POLITICA DE SEGURIDAD DE LA INFORMACIÓN

COOPERATIVA DE AHORRO Y CRÉDITO UNIMOS

JUNIO 2022

REGISTRO DE APROBACIONES		
ELABORO	REVISO	APROBÓ
Área de Riesgo y Calidad	Comité de Riesgo SIAR	Consejo de Administración Acta No 229 28-junio-2022

CONTENIDO

REGISTRO DE APROBACIONES		
ELABORO	REVISO	APROBÓ
Área de Riesgo y Calidad	Comité de Riesgo SIAR	Consejo de Administración Acta No 229 28-junio-2022

1. OBJETIVO

La presente Política de Seguridad de la Información es una declaración de las responsabilidades y de la conducta aceptada para mantener un ambiente seguro en COOPERATIVA DE AHORRO Y CREDITO UNIMOS. Esta política establece las directrices y los lineamientos relacionados con el manejo seguro de la información y el compromiso de la gerencia.

2. ALCANCE

La Política de Seguridad de la Información da los lineamientos requeridos para adoptar un Modelo de Seguridad de la Información confiable y flexible y define el marco básico que guiará la implantación de cualquier directriz, proceso, procedimiento, estándar y/o acción, relacionados con La Seguridad de la Información.

Esta Política de Seguridad de la Información aplica para todos los niveles de la organización: Usuarios (empleados y asociados), Asociados (Activos o Retirados), Terceros (proveedores y contratistas), Entes de Control, Entidades Relacionadas; que acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación. Adicionalmente la presente Política aplica a toda la información creada, procesada o utilizada en el soporte al negocio, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

3. ÁREAS INVOLUCRADAS

- Todas las áreas de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS.

4. NORMATIVIDAD

Este procedimiento se enmarca en el Anexo Numero II, del Título IV, del Capítulo IV, de la CBCF SES, de proporcionar y mantener las políticas correspondientes a la adecuada administración de los riesgos de seguridad de la información.

REGISTRO DE APROBACIONES		
ELABORO	REVISO	APROBÓ
Área de Riesgo y Calidad	Comité de Riesgo SIAR	Consejo de Administración Acta No 229 28-junio-2022

5. LINEAMIENTOS GENERALES

La información es un recurso que como el resto de los importantes activos comerciales tiene valor para una COOPERATIVA DE AHORRO Y CREDITO UNIMOS y por consiguiente debe ser debidamente protegida. La seguridad de la información protege de una amplia gama de amenazas, con el fin de garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

La información puede existir en muchas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

La seguridad de la información se define aquí como la preservación de las siguientes características o atributos:

a) **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.

b) **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

c) **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca política, práctica, procedimientos, estructuras organizacionales y funciones del software.

Se deben establecer estos controles para garantizar que se logren los objetivos específicos de seguridad de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS.

5.1. POR QUÉ ES NECESARIA LA SEGURIDAD DE LA INFORMACIÓN

La información y los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Las organizaciones y sus redes y sistemas de información se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos, "hacking" y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados.

La dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información incrementa la dificultad de lograr el control de los accesos. La tendencia hacia el procesamiento distribuido ha debilitado la eficacia del control técnico centralizado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben implementarse requiere una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS. También puede requerir la participación de proveedores, pasantes, asociados, terceros entre otros. Asimismo, puede requerirse el asesoramiento experto de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseño.

La definición de las Políticas de Seguridad Informática para COOPERATIVA DE AHORRO Y CREDITO UNIMOS contempla los siguientes temas:

- Principios Básicos.
- Derechos de Propiedad Intelectual.
- Seguridad Lógica.
- Seguridad del Software y el Hardware.
- Control de Cambios y desarrollo de software.
- Clasificación y Acceso a los Datos.
- Seguridad en Comunicaciones.
- Seguridad Física.

6. PROCEDIMIENTO DESCRIPTIVO

6.1. PRINCIPIOS DE SEGURIDAD INFORMATICA

Los principios sobre los cuales se establece la seguridad informática para COOPERATIVA

DE AHORRO Y CREDITO UNIMOS son:

Confidencialidad: Consiste en velar por la privacidad de la información, haciéndola accesible únicamente a usuarios autorizados.

Integridad: Se debe garantizar que la información no ha sido alterada interna o externamente al sistema.

Auditabilidad: Consiste en garantizar que todas las transacciones, incluidas las de seguridad informática, pueden ser auditadas en línea o en una forma posterior por los usuarios autorizados.

Disponibilidad: Se debe Garantizar que el sistema esté operativo y cuente con los mecanismos de respaldo necesarios para permitir la continuidad del negocio.

