

 <b>COOPERATIVA DE AHORRO Y CRÉDITO</b> <b>COOPEAIPÉ</b> <i>Empresa de Proyección Aipuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
		página				1 de 24

## COOPERATIVA DE AHORRO Y CRÉDITO COOPEAIPÉ

### ACUERDO No. 39 DE 02 ABRIL DE 2022

Por el cual se aprueba las **POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS**

El Consejo de Administración de COOPEAIPÉ, en uso de sus facultades legales y estatutarias y,

#### CONSIDERANDO

- Que, es deber del Consejo de Administración, proferir los actos Administrativos necesarios para el normal desarrollo del objeto social de la Entidad.
- Que, de acuerdo con el TÍTULO IV SISTEMA DE ADMINISTRACIÓN DE RIESGOS CAPÍTULO IV SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO – SARO ANEXO 2 INSTRUCCIONES SOBRE SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS de la Circular Básica Contable y Financiera se debe adoptar una política de buenas prácticas en materia de seguridad de la información, que les permita identificar los riesgos operativos tecnológicos, así como la posible materialización de incidentes de seguridad que pongan en riesgo la confidencialidad, integridad y disponibilidad de los activos de información, y se adopten, de manera preventiva, los mecanismos que minimicen su impacto, como un elemento que fortalezca la confianza de las organizaciones que conforman el sector solidario actual.
- Que, de acuerdo con la LEY 1273 DE 2009 (ENERO 5 DE 2009) " de la protección de la información y de los datos" se debe adecuar y preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
- Que, en vista de lo anterior

#### ACUERDA:

**Artículo 1.** Aprobar las Políticas De La Seguridad Y Calidad De La Información Para La Prestación De Los Servicios Financieros para COOPEAIPÉ, código **SIPO1 POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS V1** anexo 1, así mismo lo no previsto en ellos se regirá por las leyes vigentes sobre la materia.

**Artículo 2. ÁMBITO DE APLICACIÓN:** La presente Política será aplicable a todos los miembros del Consejo de Administración, Junta de vigilancia, comités especializados, funcionarios y, en general, a todos los asociados de la Cooperativa de Ahorro y Crédito COOPEAIPÉ.

**Artículo 3. CONFIDENCIALIDAD Y MANEJO DE INFORMACIÓN:** Las actuaciones contempladas en esta política, son de estricto carácter confidencial y, en consecuencia, no deberá divulgarlas individualmente, por lo tanto, los asuntos o decisiones tratados o

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

<b>COOPERATIVA DE AHORRO Y CRÉDITO</b>  <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS
	Código SI-PO-1	Versión 1 Emisión Abril/2022 pagina 2 de 24

adoptados, así como todos los aspectos internos de **COOPEAIPE** relacionados, solamente podrán ser dados a conocer a través de los canales formales de comunicación de **COOPEAIPE** y únicamente a las personas, órganos o entidades a quienes corresponda conocerlos.

**Artículo 4. APLICACIÓN DE NORMAS SUPERIORES:** Los casos no previstos en esta política y que no hayan sido desarrollados mediante reglamentaciones internas, se resolverán conforme a la Ley o Decretos especiales y concordantes sobre la materia, las normas emanadas de la Supersolidaria o el Organismo competente.

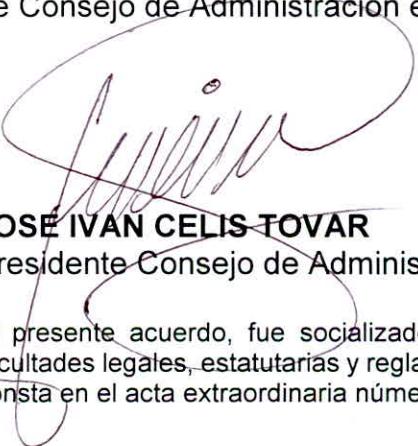
**Artículo 5. MODIFICACIONES:** Cualquier modificación parcial o total se realizará por convocatoria del Consejo de Administración y justificada por acto Administrativo (Acuerdo) y la decisión debe ser unánime y los ajustes realizados sólo tendrán validez a partir de la fecha de aprobación de este organismo. En todo caso se tomarán en cuenta las normas vigentes, en especial las que guardan relación con la Circular Básica Contable y Financiera expedida por la Supersolidaria, y/o las normas o circulares que lo complementen, modifiquen o sustituyan.

**Artículo 6. NORMAS APPLICABLES:** además de las normas de la presente política, se ceñirá a las que sean pertinente de la legislación cooperativa y solidaria, el Estatuto u otros reglamento interno o mandatos especiales de la Asamblea General o a normas de cumplimiento obligatorio emanadas de autoridades competentes.

