YUYAY Ltda.

COOPERATIVA DE AHORRO Y CRÉDITO

Identidad y Confianza

Manual de Políticas, Procesos y Procedimientos para el Manejo de Canales Virtuales.

Contenido

1. Registro de cambios

REGISTRO DE CAMBIOS EN EL DOCUMENTO			
Versión	**Motivo**	**Realizado por**	**Fecha**
1.0	Creación	Ing. Juan Pablo Mejia	18/julio/2023
2.0	Actualización	Ing. Carlos Montoya	12/septiembre/2024
3.0	Actualización	Ing. Juan Pablo Mejia	15/marzo/2026

2. Antecedentes.

El siguiente manual de Políticas, procesos y procedimientos de seguridad para el manejo de canales virtuales se torna necesario debido al tratamiento diario de la información en la Cooperativa de Ahorro y Crédito “Yuyay Ltda.” que se accede mediante servicios, aplicaciones, sistemas que la contienen y en los mismos se debe garantizar una correcta gestión de seguridad. En la actualidad se manejan credenciales de autenticación que deben generarse actualizarse y revocarse de manera óptima y segura. Para el control de accesos se manejan desde sistemas operativos, aplicaciones o aplicaciones online y en cualquiera de estos casos hay que establecer ciertos procedimientos para el manejo de contraseñas y el manejo de seguro de los sistemas de transacción.

Es necesario mencionar que en el control de accesos el nombre que utilizamos de usuario nos identifica y la contraseña nos autentica es decir utilizamos los privilegios de identificación, autenticación y autorización y se cumple lo establecido de “Somos quienes decimos ser”

Como las contraseñas son uno de los factores más utilizados para asegurar nuestros sistemas de información hay que considerar este factor y así evitar el acceso no autorizado a los datos y servicios de nuestra Cooperativa.

Las medidas de seguridad es necesario difundir a los usuarios, proveedores y así mismo revisar su cumplimiento y actuar con las buenas prácticas establecidas de la seguridad de la información una de las acciones más importantes es socializar periódicamente las medidas de seguridad, mantenernos en constante actualización garantizar la seguridad al ingresar al sistema.

Por otra parte, el usuario del sistema de transacción virtual debe ser consciente del manejo seguro de su información para evitar que se vea vulnerada; para ello es indispensable generar las presentes políticas de seguridad.

3. Definiciones.

Autorización de Accesos: Controla el acceso de los usuarios a zonas restringidas a distintos equipos y servicios después de haber superado el proceso de autenticación.

Autenticar: Proceso, dispositivo o sistema utilizado para la comprobación de credenciales de acceso y verificación de la identidad de un usuario.

Confidencialidad: Es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.

Disponibilidad: Acceso a la información en el tiempo y forma en que esta sea requerida.

Evento fortuito o fuerza mayor: se refieren a aquellos eventos tales como huelgas o paros, actos de vandalismo terrorismo manifestaciones, incendios, terremotos, inundaciones u otros similares.

Encriptar: es el proceso mediante el cual la información o archivos son cifrados en formas lógica y controlada, con el objetivo de evitar que alguien no autorizado pueda interpretarla, verla o copiarla.

Información: Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado y distribuido.

Integridad: Es la garantía de mantener la calidad y exactitud de la información.

Seguridad de la información: son los mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.

Servicio financiero por internet: Son los suministrados a través del sitio web que corresponda a uno o mas dominios de la entidad, indistintamente del dispositivo tecnológico a través del cual se acceda.

Servicio financiero móvil: Son los suministrados por las entidades a los socios, clientes o usuarios, a través de terminales electrónicos móviles.

Tiempo real: se refiere a las transacciones que se ejecutan de manera inmediata y que sus resultados de ejecución son visualizados al instante que se realizan.

Transacción electrónica: Es cualquier actividad que involucra la transferencia de información digital para propósitos específicos.

Trasferencia electrónica: Son las transacciones de fondos e información, realizadas por cualquier usuario habilitado, para este fin, haciendo uso de los diferentes terminales electrónicos. Puede referirse a ordenes de cobro ordenes de pago, abonos a cuentas, débitos en puntos de venta retiros de dinero, incluye operaciones que atienden mensajes de consultas de movimientos o saldos de cuenta.