6.2. COMPROMISOS Y RESPONSABILIDADES

6.2.1. COMPROMISO CON LA SEGURIDAD DE LA INFORMACIÓN Y LA TECNOLOGÍA

COOPERATIVA DE AHORRO Y CREDITO UNIMOS está obligada a controlar los riesgos y el manejo efectivo de sus activos tecnológicos y de su información. COOPERATIVA DE AHORRO Y CREDITO UNIMOS debe tomar las medidas apropiadas para salvaguardar la integridad y la confidencialidad de la información y para proteger el Área de Riesgos y Calidad, Informática de accesos no autorizados o asaltos tecnológicos. Esto aplica para toda la información, sin tener en cuenta en que medios se encuentre, incluyendo la que se tiene almacenada y pertenece a clientes y la información confidencial y/o personal de las personas que trabajan en COOPERATIVA DE AHORRO Y CREDITO UNIMOS.

COOPERATIVA DE AHORRO Y CREDITO UNIMOS debe:

Proveer un mecanismo para reportar, rastrear, documentar y responder a los incidentes de seguridad que se puedan presentar.

Ser responsable de la información y de la seguridad de esta.

Considerar las sanciones apropiadas para quienes no cumplan con las Políticas definidas.

Las áreas de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS debe:

Actuar de acuerdo con las Políticas de seguridad informática y participar en las revisiones de seguridad que se lleven a cabo.

Hacer parte del plan de concientización en los temas de seguridad informática para hacer que todas las personas de la empresa tengan presente la importancia y la necesidad de contar con un ambiente seguro.

6.2.2. RESPONSABILIDAD POR LA SEGURIDAD INFORMÁTICA Y CUMPLIMIENTO DE LAS POLÍTICAS

El cumplimiento de las Políticas y estándares de seguridad informática son obligatorios, esenciales y en algunos casos legalmente requeridos, para tener una adecuada protección. Estas Políticas y estándares aplican a todas las personas que laboran en la COOPERATIVA DE AHORRO Y CREDITO UNIMOS, incluyendo a las personas de firmas contratistas o proveedores que estén realizando labores en COOPERATIVA DE AHORRO Y CREDITO UNIMOS.

Todas las descripciones de cargos deben contener detalles referentes a las responsabilidades específicas para el cumplimiento de las Políticas de seguridad de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS.

Tener acceso a un sistema de información trae consigo ciertas responsabilidades en términos de seguridad. Los Propietarios de la información deben asegurarse que los usuarios entiendan las condiciones bajo las cuales se les ha brindado el acceso a la información y deben reconocer su deber de proteger a COOPERATIVA DE AHORRO Y CREDITO UNIMOS de tener una brecha de seguridad. Estas responsabilidades se deben hacer claras al usuario al momento de autorizársele el acceso para así asegurar que todos los usuarios de información y recursos tecnológicos de la empresa están cumpliendo con las Políticas de seguridad.

6.2.3. USUARIOS

Los usuarios y tenedores de información y equipos de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS deben:

Aceptar cumplir las Políticas de seguridad de la cooperativa.

Aceptar la responsabilidad personal de proteger los equipos de cómputo y la información de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS contra pérdida, modificaciones no autorizadas y accesos de terceras personas.

Los trabajadores de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS deben firmar un documento especificando que aceptan la responsabilidad de cumplir las Políticas de Seguridad Informática de la empresa.

Los acuerdos firmados por el personal de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS deben ser claros, fáciles de entender y deben incluir ejemplos de lo que constituye una violación de seguridad.

6.2.4. ASUNTOS OPERACIONALES Y DE MANEJO

Para que las Políticas y estándares de seguridad sean efectivos, la COOPERATIVA DE AHORRO Y CREDITO UNIMOS debe utilizar métodos de trabajo, prácticas de negocios y procedimientos en el contexto de cumplir con las estrategias de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS. Por lo tanto, hay algunos asuntos como el control de cambios y la documentación de sistemas, procedimientos y estructura organizacional, que aunque no están relacionados directamente con la seguridad informática, deben ser establecidos e implementados para proveer una protección adecuada de los recursos de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS.

La dirección de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS es responsable de coordinar estos asuntos y asegurar los controles adecuados, la documentación y los métodos implementados de manera que protejan los recursos de la Cooperativa, de los clientes y de las personas que laboran en COOPERATIVA DE AHORRO Y CREDITO UNIMOS. Todas las acciones tomadas deben estar encaminadas a proveer un servicio de mejor calidad, cumpliendo con los objetivos de los clientes y mejorando su posición y su ventaja competitiva.