**Artículo 7. MATERIAS NO REGULADAS:** las materias y situaciones no reguladas en la presente política, así como las dudas de interpretación, serán resueltas por el Consejo de Administración de **COOPEAIPE** con el voto favorable de la mayoría absoluta (las dos terceras 2/3 partes) de los asistentes

**Artículo 8.** Vigencia el presente manual rige a partir de la fecha de su aprobación, por parte del Consejo de Administración y deroga todas las normas anteriores sobre la materia.

**Artículo 9.** La presente política fue socializada y aprobada en reunión extraordinaria 07 de Consejo de Administración en sesión realizada el 02 de abril de 2022.

  
**JOSE IVAN CELIS TOVAR**  
Presidente Consejo de Administración

  
**AGUSTIN CHARRY CHARRY**  
secretario Consejo de Administración

El presente acuerdo, fue socializado y aprobado por el Consejo de Administración, en uso de sus facultades legales, estatutarias y reglamentarias, en reunión del día 02 del mes abril del año 2022, y según consta en el acta extraordinaria número 07 de 2022.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
			página			3 de 24

## ANEXO 1

### POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS

#### GENERALIDADES

- Las políticas de seguridad de la información descritas en este documento aplican a todos los activos de información durante su ciclo de vida, incluyendo creación, distribución, transmisión, almacenamiento y eliminación, debido a que la tecnología es imprescindible para el cumplimiento de los objetivos y la prestación de servicios de la Cooperativa de Empleados de **COOPEAIPÉ**, a sus diferentes grupos de interés en condiciones de seguridad, calidad y efectividad, se velará porque la implementación de la gestión de la tecnología responda a las políticas, necesidades y expectativas de la Cooperativa.
- Las políticas de seguridad informática fijan los mecanismos y procedimientos que debe adoptar la cooperativa para salvaguardar sus sistemas y la información que estos contienen, sin embargo, estas políticas están diseñadas para recoger las características propias de la Cooperativa.
- De la misma forma, las políticas están orientadas a garantizar el uso apropiado de los dispositivos y medios tecnológicos de seguridad de la información (computadores de escritorio, portátiles, móviles,datafonos,etc.) y de servicios como el internet, el correo electrónico, brindando a los funcionarios, contratistas, terceros y público en general, pautas para la utilización apropiada de dichos recursos, permitiendo así minimizar los riesgos de una eventual pérdida de activos de información sensativos para **COOPEAIPÉ**.
- De acuerdo con lo anterior, las políticas de seguridad requieren un alto compromiso con la Cooperativa, agudeza, destreza y experiencia técnica para detectar fallas y debilidades, y constancia para renovar y actualizar dichas políticas en función del dinámico ambiente que rodea la Cooperativa. La información utilizada para el desarrollo de las actividades y funciones y prestación de los servicios financieros diarias o contratadas por **COOPEAIPÉ**, es propiedad de la entidad, por tal razón, todos los funcionarios, estructura organizacional de la cooperativa, contratistas y terceras partes están obligados a proteger dicha información, incluso una vez haya terminado su relación contractual y/o legal con la entidad.
- Las políticas deberán ser revisadas por lo menos una vez al año o al momento de presentarse cambios significativos en el ambiente operacional o del negocio, para lo cual la administración contara con estándares, directrices y procedimientos debidamente aprobados, orientados a cubrir aspectos como la Confidencialidad,

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPE</b> <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abri/2022
			página			4 de 24

Integridad y Disponibilidad de la información y datos, independientemente de la forma, los datos pueden ser: electrónicos, impresos, en audio u otros como lo establece la ley en el tratamiento de datos de información.

## OBJETIVOS

- Proteger la información recibida y generada por COOPEAIPE en sus procesos, mediante la implementación de controles de conformidad con la norma NTC ISO IEC 27001:2013.
- Velar por la protección de los activos informáticos de apoyo en los procesos de la cooperativa.
- Gestionar los riesgos de seguridad de la información de acuerdo con las directrices de la entidad, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.
- Capacitar y sensibilizar al personal en temas relacionados con seguridad de la información, buscando un aumento progresivo en la cultura de seguridad al interior de la entidad, reflejado en el nivel de cumplimiento de políticas y procedimientos y, el reporte de eventos e incidentes de seguridad.

## ROLES Y RESPONSABILIDADES.

- Todo aquel que tenga acceso a la información de COOPEAIPE, es responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir las políticas descritas en este documento.
- Todo aquel que tenga acceso a la información de COOPEAIPE., debe tener claramente definidas sus funciones, con el fin de reducir el uso no autorizado, indebido o accidental de los activos de información.