4. Base Legal

En base a la resolución emitida por la superintendencia de Economía Popular y solidaria sobre la norma de control de las seguridades en el uso de la transferencia electrónicas **N: SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 abril 2023, y la reforma a dicha norma de agosto 2023 SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-2023-0270** se realiza la actualización del manual de políticas de seguridad para dar cumplimiento con lo establecido.

5. Objetivos.

Establecer difundir y verificar el funcionamiento de buenas prácticas para la gestión de la seguridad en el sistema de transacciones virtuales de la Cooperativa de Ahorro y crédito “Yuyay Ltda.”. Yuyay Móvil.

6. POLITICAS DE SEGURIDAD PARA EL MANEJO DE CANALES VIRTUALES.

Las entidades financieras contaran con manuales y políticas de seguridad para la protección de la información en el manejo de canales virtuales que deben ser aprobadas por alta dirección.

6.1.Política de Creación de usuarios, gestión de accesos y contraseñas.

Definir la manera de cómo se creará un usuario, así como su formato para el acceso al sistema de transacciones virtuales. Los responsables para dar cumplimiento con esta política son:

Responsables	**Actividades de cumplimiento**
Dueño del sistema (VIMASISTEM)	Implementación en el sistema de medidas de seguridad.
Área de Sistemas	Definición y socialización de las políticas y procedimientos.
Usuario	Responsable del manejo del sistema.
Aprueba: Miembros del CAD y Miembros del CAIR.	

Construcción de usuario:

El sistema debe mostrar una pantalla que permita la creación de usuarios, así mismo debe verificar que la persona sea socio de la Cooperativa mediante una consulta con el número de cedula o número de cuenta.

El sistema debe validar que el nombre del usuario contenga una longitud mínima de 8 y máxima de 15 caracteres, debe contener números y letras, debe contener caracteres especiales, el nombre de usuario distingue entre mayúsculas y minúsculas. (ej. Mariela1418@, maRiela@1418).

El sistema debe solicitar al usuario que responda a 3 preguntas de seguridad que serán utilizadas para recuperación de usuario o contraseña.

El sistema debe solicitar el número de celular y correo electrónico para que toda acción realizada sea notificada al usuario por estos medios.

Una vez registrado el correo y el número de celular del usuario el sistema debe enviar una clave temporal para la creación de la contraseña, permitiendo de esta manera eliminar el riesgo asociado con las contraseñas fijas y aumentar la

seguridad de los controles de acceso de los usuarios implementados para protegerlos

Construcción de Contraseñas:

El sistema debe validar que la contraseña de usuario contenga una longitud mínima de 8 y máxima de 15 caracteres, debe contener números y letras entre mayúsculas y minúsculas, debe contener caracteres especiales.

El sistema no debe aceptar que se ingrese como contraseña el mismo usuario. En caso de no cumplir con el formato definido no se permite la creación de la contraseña.

Para seguridad de la información del usuario el sistema deberá solicitar el cambio de contraseñas cada trimestre es decir cada tres meses 90 días.

Recuperación de usuario y contraseña.

Recuperación de Usuario.

El sistema solicitara el número de cédula, una vez validada la información el sistema pedirá al usuario responder las preguntas de seguridad, si la información es correcta el sistema enviara el nombre de usuario al correo electrónico facilitado por el dueño de la cuenta.

Otra manera de recuperación de usuario es mediante Call Center para brindar este servicio se debe solicitar al dueño de la cuenta:

número de cedula
responder a las preguntas de seguridad
el correo y numero de celular ingresados.

o también se puede acercar a las oficinas de la Cooperativa al área de información y verificaran la identidad mediante la cedula.

Recuperación de Contraseñas

Si el usuario olvidó su contraseña el sistema deberá mostrar la opción “recuperar contraseña”:

El sistema solicitara el nombre de usuario, al verificar que el nombre de usuario es correcto solicitara responder las preguntas de seguridad registradas

anteriormente, se enviara una clave temporal al correo, podrá ingresar la clave generada y su nueva contraseña.

El sistema notificara mediante correo el cambio de contraseñas.

Ingreso de usuarios al sistema de transferencias.

Ingresar por canales seguros al sistema.

Al ingresar el usuario y la contraseña, el sistema debe verificar los datos ingresados para luego buscar en la base de datos y comparar resultados, si los datos son correctos el sistema utilizará como segundo factor de autenticación una clave o denominado clave OTP que se enviará al correo y al número de celular facilitados en el registro, el usuario insertará la clave recibida y el sistema permitirá el acceso.