6.2.5. RESPONSABILIDAD EN EL USO DE LA INFORMACIÓN Y RECURSOS

La COOPERATIVA DE AHORRO Y CREDITO UNIMOS y cada una de las personas que interactúan con ella deben cumplir con los términos estipulados en las licencias de uso de software y en los contratos de adquisición de estas.

Los funcionarios que tengan conocimiento de cualquier uso indebido de la información usada en la COOPERATIVA DE AHORRO Y CREDITO UNIMOS, deben notificarlo a el Área de Riesgos y Calidad *GRC-S2-PR3-F1 FORMATO REPORTE DE EVENTOS DE RIESGO OPERATIVO*.

Los funcionarios deben utilizar la información de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS exclusivamente para fines relacionados con la Cooperativa, quedando prohibido explícitamente cualquier uso comercial y/o privado no autorizado.

Cada persona que tenga a su cargo un computador o conexión a COOPERATIVA DE AHORRO Y CREDITO UNIMOS es responsable de la información que se encuentra bajo su manejo.

Cada funcionario es responsable del uso del software instalado en el equipo que se le asigna y asume la responsabilidad por el uso indebido de cualquier software no autorizado por COOPERATIVA DE AHORRO Y CREDITO UNIMOS.

Las personas que interactúan con COOPERATIVA DE AHORRO Y CREDITO UNIMOS no deben hacer copias del software suministrado, ni transferirlo a otro equipo a través de la red sin la autorización escrita.

El manejo de la contraseña de acceso, utilizada en todos los sistemas de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS que se le asigne a cada usuario es personal e intransferible, para su acceso exclusivo y se debe garantizar su confidencialidad.

Las acciones que intencionadamente rompan retarden, pongan en peligro o accedan al trabajo de otros usuarios, sin autorización específica, están prohibidas, son éticamente reprobables y serán sancionadas con las normas administrativas y jurídicas, estipuladas por la COOPERATIVA DE AHORRO Y CREDITO UNIMOS y/o las autoridades competentes, si fuera necesario.

El propietario de la cuenta es el único responsable de su uso. Cuando se detecte una actividad prohibida, COOPERATIVA DE AHORRO Y CREDITO UNIMOS responsabilizará al propietario de esta.

Todo equipo, cuenta de acceso, permiso de conexión que se utilice en la COOPERATIVA DE AHORRO Y CREDITO UNIMOS debe ser entregado a la persona mediante un acta de entrega donde se responsabiliza por su uso e integridad.

6.3. PROPIETARIOS Y USUARIOS DE INFORMACIÓN

Se debe tener un propietario para cada uno de los recursos de tecnología de la información usados por la COOPERATIVA DE AHORRO Y CREDITO UNIMOS. Las responsabilidades deben estar delimitadas de tal manera que no existan varios propietarios y responsables de un mismo recurso.

6.3.1. USUARIOS DE LA INFORMACIÓN

Son usuarios de información todas las personas que directa o indirectamente, tengan algún tipo de relación con la COOPERATIVA DE AHORRO Y CREDITO UNIMOS, dándole esta característica el uso de los recursos de la Cooperativa, tomando en cuenta esta definición, son usuarios: los Asociados, Empleados, Proveedores, etc.

Al tener el calificativo de usuario de información de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS, deben cumplir con todas y cada una de las políticas y estándares expuestos por la Cooperativa en lo que a seguridad informática se refiere.

6.3.2. LOS PROPIETARIOS DE LA INFORMACIÓN

Son propietarios de información, todas aquellas personas que trabajan en la COOPERATIVA DE AHORRO Y CREDITO UNIMOS. Por lo tanto, son responsables de protegerla adecuadamente, clasificarla, autorizar el acceso a esta.

Los Propietarios de la información son responsables de la seguridad, integridad, disponibilidad y confidencialidad de la información y deben coordinar la implementación de Políticas con otros Propietarios de información y con Propietarios de infraestructura. Los Propietarios deben especificar cómo se debe utilizar la información y como se debe proteger, además de definir cómo se administrarán los procedimientos de control y cómo se aplicarán los niveles apropiados de protección para cada una de las clases de información. (Pública, privada, restringida).

6.3.3. LOS PROPIETARIOS DE INFRAESTRUCTURA

Son propietarios de infraestructura, todos los administradores de recursos utilizados para el manejo y/o administración, de la información.

