RECOMENDACIONES GENERALES DE SEGURIDAD

- Estimado cliente, La Cooperativa **DE AHORRO Y CRÉDITO SAN MARTIN DE PORRES R.L.** NUNCA y por NINGUN MOTIVO le solicitara mediante E-MAIL o LLAMADA TELEFÓNICA, que nos brinde sus números de tarjetas, cuentas bancarias o claves (PIN). Estos datos son secretos y solo de su conocimiento.
- Si alguna vez la Cooperativa le envía un e-mail, una carta o le llama solo será para darle exclusivamente información, pero nunca para pedirle que nos de los números de cuenta o claves o ni para que haga clic en ninguna dirección web.
- Revise con frecuencia el extracto de sus cuentas con el fin de verificar la normalidad de las transacciones.
- Notifique inmediatamente a la Cooperativa cualquier sospecha de fraude o robo de sus cuentas, tarjetas o claves de acceso.

CLAVES DE ACCESO O PIN

- No guarde sus claves, memorícelas.
- Cambie periódicamente sus claves o cuando intuya que puedan ser conocidas por otras personas.
- No construya claves con tres dígitos iguales, independientemente de su posición en la clave, por ejemplo 7771 o 3331 o que todos sean iguales.
- No hay que dar su clave (PIN) a nadie, ni pasarla por internet o menos comentarla por teléfono

TARJETA DE DEBITO

La mejor forma de evitar clonaciones, desfalcos y otros fraudes en su Tarjeta de Débito Visa Electrón – COSMart, es cumpliendo estrictamente las siguientes recomendaciones:

- Cambie el PIN periódicamente para tener mayor seguridad.

En Cajeros Automáticos ATMs

- Es muy importante cubrir su clave secreta (PIN) cuando realiza retiros de efectivo en los cajeros automáticos. (ATMs).
- Por ningún motivo, reciba ayuda de extraños para realizar transacciones en los cajeros automáticos. (ATMs).

En P.O.S. (Puntos de Venta)

- Cuando digite su PIN (clave secreta), hágalo con una mano y la otra, protéjalo de la vista de terceras personas en todo tipo de establecimientos comerciales y de servicios.
- Nunca pierda de vista su Tarjeta cuando haga sus compras en comercios y otros establecimientos.

BANCA WEB(COSMARTNET)

- No habilite la función "Recordar contraseña" ubicado en las opciones de los navegadores de internet.

- No acceda a CosmarNET desde sitios públicos o computadoras no confiables.
- Por su seguridad acceda a CosmartNet desde el portal web de la Cooperativa www.cosmart.coop
- Verifique siempre, que el acceso a CosmartNET sea conexión segura mostrando en la dirección de internet (URL) "https://" al principio de la dirección y no "http".
- No acceda a vínculos que le sean remitidos mediante correos en los cuales le informen sobre "premios", "problemas con el servidor" y otros.
- No abandone o desatienda su computadora mientras opera en CosmartNET. Si tiene que ausentarse, así sea momentáneamente, seleccione la opción salir y cierre su sesión.
- Recuerde cerrar la sesión y el navegador luego de terminar sus transacciones o consultas.

BANCA MÓVIL (COSMARTMÓVIL)

- Mantén tu celular con mecanismos de autenticación (contraseña, patrón o biométrico) en todo momento a fin de evitar el acceso a la información de tu celular.
- Cuando digites la contraseña de CosmartMóvil cerciórate que no hay nadie cerca.
- No ingreses a CosmartMóvil si estas en alguna red WiFi pública.
- No dejes tu celular conectado a CosmartMóvil en manos de otras personas.
- Recordá que tu usuario y clave de CosmartMóvil son los mismos que los de CosmartNet.
- Si pierdes o cambias tu celular, debes descargarte la aplicación *Auntenticador de Google* en tu nuevo equipo; luego ingresar ve la opción Configuración personal en CosmartNet y configurar Soft token.
- Para proteger tus cuentas, si ingresas más de tres veces un usuario o clave equivocados el sistema bloqueará tu acceso.

PREVENCION DE FRAUDES POR SUPLANTACION DE IDENTIDAD(PHISHING)

PHISHING: Es una técnica para obtener información confidencial de los usuarios de forma fraudulenta. (Usuario, Contraseña, PIN, etc.), y posteriormente realizar algún tipo de fraude. El término tiene su origen en la palabra inglesa "fishing" (pesca) y hace referencia a la intención de hacer que los usuarios "MUERDAN EL ANZUELO".

Para esto los estafadores envían un correo electrónico que simula ser de la Cooperativa; haciendo referencia a que sus datos no están actualizados, que es necesario verificarlos o que se trata de una actualización, y que, en caso de no ingresar sus datos, en el enlace proporcionado se procederá a bloquear la cuenta, por ejemplo.

Si el usuario accede al enlace que le proporcionan en el correo electrónico, de forma automática será redirigido a una web manipulada, que es prácticamente exacta a la web legítima de la Cooperativa, donde todos los datos que introduzca serán capturados y empleados para la realización de acciones fraudulentas como la suplantación de identidad, el robo de dinero, o la comisión de delitos informáticos o de otra índole en nombre del estafado.

Por su seguridad recuerde estos tres (3) **NUNCAS:**

- **NUNCA** ingreses a un sitio web bancario desde un link de correo electrónico.
- **NUNCA** proporcione datos personales o financieros por teléfono o correo electrónico.

- **NUNCA Y POR NINGÚN MOTIVO;** la Cooperativa de Ahorro y Crédito San Martin de Porres R.L. le solicitara mediante E-MAIL o LLAMADA TELEFÓNICA, que nos brinde sus números de tarjetas, cuentas bancarias o claves (PIN). Estos datos son secretos y solo de su conocimiento.

Y recuerde estos tres (3) **SIEMPRES:**

- **SIEMPRE** que reciba un correo electrónico valide que este dirigido y personalizado con su nombre.
- **SIEMPRE** debe ser Usted quien inicia la comunicación a la hora de realizar una transacción bancaria.
- **SIEMPRE** debe confirmar que el acceso a un sitio web sea conexión segura, mostrando al inicio de la dirección de internet (URL) "https://" y debe aparecer el ícono de un candado cerrado.

Notifique a la Cooperativa cualquier intento de **PHISING,** al teléfono 3 3526672 o al correo info@cosmart.coop.