## POLÍTICAS.

### 1. GENERALES.

- COOPEAIPE cooperativa de ahorro y crédito legalmente constituida y vigilada por la superintendencia de economía solidaria, reconoce la información como un activo fundamental que debe ser protegido frente a amenazas internas o externas que puedan comprometer la confidencialidad, integridad y disponibilidad de la misma, así mismo se compromete a garantizar, verificar y cumplir todos los requerimientos operativos, normativos, legales y de otra índole mediante la aplicación en seguridad

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPe</b> <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
		página		5 de 24		

de la información, con la capacitación de los funcionarios y organización administrativa de la cooperativa.

- Todos los directivos, funcionarios fijos y temporales además de contratistas deben tener acceso solo a la información necesaria para el desarrollo de sus actividades; en caso de que personas ajenas a COOPEAIPe tengan que acceder a la infraestructura tecnológica, la Gerencia autorizará el acceso indispensable de acuerdo con el trabajo a realizar, con previa justificación y tiempo de realización de las operaciones y permisos al área de sistemas de la cooperativa.
- Por medio del procedimiento establecido se hará seguimiento a los accesos realizados por los usuarios, para minimizar el riesgo de pérdida de integridad de la información.
- Si se llega a presentar algún evento que ponga en riesgo la integridad, veracidad y consistencia de la información, se deberán documentar y realizar las acciones que solucionen el incidente a través de área de sistemas.

## 2. SEGURIDAD EN LAS COMUNICACIONES

- COOPEAIPe realizará monitoreo constantemente de la seguridad de sus redes de datos, mediante tecnologías basadas en hardware y/o software para proteger las redes del acceso no autorizado, de los intrusos y de cualquier amenaza externa y/o interna, y garantizando que ninguna de esas amenazas logre llegar a través de las redes hacia los sistemas de información de COOPEAIPe.
- COOPEAIPe cuenta con diagramas e instructivos relacionados con la red de datos, así como los acuerdos de nivel de servicio con terceros que provean servicios sobre estas redes y el responsable de aprobar y gestionar los cambios relacionados con dichos registros será desde el área de Sistemas de la cooperativa

## 3. ACUERDOS DE CONFIDENCIALIDAD

- En todos los casos COOPEAIPe previo a cualquier relación contractual o comercial con terceros firmará acuerdos de confidencialidad.

## 4. AUTORIDADES COMPETENTES

- El Representante Legal es el encargado de mantener el contacto con las autoridades policiales, entidades de control y cualquier otro organismo estatal o privado que consideren necesario para actuar en caso de una emergencia o para mantenerse informados acerca de las últimas novedades en materia de regulación.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

<b>COOPERATIVA DE AHORRO Y CRÉDITO</b>  <i>Empresa de Proyección Aipuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código   SI-PO-1	Versión   1	Emisión   Abril/2022	pagina	6 de 24	

## 5. LAS AUDITORIAS

- Para garantizar la independencia de criterio, COOPEAIPe efectuará al menos una vez al año revisiones independientes del estado de la seguridad de la información, utilizando tecnologías, personal o auditorías externas que permitan que un tercero experto e independiente valide el cumplimiento de las buenas prácticas en seguridad de la información y el cumplimiento de las políticas aprobadas por el Consejo de Administración.
- La Dirección de Auditoría Interna realizará la vigilancia, control y seguimiento al cumplimiento de la normatividad expedida en materia de protección de la información personal, tanto al interior de la empresa como en sus proveedores.

## 6. DE DISPOSITIVOS MÓVILES Y TELETRABAJO.

- Los dispositivos móviles (propiedad de COOPEAIPe) utilizados dentro o fuera de las instalaciones de la Cooperativa y en funciones propias de la entidad, deben ser exclusivamente utilizados para brindar apoyo a las actividades de la entidad y deben ser sujetos a un grado equivalente de protección al de los equipos, se deben aplicar las siguientes pautas:
- Las computadoras personales no se deben utilizar en la entidad para conectarse a Internet u otras redes si no existen controles para los virus y firewall de la computadora personal, instalados y en constante funcionamiento.
- Durante los viajes, los equipos (y medios) no se deben dejar desatendidos en lugares públicos. Las computadoras portátiles se deben llevar como equipaje de mano y además deben contar con una contraseña que permita mantener su nivel seguridad.
- Los portátiles son vulnerables al robo, pérdida o acceso no autorizado durante los viajes. Se les deben proporcionar una forma apropiada de protección al acceso (ej. Contraseñas de encendido, encriptación, etc.) con el fin de prevenir acceso no autorizado.
- Las instrucciones del fabricante concernientes a la protección del equipo se deben seguir en todo momento (p. ej.: para protegerse contra la exposición de campos electromagnéticos muy fuertes).
- Los equipos tecnológicos (computadores, discos portátiles, USB, móviles, entre otros) de la Cooperativa, así como la información almacenada en los mismos, son propiedad de COOPEAIPe, y pueden ser inspeccionados, o utilizados de cualquier manera y en cualquier momento en que la entidad lo considere. Estos deben ser devueltos a COOPEAIPe en el momento en que el usuario deje de tener relación laboral con la entidad.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Aipuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
			página			7 de 24