Bloqueo de usuarios.

Si un usuario digita erróneamente 3 veces la contraseña; el aplicativo se bloqueará automáticamente por el tiempo de una hora.

En el momento que el usuario sospeche que el acceso al aplicativo ha sido comprometido y/o detecta transacciones no autorizadas y requiere por diferentes motivos adicionales el bloqueo de usuario, debe solicitarlo, mediante Call Center o atención al cliente. Si lo hace por medio Call Center, los Operadores validarán los datos e identidad con las preguntas de desafío que se registró al crear el usuario

Se recomienda al usuario acercarse de inmediato o al siguiente día, a cualquiera de las oficinas de la Cooperativa para realizar lo siguiente:

- Solicitar la revisión de débito de la cuenta.

- Presentar el Reclamo.

- Actualizar tu información.

En el caso de que el usuario presente la solicitud por medio del área de información adicional a las preguntas de desafío se solicitará el documento de identificación (CI), con el objetivo de validar de manera segura tu información.

6.2.Políticas de seguridad para las transferencias virtuales.

Garantizar que el usuario se mantenga informado de todas las actividades que realiza en el sistema de transacciones virtuales para evitar incidentes de seguridad derivados de usos carentes de medidas.

Facilitar a los usuarios las obligaciones y buenas prácticas en materia de seguridad en el manejo de canales virtuales.

Contar con una plataforma Tecnológica que permita una encriptación sólida.

Establecer las prácticas de seguridad en la aplicación móvil, que permite a los usuarios asegurar que hay una conexión cifrada que protege las comunicaciones mutuas mientras navegan y así garantizar la seguridad e invulnerabilidad de los datos de los usuarios, tanto almacenados como en tránsito.

Reconocer la validez de transferencias realizadas.

Antes de realizar transacciones, se deberá registrar el beneficiario al cual se desea transferir y el sistema deberá solicitar datos como:

Numero de cedula
Nombres y Apellidos.
Número de cuenta.
Monto de transacción.
Correo electrónico.
Observaciones

Una vez ingresados los datos se pulsará el botón aceptar y el sistema enviará una clave OTP al correo y celular del usuario, la misma que se ingresará en un cuadro de texto para autenticar la solicitud y validar la transacción.

Establecer límites para cada transferencia autorizada.

Al momento de realizar una transferencia por parte del usuario el sistema deberá permitir que el monto máximo sea de $4.999,00 caso contrario mostrara un mensaje de “Monto Supera el límite de transferencia” o mensaje similar.

Si el usuario requiere realizar una transacción con un monto mayor al establecido deberá realizar una solicitud a la Cooperativa de Ahorro y crédito Yuyay Ltda. para que se le aumente el cupo para la transacción.

Imposibilitar que el valor de la transferencia supere el saldo disponible o el límite establecido para un período de tiempo.

El sistema de transacción deberá manejar el control de saldos para las transferencias o pagos, y por otro lado manejar códigos OTP que se envía a email o mensajes de celular SMS con un tiempo determinado y permitir que se caduque la operación.

Permitir que el saldo de la cuenta del cliente, socio o usuario se consulte, valide, acredite o debite en tiempo real.

El sistema de transacciones debe permitir al usuario realizar las consultas de saldo en tiempo real, así como de igual forma la transferencia se debe realizar en tiempo real en el caso de las transferencias internas y las extenas según los cortes habilitados por el Banco Central, para verificar que se cumpla con lo establecido deberá existir una opción para consultas y el sistema mostrara en el estado de cuenta el débito y el crédito para el acreedor.

Registrar las direcciones IP y números de telefonía móvil desde las que se realizan las transacciones desde otros países.

Se debe registrar en el sistema las direcciones IP de la máquina y los números de telefonía móvil desde donde se realiza las transacciones así mismo esta información se debe dar a conocer al cliente mediante correos o mensajes de texto.

Para permitir transacciones desde direcciones IP o telefonía móvil de otros países se debe tener tiene la autorización expresa del socio.

Implementar mecanismos que permitan detectar la copia de los diferentes componentes de su sitio web.

Verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de sistema de nombres de dominio.

