



POLÍTICAS DE SEGURIDAD DE CAJA SMG

Con el compromiso de proteger la privacidad y la integridad de la información personal y financiera de nuestros socios, CAJA SMG cuenta con medidas de seguridad que le permiten realizar sus transacciones desde la computadora o teléfono de manera segura.

Estas medidas de seguridad contemplan la interacción que usted tiene con LA CAJA desde el momento de ingresar la contraseña, hasta el momento que termina la sesión.

Desde el momento que accede a la página del sitio privado de CAJA SMG, EL SOCIO se encuentra en una **SESIÓN SEGURA**. Esto lo puede confirmar en la dirección que aparece en la barra del navegador y que comienza con <https://eaja.cajasmg.com/cajaenlinea/>

En la parte inferior del navegador aparece el candado cerrado, lo que confirma que se están aplicando las medidas de seguridad, como lo es el cifrado de la información que es transmitida y recibida.



Los servidores Web de LA CAJA cuentan con seguridad de encriptación de datos a 128 bits bajo el protocolo estándar SSL (Secure Socket Layer) para garantizar la seguridad de las operaciones y la confidencialidad de los datos personales de EL SOCIO.

CAJA SMG utiliza un certificado digital expedido por Verisign, Inc., compañía de gran reconocimiento para la certificación de sitios de Internet a nivel mundial.



Si la sesión de banca por Internet está inactiva por 10 minutos, se producirá una desconexión automática de la sesión. En la pantalla se mostrará un mensaje explicativo que le solicitará que reinicie su sesión.

Si no se ha respondido a una petición de marcación del servicio de información telefónica automática, volverá a preguntar por tres ocasiones, colgando la llamada al final del tercer intento.

Todos los sistemas de Banca Electrónica de LA CAJA están protegidos con firewalls, programas antivirus que son continuamente actualizados. Además, periódicamente se realizan auditorías de seguridad.

En LA CAJA se efectúa un monitoreo continuo que permite identificar intentos no autorizados de acceso.

La contraseña de usuario debe contener entre 8 y 10 caracteres máximo, debe ser una combinación de letras y números. Los caracteres válidos son: Letras a-z(minúsculas), A-Z(mayúsculas), Números 0-9, Excepto la letra Ñ, ñ.

Si se intenta acceder en más de tres ocasiones con una palabra clave incorrecta, se procede a bloquear la misma. Para solicitar activación de la misma deberá comunicarse al 01-800-CAJASMG en horario laborable.

Los sistemas de Banca Electrónica solicitarán cambio obligado de contraseña por lo menos cada 3 meses cumplidos.

Si EL SOCIO por alguna razón necesita el cambio de contraseña, lo podrá hacer a voluntad desde el sitio de Caja por Internet o servicio de información telefónica en las opciones disponibles para este efecto.

Si EL SOCIO ha olvidado su contraseña, debe solicitarse el cambio de contraseña por olvido a un ejecutivo en la sucursal más cercana, para que éste le entregue una nueva contraseña. EL SOCIO estará obligado a cambiar la contraseña el siguiente inicio de sesión.

No puede haber dos sesiones abiertas de Caja por Internet o servicio de información telefónica con el mismo número de usuario. En caso de que una segunda persona intente iniciar una segunda sesión, se cancelará la primera sesión y presentará un mensaje a EL SOCIO.

Se inactivará a los usuarios sin inicio de sesión en un lapso de seis (6) meses. Si EL SOCIO desea activar su cuenta debe acercarse a la sucursal más cercana para que ésta sea activada.

LA CAJA se reserva el derecho de bloquear el acceso a los usuarios que se pueda comprobar que han proporcionado datos falsos, o por cualquier otra razón de seguridad.

MODIFICACIÓN A LAS POLÍTICAS DE PRIVACIDAD Y POLÍTICAS DE SEGURIDAD

CAJA SMG se reserva el derecho de realizar cambios, modificaciones o actualizaciones en las Políticas de Seguridad a su entera discreción.

