctese

Antes de empezar el teletrabajo familiarícese con los dispositivos corporativos, las políticas y los procedimientos. Asegúrese de comprender el equipo, las cosas que se deben hacer y no hacer y dónde obtener ayuda.



Acceso remoto seguro

Conéctese a la red corporativa solo a través de la VPN corporativa y proteja los elementos (p.ej. tarjeta inteligente) requeridos para la conexión VPN.



Proteja su equipo y ambiente de teletrabajo

No permita a los miembros de su familia acceder a sus dispositivos de trabajo. Bloquéelos o apáguelos cuando no les esté prestando atención y siempre guárdelos en lugar seguro para evitar pérdidas, daños o robos. Evite miradas indiscretas utilizando pantallas de privacidad y no inclinando la pantalla hacia ventana o cámaras.



Informe

Si ve alguna actividad inusual o sospechosa en algún dispositivo que esté usando para teletrabajar, contacte inmediatamente con su superior a través de los canales apropiados.



Manténgase alerta

Tenga cuidado con cualquier actividad sospechosa y con solicitudes, especialmente relacionadas con asuntos financieros. ¡Podría ser un fraude al CEO! Si duda, llame al solicitante para verificar. No haga clic en enlaces o archivos adjuntos recibidos en emails y mensajes de texto no solicitados.



Evite facilitar información personal

Nunca responda con información personal a mensajes, incluso si afirman ser un negocio legítimo. En su lugar, contacte directamente con la empresa para confirmar su solicitud.



Desarrolle nuevas rutinas

Discuta los planes de trabajo con su superior directo y los miembros del equipo durante el período de teletrabajo, incluyendo la distribución de tareas, plazos y canales de comunicación.



Uso de dispositivos privados

Si usar su dispositivo personal es la única opción y su superior lo permite, asegúrese de que su sistema operativo y software estén actualizados, incluido el antivirus/antimalware, y la conexión es segura a través de una VPN aprobada por su empresa.



Mantenga los negocios separados del ocio

Evite hacer un uso personal de los dispositivos de teletrabajo.