Implementar un dispositivo de filtrado web (WAF – Web Application Firewall) para proteger a las aplicaciones de este tipo de ataques vía internet.

Generar Comprobantes.

Permitir al usuario obtener reportes para la conciliación de sus movimientos realizados a través de cualquier terminal electrónico, informa la temporalidad máxima a la que accede la consulta.

El sistema debe permitir al usuario realizar consultas de sus movimientos realizados y generar reportes, en el reporte reflejara el tipo de transferencia, la fecha desde, hasta cuando desea realizar la consulta y el sistema mostrara en el registro la Hora con sus fechas, Descripción, Cuenta origen, Monto, Cuenta destino, Entidad destino, Estado, Referencia.

Generar el comprobante de la transacción con el detalle necesario para la conciliación.

En el sistema deberá existir la opción de generar y descargar el reporte de las transacciones realizadas tanto de las internas como de las externas, con los siguientes datos.

Tipo de Transacción

Cliente

Fecha

Cuenta

Datos del beneficiario

Detalle de la transferencia.

Contratación de pólizas en línea

En el sistema tendrá la funcionalidad de realizar pólizas en línea cuya parametrizacion será la misma del core financiero los campos solicitado serán:

Capital

Plazo

Frecuencia pago interés

Contratación de ahorro programado en línea

En el sistema tendrá la funcionalidad de realizar ahorros programados en línea cuya parametrizacion será la misma del core financiero los campos solicitado serán:

Valor Periódico

Numero de cuotas

Frecuencia pago interés

Fecha primera cuota

Orden de retiro en línea

En el sistema tendrá la funcionalidad de generar órdenes de retiros en línea las mismas que podrán ser ejecutadas en cualquier oficina de la cooperativa para la generación de estas órdenes se deben ingresar los siguientes campos:

Monto

Numero cedula beneficiario

Nombres beneficiario

Celular beneficiario

Correo beneficiario

Retiro Cajero Digital

El sistema tendrá la funcionalidad de generar órdenes de retiros en línea con la generación de códigos QR las mismas que podrán ser efectivas en los cajeros digitales que tenga la cooperativa los campos solicitados en esta función de la app son:

Monto

Código OTP

Pagos QR

La App tiene la funcionalidad de realizar pagos y cobros mediante códigos QR los campos solicitados para realizar esta operación son:

Monto “Campo obligatorio”

Motivo “Campo opcional”

Para receptar un pago únicamente se genera el QR el mismo que se puede compartir

Dentro del apartado de Comercios podemos realizar el pago a todos los comercios que tiene registrada la institución

Red Chas

La institución forma parte de la red chas donde se puede realizar pagos a todos los establecimientos que formen parte de la mencionada red.

Cajeros Automáticos

Para garantizar seguridad, correcto funcionamiento y control del efectivo. Se establece lo siguiente:

1. Seguridad del cajero automático

- Instalación de cámaras de vigilancia.
- Ubicación en lugares iluminados y seguros.
- Sistemas de alarma y sensores contra manipulación.
- Monitoreo constante desde centros de control.

2. Manejo del efectivo

- Procedimientos para carga y recarga de dinero en el cajero.
- Transporte de valores realizado según el proceso que maneja la institución.
- Conteo y verificación del efectivo antes y después de la carga.
- Registro detallado de cada operación de abastecimiento.

3. Control de acceso

- Solo personal autorizado puede abrir o manipular el cajero.
- Uso de llaves, códigos o autenticación doble.
- Registro de fecha, hora y responsable de cada intervención.

4. Mantenimiento y soporte técnico

- Revisiones periódicas para evitar fallas.
- Limpieza y mantenimiento preventivo.
- Atención rápida ante errores o fallos reportados por usuarios.

5. Protección al usuario

- Límites de retiro por transacción o por día.
- Protección del PIN del cliente.
- Bloqueo automático de tarjeta después de varios intentos fallidos.

6. Gestión de incidentes

- Procedimientos a cargo del área de operaciones para casos de:
    - tarjetas retenidas
    - dinero no entregado
    - fallas del sistema
    - intentos de fraude o vandalismo

7. Cumplimiento normativo

- Auditorías periódicas.

- Reportes de operaciones sospechosas para prevenir fraudes o lavado de dinero.

6.3.Medidas para Garantizar la seguridad de la información de los usuarios.