Son responsables por la funcionalidad, operación, continuidad, manejo y uso de todos los sistemas compartidos, las redes, el soporte y el mantenimiento, el software estándar, los sistemas telefónicos y de comunicaciones y los servicios relacionados. Los Propietarios de infraestructura son responsables de coordinar los servicios de recuperación de los elementos de tecnología informática y de implementar, manejar efectivamente las funciones y procedimientos de seguridad para cumplir con las necesidades de los Propietarios de la Información.

6.4. POLÍTICAS PARA COOPERATIVA DE AHORRO Y CREDITO UNIMOS

UNIMOS se compromete a velar por el cumplimento de las condiciones necesarias para una gestión segura de la información, de acuerdo con el propósito de la organización, determinando así el marco de referencia para establecer los objetivos de seguridad de la información.

Además, se compromete con el cumplimento de los requisitos aplicables con el marco normativo y la mejora continua del sistema.

- **Propósito de la organización**: Implementación de nuevas tecnologías, desarrollen procesos de administración de información seguros, que generen confianza en los servicios ofrecidos.
- **Objetivo de seguridad de la información:** el objetivo de la estrategia de seguridad de la información de UNIMOS es alcanzar el estado deseado definido por los atributos de seguridad de la información como los son la integridad, la confidencialidad y la disponibilidad de esta.
- **Requisitos aplicables:** Anexo 2 del Título IV de Capitulo IV de la Circular básica Contable y Financiera (CBCF) SES.
- **Mejora continua:** Revisión anual de los componentes generales del sistema.

6.4.1. POLÍTICAS DE CONOCIMIENTO GENERAL

Se denominan políticas de conocimiento general, todas aquellas políticas, implícitas en todas y cada una de las tareas desarrolladas dentro de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS.

Dentro de este nivel de políticas se encuentran:

- Todos los usuarios, son responsables por garantizar la Confidencialidad, integridad, y disponibilidad de la formación que se les ha sido entregada.

- Utilizar toda la información a la que tenga acceso en virtud de la labor encomendada, únicamente en el marco de este y para su desarrollo, preservándola en estricta confidencialidad, aun después de finalizada la relación contractual.

- Devolver a la COOPERATIVA DE AHORRO Y CREDITO UNIMOS, todo documento, publicación, material o antecedente sustentado en cualquier soporte que constituya una información confidencial, a la terminación del contrato.

- Los recursos de cómputo empleados por el usuario deberán ser afines al trabajo desarrollado, no deberán ser proporcionados a personas ajenas, no deberán ser utilizados para fines personales.

- Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.

- El contenido de la información usada, consultada, publicada o trasmitida no puede ser de material ilegal, de acoso, difamatorio, abusivo, amenazador, nocivo, vulgar, obsceno, masivo (Entiéndase por material masivo todo aquel que sea ajeno a COOPERATIVA DE AHORRO Y CREDITO UNIMOS, tal como cadenas, publicidad y propaganda comercial, política o social, etc.) o de cualquier otra manera censurable.

- Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS, de acuerdo con las políticas que en este documento se mencionan.

- Construir contraseñas robustas para ingresar a los sistemas de información de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS, cambiarlas periódicamente y no dejar las contraseñas escritas en elementos o lugares donde personas no autorizadas puedan descubrirla.

- Las contraseñas de acceso a los sistemas de información de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS deben ser tratadas como información confidencial de la Cooperativa y no se deben divulgar ni compartir con ninguna persona.

- Colaborar en lo que sea necesario, a solicitud del Área de Riesgos y Calidad, con el fin de contribuir a la seguridad de los recursos de administración de la información.

- Esta estrictamente prohibido el uso de medios de almacenamiento personales en las computadoras de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS.

- El usuario deberá comunicarse con el Área de Riesgos y Calidad en caso de problemas de virus para buscar la solución.

- Solicitar la instalación de software al Área de Riesgos y Calidad para su debida autorización y gestión con la MIS de COMPERSAR.

- Cumplir, en general, con las políticas y normas de seguridad de información, continuidad y servicios tecnológicos de la Cooperativa.

- El uso de los recursos informáticos y de telecomunicaciones debe ser moderado para no congestionar las redes y sistemas, y no interrumpir las actividades propias o de compañeros de trabajo.

REGISTRO DE APROBACIONES		
ELABORO	REVISO	APROBÓ
Área de Riesgo y Calidad	Comité de Riesgo SIAR	Consejo de Administración Acta No 229 28-junio-2022

- La información altamente confidencial o de uso restringido, debe guardarse y transmitirse de manera cifrada o a través de medios seguros de usos exclusivo de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS.

- Reportar inmediatamente a el Área de Riesgos y Calidad y Gerencia, cualquier evento que pueda comprometer la seguridad de los recursos informáticos de la COOPERATIVA DE AHORRO Y CREDITO UNIMOS, como por ejemplo divulgación de información confidencial, accesos no autorizados, infección por virus informático, modificación o pérdida de datos y cualquier actividad poco usual.

