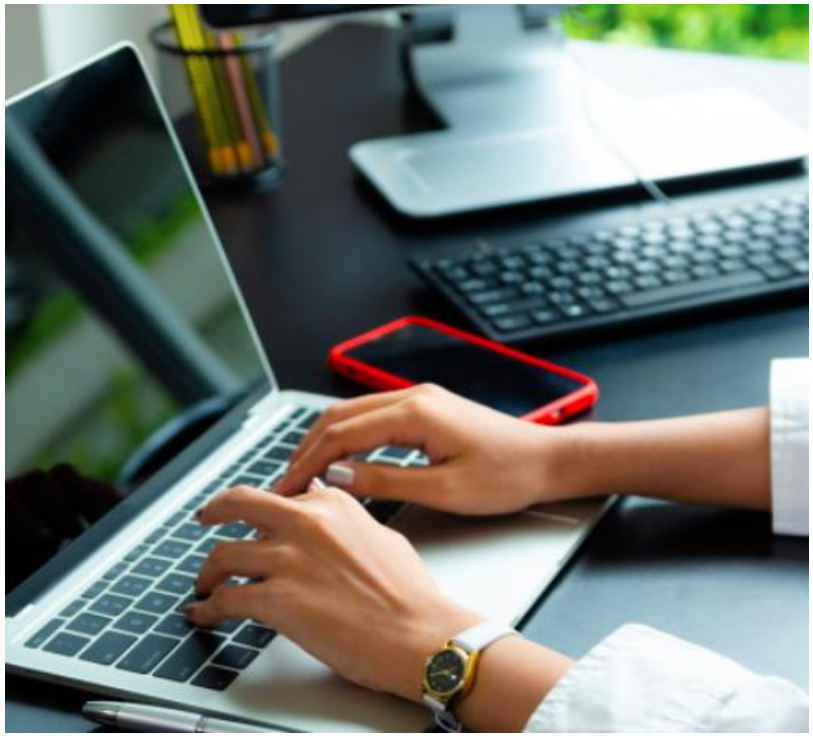
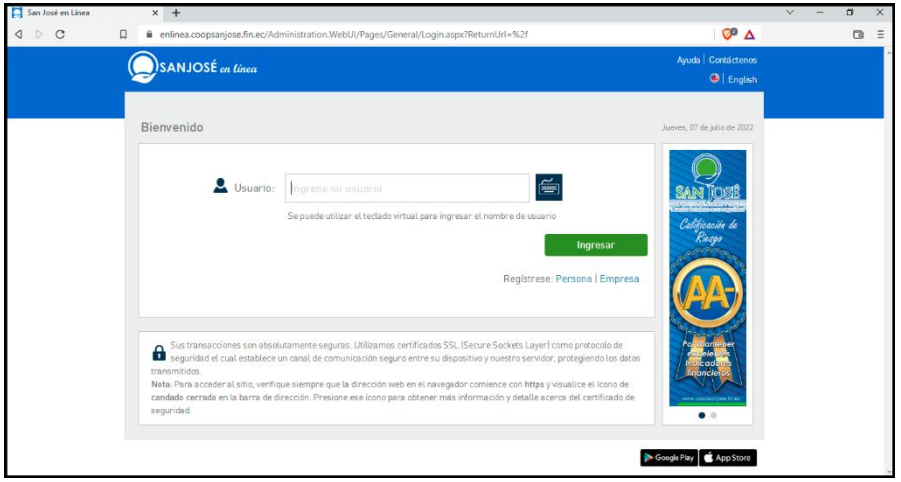


USO SEGURO DE SAN JOSE EN LÍNEA

- Para realizar transacciones en línea, ingresa desde el computador personal de tu oficina o casa. Nunca ingreses desde sitios públicos (cafenet, cybers, aeropuertos, hoteles).
- Verifica que en la barra de direcciones se visualice "***https://***" seguido de "***https://enlinea.coopsanjose.fin.ec/".***
- Valida que el icono del candado se encuentre cerrado, la conexión sea segura y en el certificado de seguridad conste el nombre de la Cooperativa San José; tal cual se presenta en la imagen
- Revisa regularmente el estado de tu cuenta, si detectas transacciones inusuales, comunica de inmediato a Atención al Cliente.
- Al finalizar de transaccional asegúrate de cerrar la sesión.

NAVEGACIÓN SEGURA

- Nunca inicies sesión en equipos públicos o en los cuales tengan acceso otros usuarios.
- Verifica que las paginas transaccionales a las que accedas comiencen con ***https://*** antes del nombre de la institución a la que quieres acceder***(https://enlinea.coopsanjose.fin.ec/).***
- No te conectes a redes WIFI desconocidas o de acceso público.
- Deshabilita la opción de "***Recordar contraseñas"*** en el navegador web.
- Elimina periódicamente el historial de navegación, las cookies y los archivos temporales.
- Mantén actualizado tu computador (Antivirus, Sistema Operativo, Aplicaciones, Navegadores)
- Nunca ingreses tus datos personales, usuarios, claves de acceso en páginas no seguras.
- Evita compartir datos personales en redes sociales (cédula, dirección, teléfonos, correo, números de cuentas)



SEGURIDAD EN CORREO ELECTRÓNICO

- Mantén la privacidad de tu dirección de correo. No lo publiques en redes sociales o páginas web de acceso público.
- Evita abrir correos catalogados como SPAM o Correo no deseado.
- Valida con tu soporte técnico los correos electrónicos que te alerten sobre problemas en tu cuenta y te soliciten verificación de contraseña.
- Descarta correos electrónicos solicitando información sobre tus claves, tarjetas y/o cuentas. Ninguna institución financiera solicita información personal vía correo electrónico.
- No contestes correos electrónicos que te soliciten información financiera o tus datos personales, incluso si tiene apariencia oficial. Los ciberdelincuentes envían correos electrónicos haciéndose pasar por personal de una entidad, usando logos o imágenes de las instituciones financieras con el único objetivo de capturar tus claves de acceso y datos bancarios.
- Si sospechas de un correo no lo abras y nunca hagas clic en los enlaces adjuntos porque te direccionarán a una web maliciosa.

SEGURIDAD EN EL USO DE CONTRASEÑAS

- Mantén las contraseñas en secreto, no las compartas con nadie.
- Utiliza diferentes contraseñas para cada una de las cuentas o aplicativos a los que accedas (Correo, Redes sociales, Cuenta bancaria).
- No utilices palabras completas, nombres, fechas de nacimiento u otro dato que se pueda adivinar fácilmente.
- Utiliza contraseñas de calidad que contengan mayúsculas, minúsculas, números y caracteres especiales.
- No ingreses tu contraseña en computadores compartidos o de uso público.
- Habilita el doble factor de autenticación en las cuentas importantes.

SEGURIDAD EN LLAMADAS TELEFÓNICAS

- Ninguna institución financiera solicita claves, usuarios, datos de tus cuentas o tarjetas por vía telefónica.
- No entregues tus datos personales en llamadas desconocidas (Números de tarjetas, Cuentas, Usuarios, Contraseñas, PIN, Tokens)
- Si tienes alguna sospecha, cuelga inmediatamente y comunícate directamente a los números de teléfonos institucionales.

SAN JOSÉ
COOPERATIVA DE AHORRO Y CREDITO