Para garantizar la seguridad de la información de los usuarios se deberá:

- Mantener comunicado a los usuarios sobre las medidas tomadas por la empresa con respecto al manejo de la seguridad de los canales virtuales, por medio de envió de mensajes de texto por correo electrónico y publicidad en redes sociales.
- Notificar mediante correo y mensajes a los usuarios, de toda actividad realizada en el sistema como la hora de ingreso, cambios de contraseñas, transacciones realizadas, sesiones caducadas, sesiones finalizadas.
- Establecer y ejecutar procedimientos de auditoría por lo menos una vez al año, implementando técnicas de Ethical Hacking para determinar vulnerabilidades existentes en el sistema.
- Se debe registrar en el sistema las direcciones IP de la máquina y los números de telefonía móvil desde donde se realiza las transacciones así mismo esta información se debe dar a conocer al cliente mediante correos o mensajes de texto con una previa autorización.
- El sistema debe estar Parametrizado para que se caduque luego de 5 minutos de inactividad, luego del cual, necesariamente hay que volver a ingresar.
- El cambio de contraseñas el sistema transaccional solicitara al usuario realizar cada 90 días (3 meses).
- En el manual de captaciones el área operativa deberá definir el monto del cobro de transferencias interbancarias para realizar la respectiva implementación en el sistema de transferencias.
- El sistema de transacciones deberá crear roles y funciones necesarios para el manejo operacional-
- El sistema deberá conservar el registro de transacciones por 24 meses con: datos de usuario, datos de transacción, datos de beneficiario y direcciones IP de los dispositivos desde donde se realiza la transferencia.

7. Responsabilidades.

Concejo Administrativo, Aprobar el Manual de políticas procesos y procedimientos.

El comité de riesgos conocerá las políticas procesos y procedimientos y recomendará su aprobación a concejo administrativo.

El representante legal deberá implementar las políticas de seguridad de seguridad en canales virtuales.

El área de sistemas recomendara la implementación de las políticas de seguridad y sus actualizaciones tomando en cuenta estándares de buenas prácticas.

El auditor informático verificara la efectividad de las políticas establecidas.

8. Disposiciones Generales.

Todas las dudas o lo no previsto en este Manual, conocerá y resolverá en única y última instancia el Gerente General y dará a conocer al Consejo de Administración, siempre y cuando no afecten los intereses de la Cooperativa.

El presente manual entrará en vigor una vez que el Consejo de Administración lo apruebe

Realizado por: Ing. Juan Pablo Mejía.
Coordinador del Área de Sistemas

Revizado por: Econ. Rumiñahui Pichazaca GERENTE COAC Yuyay Ltda.	**Aprobado por:** Bioq. Fanny A. Zaruma PRESIDENTA DEL CAD

Yo, Pacha Dolores Guaman, secretaria del Consejo de Administración de la Cooperativa de Ahorro y Crédito Yuyay Ltda., certifico que el presente manual, fue aprobado en el seno de la sesión del Consejo de Administración efectuada en la sede matriz de la COAC YUYAY Ltda., Ubicada en la comunidad San Rafael del cantón y provincia Cañar, a los **17** días del mes de Marzo del año 2026. Acta N. XX

Econ. Pacha Dolores Guaman
SECRETARIA DE CAD “YUYAY” Ltda.

9. APROBACIÓN DEL COMITÉ DE ADMINISTRACIÓN INTEGRAL DE RIESGOS. (CAIR)

REGISTRO DE APROBACIÓN DEL DOCUMENTO			
RUBRO	**NOMBRE/CARGO**	**FIRMA**	**FECHA**
REVISADO POR:	Eco. Maria Lucila Saeteros Zamora **Presidente del CAIR**		16/03/2025
REVISADO POR:	Econ. Rumiñahui Pichazaca M **Gerente General**		16/03/2025
RIVISADO POR:	Eco. Elias Tenesaca Quizhpilema **Secretario del CAIR.**		16/03/2025

Yo, Eco. Elias Tenesaca Quizhpilema secretario del Comité de Administración Integral de Riesgos de la Cooperativa de Ahorro y Crédito Yuyay Ltda., certifico que el presente manual, fue revisado y analizado en el seno de la sesión del CAIR efectuada en la sede matriz, San Rafael del cantón Cañar a los 16 días del mes de marzo del año 2026 mediante el acta número XX.

