

RECOMENDACIONES DE SEGURIDAD SERVICIOS BEST CTC, S.A. DE C.V.

Con la finalidad de dar certidumbre a los usuarios de los servicios proporcionados por **Servicios Best CTC, S.A. de C.V.**, al público en general, así como para incrementar la seguridad y evitar ser sorprendidos por terceros utilizando de forma no autorizada nuestro nombre, marcas, logotipos, y en general, atributos de propiedad intelectual; se ponen a sus disposiciones las siguientes:

I. **Recomendaciones de Seguridad General:**

- a. Evitar comprar software sin licencia:** Considera que la mayoría del software sin licencia puede contener programas maliciosos, cuyo objetivo es sustraer información personal, claves, contraseñas, accesos bancarios, etc.
- b. Utilizar responsablemente los recursos informáticos:** Accesa a sitios de buena reputación para hacer compras o consumir servicios o información; considera que hay páginas que se utilizan para vulnerar la seguridad de los usuarios.
- c. Cuida los datos críticos:** Toma en cuenta que los datos personales, familiares, de amistades o conocidos son información muy valiosa para los ciberdelincuentes, no los proporciones a cualquier persona.
- d. Utilizar responsablemente las redes sociales:** Evita publicar fechas y horas de tus viajes, asistencia a eventos sociales o deportivos, ubicación de tu centro de trabajo, escuelas o colegios de tus familiares; considera que la "ingeniería social" es el uso de esta información por parte de los ciberdelincuentes y está directamente asociada con ataques de esta naturaleza.
- e. Utiliza contraseñas robustas:** Emplea el uso de caracteres alfanuméricos, letras mayúsculas y minúsculas, así como símbolos para crear tus contraseñas; evita utilizar fechas de nacimiento y/o nombres, así como información a la que más personas puedan tener acceso.
- f. Ignora las fuentes desconocidas:** No abras los archivos adjuntos de fuentes, y/o correos electrónicos desconocidos aun cuando el usuario parezca conocido, siempre asegúrate de que la dirección sea genuina; considera, además, que muchos enlaces que se comparten en la red pueden llevarte a sitios fraudulentos que buscan infectar tus dispositivos o tomar el control de tus equipos.

- g. Actualiza el software de tus dispositivos:** Las actualizaciones te protegen de posibles ataques, ya que su finalidad es minimizar las vulnerabilidades que puedan existir en el uso de tus equipos.
- h. Cierra tu sesión y bloquea tus pantallas:** Al no estar al pendiente de tus sesiones abiertas, alguien más podría tomar control de estas.
- i. Operaciones privadas en WiFi gratuito:** Cuando estés conectado desde redes de WiFi públicas, evita realiza operaciones privadas, efectuar pagos en línea o transacciones bancarias u otras delicadas, fin de mantener protegida tu información.
- j. Verifica las aplicaciones que descargas:** Descarga programas y aplicaciones desde fuentes seguras y oficiales, y verifica que los permisos que solicitan sean sólo los indispensables para su funcionamiento, ten cuidado con aquellas que requieran permisos para el uso de cámara, ubicación o contactos personales.
- k. Lugares de recarga de batería:** Procura utilizar conexiones eléctricas para la recarga de tus equipos, considera que a través del puerto USB se puede tener acceso a la información de los dispositivos.

II. Programas Maliciosos:

A nivel mundial se han detectado diversos programas maliciosos (conocidos popularmente como "virus"), mismos que se transmiten a través de tecnologías de comunicación entre algunos dispositivos fuera de las redes de telecomunicación, tal es el caso de la conectividad Bluetooth o infrarroja.

Servicios Best CTC, S.A. de C.V., al ser una empresa comprometida con la calidad de sus servicios, protege la transmisión de datos e información a través de sus redes, utilizando para ello, fuertes medidas de seguridad.

No obstante, existen equipos o dispositivos que ofrecen al usuario distintas funcionalidades externas a nuestra red, en este sentido, si percibe que sus dispositivos llevan a cabo funciones sin su consentimiento, o cree que se encuentran comprometidos, le recomendamos que cese de utilizarlos inmediatamente y tome las medidas correctivas necesarias para garantizar la seguridad de sus datos e información

III. Publicidad y Promociones:

Te recordamos que la publicidad y las promociones de **Servicios Best CTC, S.A. de C.V.** pueden ser consultadas en nuestros Centros de Atención a Clientes, a través del correo electrónico soporte@ctctelecom.com.mx o en nuestros sitios web www.ctctelecom.com.mx o www.ctctelecom.mx, así como las redes sociales y/o medios que de estos se derivan; en este sentido, te recomendamos verificar siempre las fuentes oficiales y autorizadas para mantenerte al día de la información, evitando así, ser susceptible de fraudes o estafas.

Cada uno de los medios anteriores contiene sus propios términos y condiciones de uso, así como las políticas de privacidad y uso de la información.