invex®
Tips de Seguridad

INVEX incrementa las medidas de seguridad de las transacciones realizadas a través portal invex.com. Nos preocupamos por su tranquilidad, para ello contamos con los más estrictos y sofisticados procedimientos que permiten garantizar la seguridad de sus inversiones.

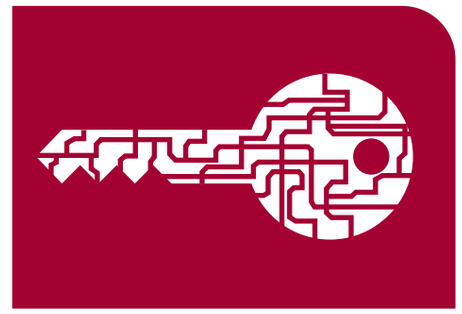
Recomendaciones importantes para el uso seguro del portal invex.com:

En su PC

- Prefiera realizar sus movimientos bancarios en su computadora personal
- Evite realizar movimientos en computadoras ajenas o en sitios públicos con accesos a Internet no protegidos.
- En caso de ser necesario el uso de equipos en cafés Internet o centros de negocio, asegúrese de borrar todos los archivos temporales de Internet y apague la computadora al terminar
- Evite acceder al portal invex.com a través de hipervínculos. Teclee directamente la dirección de Internet en la barra de direcciones www.invex.com
- Actualice su antivirus por lo menos cada tercer día, para asegurar la información almacenada en su PC
- No se aleje de su PC cuando esté realizando un movimiento por Internet

Su contraseña

- Memorice su usuario y clave de acceso, no los apunte ni los comparta
- Procure que su contraseña contenga letras y números poco comunes
- Procure que su contraseña de **INVEX Net** no sea igual la que utilice en otros sistemas
- Cuando digite su contraseña procure que nadie esté observando
- Nunca utilice como contraseña su fecha de nacimiento, su dirección, nombres de familiares o mascotas.
- Realice el cambio de sus contraseñas por lo menos cada 3 meses



Reporte de problemas

Si sospecha del robo de contraseña o recibe algún correo solicitando el información personal o de sus claves, comuníquese inmediatamente a los siguientes teléfonos:

Interior de la República:
01800 1205050

Área Metropolitana (Cd México):
5350 2323

Si prefiere, envíenos un correo electrónico a la siguiente dirección: atención@invex.com

Te recordamos que **INVEX** Banco, nunca envía correos electrónicos ni mensajería a tu domicilio solicitando actualizar información personal, bancaria o información confidencial como clave, NIP o nombres

invex®
Tips de Seguridad

Token

El Token es un dispositivo electrónico que despliega un código numérico distinto cada 60 segundos, mismo que en combinación con tu usuario y contraseña, ofrecen un mayor nivel de seguridad en tus operaciones bancarias vía Internet.

Recuerde guardar su token de forma segura y evitar extraviarlo o exponerlo a robos

Phishing

El **"Phishing"** es una modalidad de estafa diseñada con la finalidad de robar la identidad al usuario. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

¿Cómo Funciona el Phishing?

En esta modalidad de fraude, el usuario malintencionado **envía millones** de **mensajes falsos** que parecen provenir de sitios **Web** reconocidos o de su confianza, como su **banco** o la **institución de su tarjeta de crédito**. Dado que los mensajes y los **sitios Web** que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de **tarjeta de crédito**, **contraseñas**, **información** de **cuentas** u otros **datos personales**.

Para que estos mensajes parezcan aun **más reales**, el estafador suele incluir un **vínculo falso** que parece dirigir al sitio **Web legítimo**, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio **Web oficial**. Una vez que el usuario está en uno de estos **sitios Web**, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva **tarjeta de crédito** o **robar su identidad**.