ECO. ELIAS TENESACA QUIZHPILEMA
SECRETARIO DEL CAIR

10. Anexos.

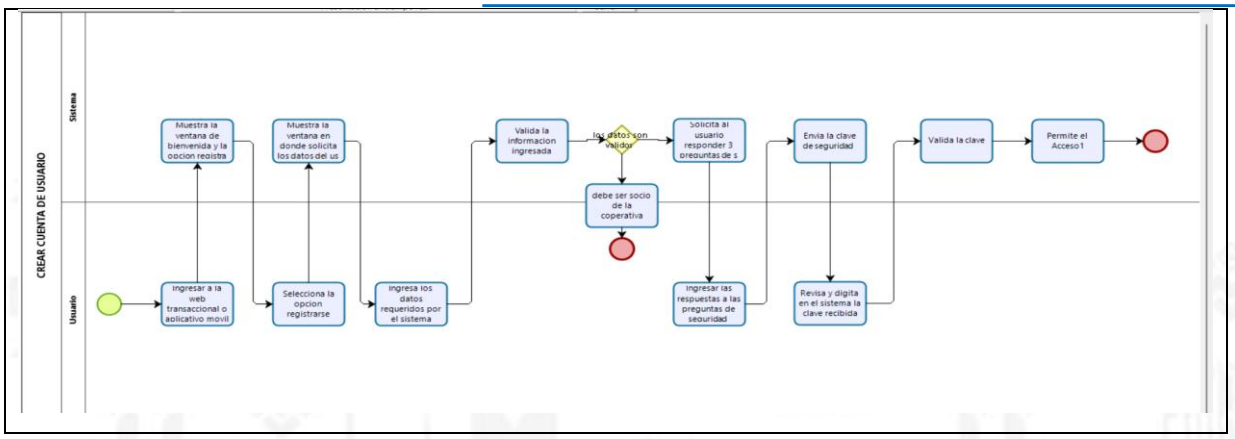
Los procesos creados tendrán las siguientes características:

- Nombre del proceso,
- el código que se describe como: Procesos de Transacciones Electrónicas (PTE),
- actores del proceso,
- el objetivo del proceso,
- la precondición que hace referencia al estado antes de la implementación del proceso.
- la Post condición que hace referencia al estado después de la implementación del proceso-
- Acciones que deben realizar los autores.
- Y el proceso plasmado en diagrama.

10.1. **Proceso Crear Cuenta de usuario**.

Nombre del proceso	Crear Cuenta de usuario	**Código: PTE 1.**
Actores.	Sistema, Usuario	
Objetivo.	Socializar sobre el formato de creación de usuario.	
Precondición.	El usuario requiere crear una cuenta en la web transaccional Yuyay o en el aplicativo Yuyay Móvil.	
Post Condición	Usuario con cuenta en la Web transaccional y Aplicativo Yuyay Móvil.	
Acción del usuario	**Acción del sistema**	

1.- Ingresar a la web transaccional Yuyay o a la aplicación Yuyay Móvil.	**2.-** Muestra ventana de bienvenida con las opciones de iniciar sesión y registrarse.
3. Selecciona la opción registrarse.	4.- Muestra una ventana solicitando datos al usuario como CI, Numero de cuenta, nombres, apellidos, contraseña, .
5. Ingresa los datos requeridos por el sistema.	6.- Valida la información ingresada para luego buscar en la base de datos y comparar resultados, si los datos son correctos el sistema muestra la próxima ventana para el registro y si no son correctos mostrara un mensaje de datos incorrectos.
	7.- Solicita responder a 3 preguntas de seguridad
8.- Ingresar las respuestas a las preguntas de seguridad	9.- Envía clave de seguridad al usuario mediante el correo y numero de celular.
10.- Revisa he ingresa la clave recibida en el sistema	11. Valida la clave
	12. Permite el acceso
DIAGRAMA	