- Un equipo portátil, teléfono inteligente o cualquier otro sistema tecnológico usado para actividades de **COOPEAIPÉ** que contenga información sensible, no se deberá prestar a nadie y será responsabilidad exclusiva del funcionario que lo tenga asignado.
- El contratista que utilice equipos de cómputo de su propiedad para el desarrollo del objeto del contrato en las instalaciones de la cooperativa deberá acatar el procedimiento establecido por la entidad además de:
  - Declara de buena fe y bajo su responsabilidad que tiene y usa software legal y que no infringe ninguna ley de protección de derechos de autor y propiedad intelectual como lo estipula la ley.
  - Declara que cuenta con las herramientas tecnológicas necesarias para proteger sus equipos minimizando los riesgos de seguridad, como mínimo debe contar con software antivirus licenciado.
- **COOPEAIPÉ** se reserva el derecho de monitorear y revisar cuando se requiera, el software instalado en equipos de cómputo y servidores conectados a la red de la entidad.
- COOPEAIPÉ, para la utilización de la red y sistema operativo en los dispositivos tecnológicos con personal ajeno a su estructura administrativa contara con un sistema de seguridad de permisos limitados y autorizados por el área de sistema de acuerdo al permiso autorizado por la gerencia.
- Esta política contempla los controles requeridos por el estándar ISO 27001: 2013 en el dominio 6.
- COOPEAIPÉ permite la conexión a la red LAN por parte de computadores portátiles cuyo propietario sea externo a la entidad siempre y cuando se mantenga conectado solamente a la red de invitados dispuesta para tal efecto.
- Cuando requiera conectividad a la red interna, se deberá surtir un proceso de autorización por parte del área de Sistemas y tener una declaración firmada del dueño del equipo en la cual se compromete a cumplir las políticas de seguridad de la información.
- Está prohibida la copia, extracción de datos, documentos o cualquier clase de información que haya sido clasificada hacia portátiles o elementos de cómputo que no sean propiedad de COOPEAIPÉ para lo cual se cuenta con los mecanismos para registrar dichas situaciones.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Alpuna</i>	<b>PROCESO</b>	<b>GESTIÓN DE SISTEMAS</b>				
	<b>POLÍTICA</b>	<b>POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS</b>				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022

## 7. ADQUISICIÓN Y DESARROLLO DE SISTEMAS

- COOPEAIPÉ evaluará adicional a los requerimientos funcionales, los requerimientos de seguridad de la información para la especificación de sistemas nuevos, de forma que estos sean fundamentales en los nuevos desarrollos o adquisiciones de software.
- COOPEAIPÉ Garantiza que los sistemas existentes cuentan con especificaciones de seguridad en su ciclo de desarrollo o puesta en producción.
- COOPEAIPÉ propende por la protección de la confidencialidad, integridad, disponibilidad y usabilidad de la información que publique a través de sus medios electrónicos, garantizando que dicha información es veraz y confiable, aunque su contenido sea propio o alimentado por terceros. Para ello podrá soportarse en tecnologías, hardware, software o servicios que ayuden en el control automatizado y/o manual para evitar posibilidades de modificación, manipulación o acceso no autorizados.
- COOPEAIPÉ garantiza la seguridad y la calidad de las transacciones electrónicas que se encuentren a su cargo, bien sea a través de desarrollos propios o servicios de terceros
- En todos los casos COOPEAIPÉ debe incluir términos y condiciones de los productos o servicios según su canal.

