CIRCULAR EXTERNA

RESTRINGIDA

CONSECUTIVO	259	**FECHA**	28	AGO	2023	**ANEXOS: SI** ☐ **NO** ☒	
TEMA: **CONTROL DE SEGURIDAD PARA ACCEDER A LOS CANALES MÓVILES**							
COMPLEMENTA CIRCULAR(ES): NINGUNA		**MODIFICA CIRCULAR(ES):** NINGUNA				**DEROGA CIRCULAR(ES):** NINGUNA	

Como parte de nuestro compromiso constante con la protección de datos y en pro de mitigar los eventos de fraudes por clonación (SIM Swapping o SIM Hijacking), nueva modalidad de estafa donde se ve afectado el asociado a través de su línea telefónica celular, Visionamos implementó un nuevo control el cual permite capturar los datos del dispositivo móvil de un asociado como (marca, modelo, Sim del dispositivo, versión, el IMIE); proceso que implica establecer una relación segura generando un identificador único basado en la data capturada, que tiene como objetivo verificar la autenticidad del dispositivo y la tarjeta SIM al realizar procesos de enrolamiento, recuperación de usuario y recuperación de contraseña para acceder a la aplicación móvil de la Red Coopcentral.

El propósito de este nuevo control es:

1. Mayor seguridad: La identificación de dispositivos móviles celulares y datos de tarjetas de SIM Card, ayudará a prevenir el acceso no autorizado a las aplicaciones móviles y a proteger la información confidencial de sus asociados.

2. Reducción de riesgos: Minimiza las posibilidades de fraude al verificar la autenticidad de los dispositivos móviles que están accediendo a nuestras plataformas versus la información ya registrada en nuestras bases de datos.

3. Confianza reforzada: Esta mejora refuerza nuestro compromiso con la seguridad de la información y demuestra nuestra dedicación a salvaguardar los activos digitales de nuestra Red Coopcentral y de sus asociados.

4. Flexibilidad de configuración: Este control permite parametrizarse, lo que da la posibilidad a la entidad de tomar la decisión de activarlo o no.

Responsabilidad de la entidad:

Si bien las medidas de seguridad adoptadas por Visionamos SPBV para la mitigación de fraude bajo la modalidad de SIM Swapping (Clonación de Tarjeta SIM) ayudarán a mitigar la ocurrencia de estos hechos delictivos o fraudulentos, es importante aclarar el alcance del proceso y el rol que las entidades deben asumir ante la funcionalidad del control de seguridad implementado; las entidades deben realizar el proceso de validación de identidad de sus asociados, establecer las políticas y/o procedimientos para todos los casos que sean expresados en esta circular y que impliquen una validación directa con el asociado ya sea virtual y/o presencial en cada una de las entidades de la red Coopcentral de las cuales posean productos y/o servicios.

Condiciones para tener en cuenta canal Móvil:

1. Cuando un asociado se va enrolar por primera vez, el sistema solicitará el proceso de registro del dispositivo móvil, pero como no se cuenta con información previa para la validación, el sistema procederá con el bloqueo del usuario de manera automática (salvaguardando la integridad de la aplicación, del dispositivo y del asociado) y la entidad participante tendrá la responsabilidad de constatar la identidad del asociado que está realizando el proceso; una vez verificada su identidad, el Usuario administrador de la herramienta de la Entidad **"Centro de Soluciones"** ingresará al aplicativo para desbloquear el usuario y permitir al asociado el ingreso a la aplicación móvil de la Red Coopcentral.

   Es de aclarar que la entidad deberá establecer las políticas o procedimientos internos para la validación de identidad del asociado, a través de canales telefónicos o presenciales.

2. Todos los asociados que se encuentran enrolados previo al despliegue de este nuevo control **no** requieren realizar un nuevo registro del dispositivo móvil con el cual están accediendo actualmente, Visionamos ya cuenta con esta data para las respectivas validaciones.

3. Si un asociado intenta realizar el proceso de recuperación de usuario con un nuevo dispositivo, este le generará un mensaje de seguridad el cual le notifica al asociado lo siguiente: **"Señor usuario, por motivos de seguridad no es posible continuar con su proceso de recuperación de usuario, por favor consulte con su entidad**

para más información”, el asociado deberá contactar a la entidad Participante y esta deberá realizar el mismo proceso notificado en el numeral 1 de esta circular.

4. Sí un asociado intenta realizar un proceso de recuperación de contraseña con un nuevo dispositivo, el sistema solicitará registro de este dispositivo, pero después de la gestión de registro bloqueará el usuario de manera automática, por lo tanto, el asociado deberá contactar a la entidad participante y esta deberá realizar el mismo proceso notificado en el numeral 1 de esta circular.

5. En caso de que un asociado desinstale la aplicación móvil de su dispositivo y la vuelva instalar e intente acceder a la aplicación Móvil de la Red Coopcentral, el sistema solicitará nuevamente el registro del dispositivo debido a que el número UUID cambia; la entidad deberá realizar el mismo proceso notificado en el numeral 1 de esta circular.

   Definición de UUID: *Un Identificador Único Universal*

6. Las actualizaciones de versión de la aplicación móvil seguirán funcionando sin ningún inconveniente, ya que este tipo de proceso no cambiará el UUID.

<u>Modificaciones en el Portal Transaccional Web</u>

- Se inhabilita la opción de recuperación de usuario y recuperación de contraseña del portal transaccional (WEB) opción configurable para cada entidad.
- El proceso de enrolamiento ya no estará disponible a través del portal transaccional, este funcionará únicamente a través de la aplicación móvil de la Red Coopcentral, opción configurable para cada entidad.

A partir del **5 de Octubre 2023**, estaremos habilitando este nuevo control en producción, y próximamente estaremos compartiendo un manual funcional del proceso operativo que deberá realizar la entidad Participante en la herramienta “Centro de soluciones”.

Es importante tener presente que este nuevo control permite ser parametrizable, esto quiere decir, que si una entidad participante no acepta este nuevo ajuste de acuerdo con

las condiciones que se están planteando, puede solicitar a través de la Mesa de ayuda “RedCOOP” la inactivación de este proceso bajo la responsabilidad de la entidad, por lo tanto, continúa con los procesos tal y como se encuentran actualmente definidos.

Estamos seguros de que este ajuste seguirá fortaleciendo nuestra posición de seguridad en línea y protegerá los intereses de todas las entidades y/o asociados de la Red Coopcentral.

Agradecemos su confianza y compromiso con la seguridad de la información y ciberseguridad.

Cordialmente,

(Original firmado)
LUIS SANTIAGO GALLEGO VANEGAS
Gerente General