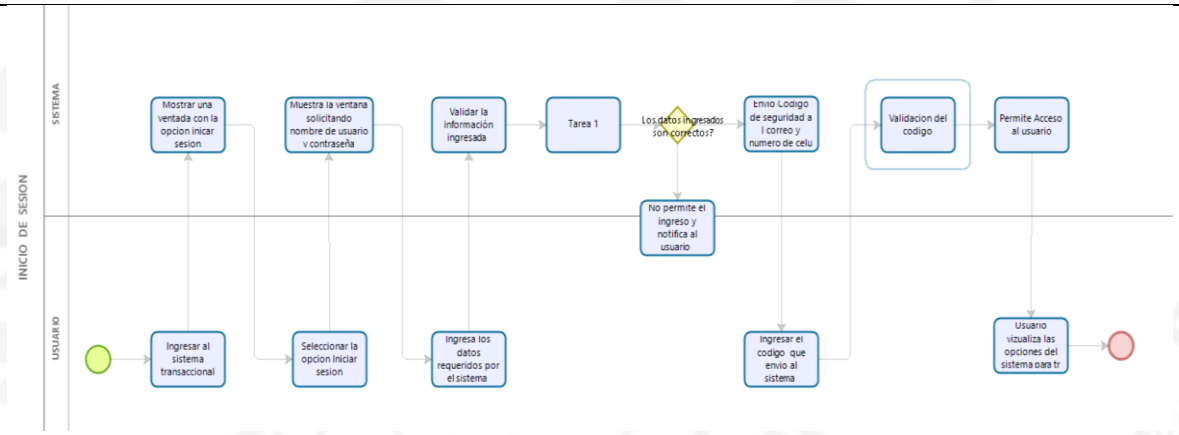


10.2. Proceso Inicio de sesión en al sistema Transaccional.

Nombre del proceso	Inicio de sesión al sistema transaccional	**Código: PTE 2.**
Actores.	Sistema, Usuario	
Objetivo.	Socializar al usuario sobre el ingreso al sistema transaccional	
Precondición.	El usuario desconoce los pasos para el inicio de sesión en el sistema de transacciones	
Post Condición	Usuario conoce el proceso de inicio de sesión en el sistema transaccional	
Acción del usuario	**Acción del sistema**	
1.- Ingresar a la web transaccional Yuyay o a la aplicación Yuyay Móvil. 3. Selecciona la opción iniciar sesión. 5. Ingresa los datos requeridos por el sistema.	**2.-** Muestra ventana de bienvenida con las opciones de iniciar sesión. 4.- Muestra una ventana solicitando usuario y contraseña. 6.- Valida la información ingresada para luego buscar en la base de datos y comparar resultados, si los datos son incorrectos no se permite el acceso.	

8.-Ingresar el código enviado al correo y numero de celular.	7.- Una vez verificados los datos se envía un código de seguridad al correo y numero de celular y se muestra al usuario la ventana de ingresar el código que son de 6 dígitos. 9.- Validación de código permite acceso.