- El Área de Riesgos y Calidad mantendrá registros del manejo de la información y los recursos informáticos (formatos de control, aceptación de los usuarios de las políticas de seguridad, reportes de capacitaciones, etc), como elemento probatorio en caso de presentarse algún comportamiento indebido.

- Es responsabilidad de los dueños de la información crítica no dejar copias impresas o documentos físicos en lugares de fácil acceso a personal no autorizado

6.4.2. ASPECTOS NO PERMITIDOS:

- Interceptar, recopilar o almacenar datos sobre terceros sin su conocimiento o consentimiento.

- Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red.

- Enviar mensajes no solicitados (spam), virus, o ataques internos o externos.

- Obtener acceso no autorizado a equipos, sistemas o programas, tanto al interior de la red como fuera de ella. Tampoco se podrá utilizar la red WIFI para obtener, manipular y compartir cualquier archivo de tipo musical o filmográfico, sin tener los derechos de propiedad intelectual.

- Dañar equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red. Ser usada con fines de lucro, actividades comerciales o ilegales, por ejemplo, hacking. Ser utilizada para crear y/o la colocar un virus informático o malware en la red.

- Transmitir, copiar y/o descargar cualquier material que viole cualquier ley. Esto incluye entre otros: material con derecho de autor, pornografía infantil, material amenazante u obsceno o material protegido por secreto comercial o patentes.

6.5. POLITICAS DE LOS REQUERIMIENTOS DE MEDIOS TECNOLÓGICOS Y SEGURIDAD DE LA INFORMACIÓN

6.5.1. Controles Criptográficos

Los sitios web creados para el procesamiento de la información del negocio, deben ser sitios seguros y utilizar certificados digitales emitidos por un ente certificador legalmente constituido en el país.

6.5.2. Intercambio de información.

No estará permitido intercambiar información con entidades externas sin la debida autorización y/o acuerdos de confidencialidad que garantice los tratamientos de información pertinentes.

6.5.3. Trabajo Remoto.

El acceso remoto por parte de los usuarios a los servicios de los servidores de la cooperativa debe estar autorizado por el comité de riesgos o quien delegue la gerencia general.

6.5.4. Acceso a las redes WIFI

El acceso a las redes inalámbricas por parte de los empleados, a través de WiFi, se debe realizar con autenticación usuario y contraseña, independientemente de la herramienta que se quiera utilizar para controlar el acceso.

Las redes WiFi para asociados o visitantes se debe realizar mediante accesos independientes y por redes lógicas independientes a las redes corporativas.

6.5.5. Prestación de servicios por terceras partes.

Cuando existan cambios en los servicios que prestan las terceras partes, estos serán documentados e incluidos en los acuerdos de servicios o contratos.

La organización realizará auditorías a las terceras partes para evaluar la seguridad de la información y, como mínimo, se evaluarán integridad, disponibilidad, confidencialidad y calidad del servicio.

6.5.6. Análisis de Vulnerabilidades.

Se solicitará al menos una vez al año el informe de vulnerabilidades a los terceros que provean servicios y sus planes de remediación.

6.5.7. Política de continuidad del negocio.

El establecimiento de los controles y monitoreo de los riesgos operativos del SARO se basarán en acciones que busquen la continuidad de las actividades normales de la Cooperativa. Para tal fin la Cooperativa cuenta con un Plan de Continuidad del Negocio, en el cual se detallan los aspectos a tener en cuenta en caso de materializarse eventos de riesgo operativo que afecten los recursos disponibles para la adecuada ejecución del plan operativo de la entidad.

Dicho documento contiene los lineamientos específicos adoptados por la entidad en materia de Continuidad de negocio, alineados con las buenas prácticas asociadas a la gestión de riesgos.

Control de Cambios

REGISTRO DE APROBACIONES		
ELABORO	REVISO	APROBÓ
Área de Riesgo y Calidad	Comité de Riesgo SIAR	Consejo de Administración Acta No 229 28-junio-2022

Control de cambios	Fecha	Resumen del cambio
Versión 1	31/05/2022	Emisión del documento
Versión 2	28/06/2022	Se modifica numeral 6.4 Políticas para Cooperativa de Ahorro y Crédito Unimos

REGISTRO DE APROBACIONES		
ELABORO	REVISO	APROBÓ
Área de Riesgo y Calidad	Comité de Riesgo SIAR	Consejo de Administración Acta No 229 28-junio-2022