Si tiene alguna duda sólo tiene que llamar al 01-800 2252 764, o escriba al correo electrónico: servicioselectronicos@cajasmg.com

Se considera que, al consultar cualquiera de las secciones del sitio de www.cajasmg.com de CAJA SMG en Internet, se aceptan los términos y condiciones expuestos en este documento.

Todos los productos y servicios prestados por CAJA SMG se encuentran sometidos a la legislación vigente y bajo la supervisión de la CNBV.

© CAJA SMG, 2010. Todos los derechos reservados.

CONSEJOS DE SEGURIDAD PARA UNA NAVEGACIÓN MÁS SEGURA.

Éstas son algunas de las recomendaciones más importantes para EL SOCIO:

Su identificación de usuario y número de NIP o contraseña son de uso estrictamente personal y son confidenciales, sólo deben ser conocidos por usted, y para uso de acceso a los servicios contratados.

No anote su clave en ningún documento físico, ni electrónico. Memorícela.

No comunique su NIP o contraseña a nadie por ningún medio, escrito, telefónico, etc.

CAJA SMG no le solicitará en ningún momento que suministre su número de NIP.

Desconfíe de cualquier toma de datos personales realizada a través de Internet.

CAJA SMG no solicitará información confidencial, personal, financiera o contraseñas de sus clientes vía correo electrónico o mediante otros mecanismos no seguros.

No entregue nunca información personal o financiera a través de un e-mail.

No entre a sitios en Internet, a través de enlaces adjuntos en e-mails de ninguna institución financiera.

Verifique que la información enviada a través de mensajería tenga su nombre y apellido.

No confíe en promociones obtenidas fácilmente, ni responda correos electrónicos solicitando información personal de forma urgente.

No ejecute archivos adjuntos de terceros o desconocidos, directamente desde el mensaje; guarde el archivo al disco duro, y ejecute el antivirus sobre el archivo antes de abrirlo.

No participe en cadenas de correos: esto puede distribuir su dirección de correo de forma no autorizada.

Si necesita introducir datos en un sitio Web, debe asegurarse que en la parte inferior de la ventana de su explorador, aparece un candado o llave cerrados, los cuales indican una conexión segura y encriptada.

No deje su computadora desatendida cuando esté utilizando el servicio en línea.

Evite claves con secuencias de números correlativos, el mismo número de cliente, fechas de nacimiento, números telefónicos, nombres de parientes o propios, ya que pueden pertenecer a cualquier formulario de otro sitio. La clave de acceso debe ser fácil de recordar para Ud. pero difícil de adivinar para un extraño.

Cambie su contraseña por lo menos cada 30 días. No reutilice contraseñas previas.

Su NIP de acceso debe tener por lo menos 8 caracteres, que pueden ser números, letras o combinación de ambos.

Verifique los datos de la última conexión al sistema mostrado en el sitio Web. Estos deben coincidir con el último acceso que usted tenga anotado o recuerde haber realizado.

Si sospecha que alguna de sus claves es conocida por una persona no autorizada, debe cambiarla inmediatamente, para que nadie, solo usted, acceda a sus cuentas.

Comuníquese con LA CAJA en caso de que sospeche de una actividad fraudulenta a través de su clave de acceso al servicio electrónico.

Debe verificar si el sitio donde le ofrecen el servicio de Banca en Línea está certificado por una entidad de reconocimiento internacional en certificados digitales y encriptación de datos (Verisign, Thawte, etc.), debe tener el sello de ésta, y el link donde pueda comprobar el certificado.

Tenga presente que los centros de alquiler de equipos con acce-

so a Internet (CyberCafe's) y computadores de dudosa seguridad no son recomendados para el acceso a cualquier sitio donde tenga que hacer transacciones o manejar información sensible.

Lea periódicamente las Políticas de Privacidad y de Seguridad.

PROTEJA SU COMPUTADORA:

- Actualice los programas en su computadora, según recomiende su proveedor.
- Utilice un Firewall, que le ayuda a prevenir que intrusos o virus ingresen a su computador.
- Instale un programa antivirus y manténgalo actualizado periódicamente.
- Proteja su conexión a Internet.





CAJA SMG, S.C. DE A.P. DE R.L. DE C.V.
Todos los derechos reservados. 2011