DIAGRAMA

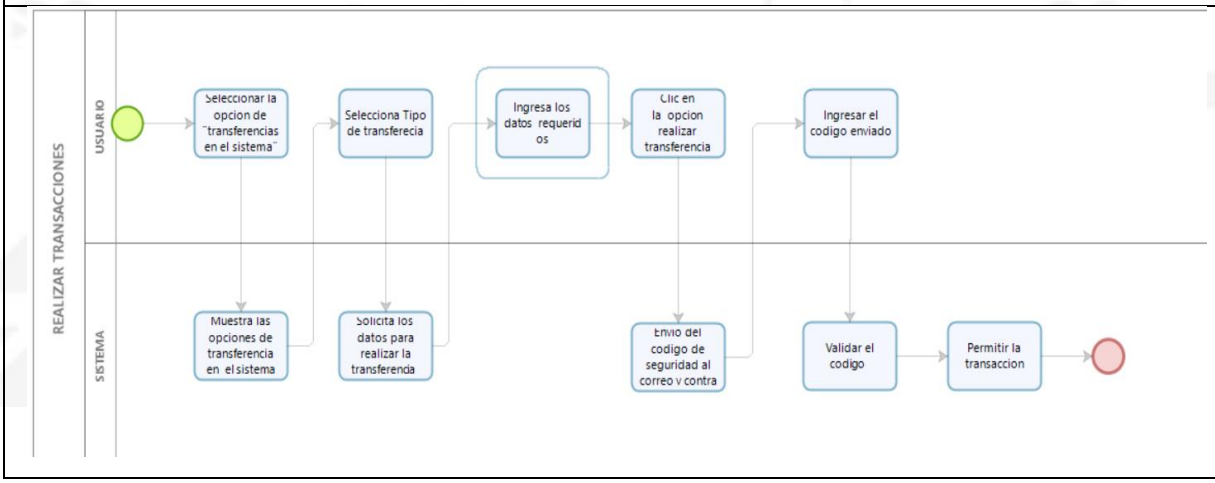


10.3. Proceso. Realizar transacciones.

Nombre del proceso	Realizar transacciones	**Código: PSTE 3.**
Actores.	Sistema, Usuario	
Objetivo.	Socializar al usuario sobre el proceso de realizar una transferencia	
Precondición.	El usuario desconoce los pasos para realizar transferencias en el sistema.	
Post Condición	Usuario conoce los pasos para realizar transferencias en el sistema.	
Acción del usuario	**Acción del sistema**	

1.-Selecciona la opción de transferencias, en el sistema	**2.-** Muestra la ventana con las opciones de transferencias internas y externas.
3.-Selecciona tipo de transferencia.	4.- despliega los datos que solicita para realizar la transferencia. -cuenta origen – cuenta destino – observaciones.
5.- Ingresa los datos requeridos por el sistema.	
6.- Clic en la opción realizar transferencia	7.- Se envía un código de seguridad al correo y numero de celular y se muestra al usuario la ventana de ingresar el código que son de 6 dígitos.
8.-Ingresar el código enviado al correo y numero de celular.	9.- Validar el código. 10.- Permite la transacción

DIAGRAMA

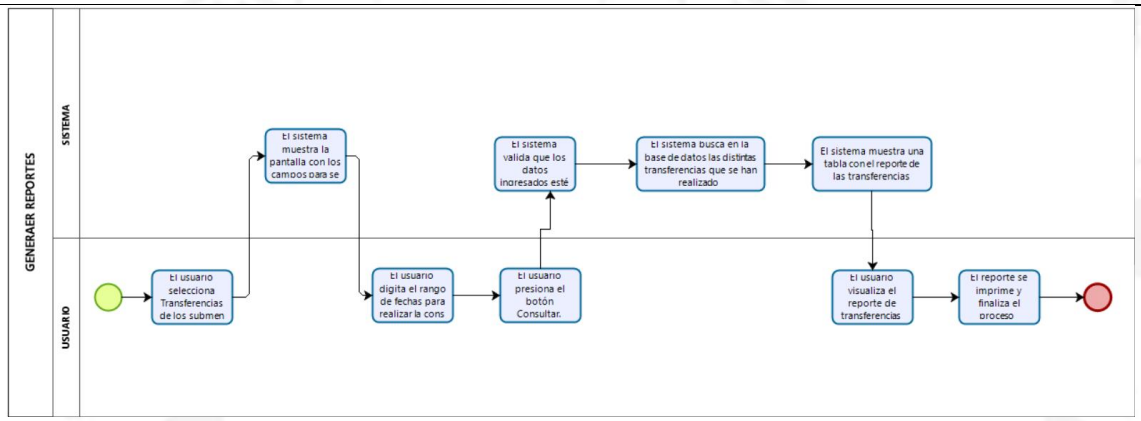


10.4. Proceso Generar Reportes.

Nombre del proceso	Generar Reportes	**Código: PSTE 4.**
Actores.	Sistema, Usuario	
Objetivo.	Presentar al usuario un reporte de las transferencias realizadas según el período de tiempo que establezca.	
Precondición.	El usuario desconoce los pasos para generar un reporte	
Post Condición	El usuario visualiza el reporte de las transferencias que ha realizado.	
Acción del usuario	**Acción del sistema**	
1. El usuario selecciona Transferencias de los submenús disponibles para realizar Consultas. 3. El Socio digita el rango de fechas para realizar la consulta. 4. El Socio presiona el botón Consultar. 5. Presiona el botón Consultar.	2. El sistema muestra la pantalla con los campos para seleccionar el rango de fechas para consultar, y el botón Consultar. 6. El sistema valida que los datos ingresados estén correctos. 7. El sistema busca en la base de datos las distintas transferencias que se han realizado según el rango de fechas que digito el usuario. 8. El sistema muestra una tabla con el reporte de las transferencias según el período de tiempo que seleccione el usuario y los campos.	

9. El usuario visualiza el reporte de transferencias	10. El reporte se imprime y finaliza el proceso

DIAGRAMA



10.5. Anexo de medidas contratadas para cumplimiento normativo