## 8. DE ACCESO A LOS RECURSOS DE INFORMACIÓN

- La cooperativa custodiará y cuidará la documentación e información que, por razón de su empleo, cargo o función, conservará bajo su cuidado o a la cual tenga acceso; e impedir o evitar su sustracción, destrucción, ocultamiento o utilización indebida.
- Vigilar y salvaguardar los útiles, equipos, muebles y bienes que le han sido encomendados, y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a los que han sido destinados a sus funcionarios y organización administrativa.
- El acceso de los usuarios a la red y a los diferentes servicios de red debe permitirse únicamente cuando sea formalmente autorizado por el jefe inmediato o la gerencia al área de sistema de la cooperativa según lo indicado en el procedimiento establecido.
- El acceso a los sistemas y recursos de información solamente se debe permitir si existe autorización formal y escrita por parte de la gerencia al área de sistemas.
- La estructura organizacional de la cooperativa (la gerencia, Consejo de Administración, Junta de Vigilancia, integrantes de comités y los funcionarios), contratistas, terceros y público en general deben garantizar que el acceso a la

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPe</b> <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
			página			9 de 24

información y la utilización de esta sea exclusivamente para actividades relacionadas con funciones propias de la entidad, y que ésta sea utilizada de acuerdo con los criterios de confidencialidad definidos por **COOPEAIPe**.

- El establecimiento de conexiones directas entre los sistemas de cómputo y comunicaciones de **COOPEAIPe** con cualquier otra empresa externa, a través de Internet o cualquier otro tipo de red, debe contar con una evaluación y autorización formal previa, basada en un análisis de riesgos de seguridad por parte del administrador de red o área sistemas de la cooperativa encargado de la seguridad informática.
- Una vez se dé por terminada la relación laboral de un funcionario, contratista o tercero, se deben retirar todos los derechos de acceso a los recursos a los cuales estuvo autorizado (usuarios en el sistema financiero, sistema de gestión documental, entre otros) y debe realizar la devolución de activos asignados a la parte administrativa para su respectivo descargue según lo indicado en el procedimiento establecido.

## 9. DE USO DE LOS RECURSOS DE INFORMACIÓN.

- Se deben utilizar los bienes y recursos informáticos asignados única y exclusivamente para el desempeño de su empleo, cargo y/o función. De la misma forma las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, debe ser utilizada en forma exclusiva para fines institucionales de la entidad.
- Los sistemas tecnológicos entregados por **COOPEAIPe** deben ser utilizados únicamente para propósitos propios de la entidad.
- No se pueden almacenar, instalar o utilizar juegos en los equipos de cómputo de **COOPEAIPe**.
- Las personas autorizadas para instalar hardware, software, intervenir técnicamente los equipos de cómputo, realizar cambios al software, a las redes o a los equipos de seguridad, o comunicaciones son las personas que cada proveedor designe bajo comunicación formal dirigida al coordinador administrativo y/o gerente, y área de sistemas de **COOPEAIPe** quienes tendrán la potestad de aceptar o denegar la autorización cuando existan causas justificables, para los funcionarios de **COOPEAIPe** se prohíbe instalar y/o modificar algún software, hardware, redes, seguridad, comunicaciones sin previa autorización o apoyo explícito de un proveedor que asesore y justifique la acción.
- Los cambios, ajustes o mejoras en la infraestructura física o lógica de aplicaciones de **COOPEAIPe**, deberán ceñirse a las políticas de seguridad informática de la entidad.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Aipuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abri/2022
			página			10 de 24

- Los proveedores de software ERP y/o proveedor de servicios de soporte hardware, software, redes y seguridad y/o, proveedores de comunicaciones deben realizar un Análisis de Riesgos para el software (aplicativo, sistema operativo) y hardware nuevo o medios de comunicación, que se planifique implementar en **COOPEAIPÉ** en coordinación del área de sistemas de la cooperativa.
- **COOPEAIPÉ** se reserva el derecho de examinar toda la información almacenada en, o transmitida por sus sistemas de cómputo y de comunicación, y debe informar a los funcionarios, contratistas y terceras partes que no deben esperar privacidad asociada con la información que almacenan o envían a través de estos sistemas.
- De acuerdo con los principios de Internet seguro No se permitirá la navegación en sitios Web de uso social, que no generan valor a la entidad: sitios como YouTube, MySpace, Facebook, hi5, WhatsApp entre otros. Tampoco se permitirá el uso de herramientas en línea y directas de chat, video chat, etc., tipo Messenger, Yahoo, Skype, siempre y cuando sea para uso personal.
- Está prohibido el uso de emisoras de radio por Internet, debido al incremento en el uso de ancho de banda, que afecta la velocidad de navegación de los usuarios de la entidad.
- No se permite la descarga por Internet de archivos de video, música, etc., por afectar el rendimiento de la red y uso del enlace de Internet.
- Los proveedores de software ERP y/o proveedor de servicios de soporte hardware, software, redes y seguridad y/o, proveedores de comunicaciones garantizarán que todos los usuarios cuenten con una configuración estándar en el uso de los recursos de la entidad, y acceso Internet, con el propósito de asegurar que lo establecido en esta política se cumpla a través del área de sistemas.

## 10. DE USO DEL CORREO ELECTRÓNICO

- El correo electrónico es un medio formal de comunicación de **COOPEAIPÉ**.
- Todos los mensajes de correo electrónico deben enviarse mostrando al final el nombre completo, cargo, el nombre de la entidad y que se está actuando en representación de **COOPEAIPÉ**.
- La conexión al correo electrónico y servicios de navegación por Internet han sido suministrados para el uso de personal autorizado únicamente para propósitos propios y oficiales de **COOPEAIPÉ**. En todas las ocasiones los intereses y el buen nombre de la entidad deben ser protegidos por los funcionarios, contratistas y terceras partes que laboran para la misma.
- Cuando se utilice el correo electrónico para asuntos relacionados con las funciones de la entidad, debe existir claridad en que algunos puntos de vista expresados

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Aipuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
			página			11 de 24

pueden ser de los individuos y no representan necesariamente la política de **COOPEAIPÉ**.

- Ningún usuario deberá permitir a otro enviar correos utilizando su cuenta, sin aclarar el remitente.
- Cuando un funcionario requiere ausentarse de la entidad por un período superior a 8 días, o en periodo de vacaciones debe programar el correo electrónico para que automáticamente responda a los remitentes indicando fecha de llegada, nombre y dirección de correo electrónico de la persona encargada durante su ausencia.
- Antes de enviar un correo deberá verificarse que esté dirigido solamente a los interesados y/o a quienes deban conocer o decidir sobre el tema, evitando duplicidades y otros inconvenientes.
- Está prohibida la reproducción y envío de mensajes tipo cadena o similares; puede ocasionar suspensión del servicio temporal o definitivamente, aunque el iniciador haya sido otra persona.
- No se deben transmitir o reproducir mensajes escritos y /o gráficos que no atañen directamente a asuntos propios de la entidad.
- La responsabilidad del contenido de los mensajes de correo será del usuario remitente. El receptor no deberá alterar los mensajes sin la autorización del emisor.
- El contenido de los mensajes de correo se considera confidencial y solo perderá este carácter en casos de investigaciones administrativas, judiciales o incidentes relacionados con seguridad de la información, entendiendo por confidencial aquella información cuyo conocimiento por parte de personas no autorizadas pueda implicar riesgos para la entidad.
- No se deberá utilizar el correo electrónico para enviar mensajes políticos, avisos clasificados, publicidad comercial o boletines cuya información no guarde relación directa con los intereses de la entidad.
- El correo electrónico no deberá usarse para enviar información con contenido discriminatorio. Se deben evitar los estereotipos de raza, género, religión, origen étnico, localización geográfica, orientación sexual, discapacidad, apariencia física o estrato social.
- No debe hacer uso del correo institucional para ningún tipo solicitud personal o ajenos a las funciones de la entidad, ejemplo: Creación de cuentas personales, solicitudes personales, como correo alterno, etc.
- Si su cuenta es accedida de manera ilegal por terceros no autorizados, se recomienda cambiar contraseña y denunciar de manera inmediata ante las autoridades competentes, adjuntando la evidencia.
- COOPEAIPÉ debe capacitar y difundir sobre las buenas prácticas de uso seguro de los medios de comunicación vigentes empleados para uso laboral

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <p><b>COOPEAIPÉ</b> Empresa de Proyección Aipuna</p>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
		página	12 de 24			

## 11. DE LA ADMINISTRACIÓN DE CONTRASEÑAS

- Elección de contraseñas: Para el buen uso de las contraseñas se debe tener en cuenta los siguientes aspectos:
  - Las contraseñas no deben ser construidas con menos de ocho (8) caracteres.
  - No utilizar contraseñas que sean únicamente palabras (aunque sean extranjeras), o nombres (el de usuario, personajes de ficción, miembros de la familia, mascotas, ciudades, marcas, lugares u otro relacionado).
  - No utilizar contraseñas completamente numéricas con algún significado (teléfono, fechas).
  - Elegir una contraseña que mezcle caracteres especiales y alfanuméricos (mayúsculas minúsculas).
- Cada contraseña es de uso personal e intransferible. Los funcionarios, contratistas y terceros que trabajan para COOPEAIPÉ no han de revelar la contraseña de su cuenta a otros funcionarios y/o terceros.
- Está prohibido intentar ingresar a los servicios de cómputo y comunicaciones por medio de la cuenta de otro funcionario.
- Los funcionarios, contratistas y terceros que trabajan para COOPEAIPÉ deben notificar inmediatamente al Subgerente Administrativo si sospechan que alguien ha obtenido acceso sin autorización a su cuenta y debe modificarla en forma inmediata.
- El usuario es responsable por la custodia de su contraseña. Debe evitar en lo posible digitar la contraseña mientras alguna persona está observando lo que escribe en el teclado. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.
- Está prohibido enviar la contraseña por el correo electrónico, (teniendo en cuenta que este no es un medio seguro) y mencionarla en una conversación.
- No se deben almacenar contraseñas en formato legible en archivos tipo "batch", scripts de login automáticos, macros de software, teclas de función de terminales, computadores sin control de acceso o en otros sitios donde personas no autorizadas puedan descubrirlos y utilizarlos.
  - Los funcionarios, contratistas y terceros que trabajan para COOPEAIPÉ deben utilizar contraseñas diferentes en cada uno de los sistemas a los cuales tengan acceso, solo se podrán utilizar contraseñas similares en diferentes sistemas cuando se haya informado directa y expresamente que esto no compromete la seguridad de la información de la entidad.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
			página			13 de 24

## 12. DE MEDIOS REMOVIBLES (UNIDADES DE ALMACENAMIENTO)

- El software antivirus está configurado para escanear de forma automática los medios removibles que son conectados a las estaciones de trabajo.
- Los medios removibles de **COOPEAIPÉ** son de uso exclusivo. El almacenamiento, etiquetado y eliminación de estos medios de almacenamiento debe estar acorde con el esquema de clasificación y deberá seguir los procedimientos relacionados con la gestión de activos de información.
- Las unidades de medios removibles de las estaciones de trabajo y equipos portátiles pertenecientes **COOPEAIPÉ** deben estar bloqueadas. Quien por necesidades estrictamente laborales requiera hacer uso de unidades de medios removibles debe solicitar al director administrativo y/o gerencia a través del área de sistema su activación quien realizará su análisis y en caso de autorización direccionaran el requerimiento al proveedor de servicios de soporte hardware, software, redes y seguridad para que aplique el cambio solicitado.
- El área de sistemas de proceso debe controlar el ingreso y salida de los equipos de cómputo de la entidad y medios extraíbles de almacenamiento de información de las instalaciones de **COOPEAIPÉ** por medio del diligenciamiento del formato establecido para tal fin.
- Los medios removibles en los que se almacene información catalogada como información pública clasificada e información pública reservada deben estar cifrados, de acuerdo con las directrices del procedimiento Gestión de activos de información

## 13. DE LA GESTIÓN DE ACTIVOS

- **Inventario de Activos**
  - El Subgerente Administrativo o quien haga sus veces y el área de sistema, anualmente identifican y documentan los activos de información.
- **Asignación de activos**
  - La asignación de equipo de cómputo se realiza de acuerdo con las obligaciones del funcionario o contratista y requerimiento solicitados por el Gerente al área de sistemas para su proceso de identificación.
- **Uso aceptable de los activos**

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código   SI-PO-1	Versión   1	Emisión   Abril/2022	pagina	14 de 24	

- La información (física y digital), y los sistemas de información, servicios, y equipos (ej. estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de la Cooperativa, son activos de la entidad y se proporcionan a los empleados, contratistas y terceros autorizados, para cumplir con los propósitos del negocio.

- **Áreas Seguras**

- COOPEAIPÉ cuenta con los siguientes controles para prevenir el acceso no autorizado a las instalaciones de la entidad:
  - El área de servidores y equipos de comunicaciones debe contar con mecanismos que permitan garantizar que se cumplen los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga.
  - Todo acceso al área de servidores y equipos de comunicaciones de COOPEAIPÉ es registrado en una bitácora con el fin de dejar rastros de auditoría.
  - Se hace seguimiento a las condiciones (temperatura, humedad, voltaje, y apertura y cierre de puertas) que pueden llegar a afectar los equipos almacenados, con el fin de dar cumplimiento a los requisitos especificados por los fabricantes de los servidores y equipos de comunicaciones que allí se encuentran.
  - El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe ser protegido contra interceptación o daño.
  - Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deben ser subterráneas o deben estar sujetas a una adecuada protección

- **Servicios de Suministro**

- La entidad cuenta con un sistema de alimentación no interrumpida redundante (UPS) que asegura ante una falla en el suministro de energía, el tiempo necesario de funcionamiento de los servidores, los cuales alojan los sistemas de información. Adicionalmente, el edificio cuenta con una planta eléctrica.

- **Mantenimiento de Equipos**

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Aipuña</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
			página			15 de 24

- El Subgerente Administrativo coordina con el apoyo del área de sistemas, las labores de mantenimiento correctivo y preventivo las cuales se realizan a través del proveedor de servicios de soporte hardware, software, redes y seguridad y cuando sea necesario será subcontratado dicho servicio, adicional se realiza seguimiento a los planes anuales de mantenimiento de la infraestructura tecnológica de la entidad.
- **Mantenimiento de software ERP (sistema financiero interno)**
  - El proveedor de software ERP debe garantizar que cada actualización generada (parches, actualizaciones de versiones de paquetes, nuevos ejecutables, nuevas bases de datos, etc.) deben cumplir con un plan de pruebas de calidad y ciclo de vida de software que garanticen que su implementación en los equipos de COOPEAIPÉ no generara ningún trauma, caída o retrasos en la atención al usuario durante su implementación a uso productivo.
  - El proveedor de software interbancario debe garantizar que cada actualización generada (parches, actualizaciones de versiones de paquetes, nuevos ejecutables, nuevas bases de datos, etc.) deben cumplir con un plan de pruebas de calidad y ciclo de vida de software que garanticen que su implementación en los equipos de COOPEAIPÉ no generara ningún trauma, caída o retrasos en la atención al usuario durante su implementación a uso productivo.

## 14. DE CONTROL DE VIRUS

- COOPEAIPÉ es responsable por suministrar un sistema efectivo de antivirus el cual debe estar instalado en cada estación de trabajo, equipos portátiles y en los servidores; los usuarios no deben desactivar esta funcionalidad o intentar manipular la configuración en sus equipos.
- Es responsabilidad de cada usuario utilizar el software para diagnosticar la presencia de virus en la información que provenga por diferentes medios (p. ej.: Internet, memorias USB, archivos compartidos, etc). Este proceso debe ser realizado antes de abrir o ejecutar los archivos, así como antes de divulgarlos, con el fin de no propagar virus informáticos u otros programas maliciosos al interior de la red.
- Los sistemas de cómputo que se sospechen han sido comprometidos por virus o software malicioso deben ser apagados y desconectados de la red en forma

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Aipuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
			página			16 de 24

inmediata. El usuario debe solicitar apoyo técnico e informar al área de Sistemas quien a su vez remitirá la solicitud al proveedor de servicios de soporte hardware, software, redes y seguridad.

- Todos los medios magnéticos suministrados por un tercero deben ser revisados por el antivirus de la entidad antes que estos sean utilizados en los computadores personales o servidores de la entidad.
- Los funcionarios, contratistas y terceras partes que trabajan para COOPEAIPÉ no deben instalar software en las estaciones de trabajo que les han sido asignadas.
- Los usuarios finales de los sistemas de cómputo y comunicaciones de COOPEAIPÉ no deben descargar software desde Internet en ninguna circunstancia.
- Antes de restaurar archivos desde copias de respaldo, dichas copias deben ser evaluadas con el software antivirus de la entidad.

## 15. DE CONFIDENCIALIDAD DE LA INFORMACIÓN

- Los siguientes elementos deben ser considerados con el objeto de que toda la información (medio físico y electrónico) de COOPEAIPÉ quede protegida en forma predeterminada:
  - Los funcionarios, contratistas y terceros que trabajan para COOPEAIPÉ no deben enviar información de carácter diferente a Dominio Público por correo electrónico, a menos que se tengan medidas adicionales de protección.
  - Toda la información de COOPEAIPÉ debe estar protegida para evitar que personas no autorizadas la consulten, divulguen o modifiquen sin consentimiento a terceras partes (funcionarios, prestadores de servicios, entidades externas y personal que realiza alguna actividad dentro de la entidad). Estas entidades tendrán acceso a la información de COOPEAIPÉ únicamente cuando se demuestre la necesidad de conocer su existencia y cuando se haga a través de una cláusula o contrato de confidencialidad.
  - Si se confirma o se sospecha que la información o datos confidenciales o privados, son extraviados o revelados a entidades no autorizadas, el Propietario de la información o quien evidenció el hecho deberá notificar inmediatamente al encargado de la seguridad de información de la entidad, con el objeto de realizar un control efectivo de posibles daños y tomar las acciones necesarias.
  - Ningún funcionario, contratista o tercero que tenga alguna relación laboral con COOPEAIPÉ revelará los controles de seguridad, la forma en que están implementados y las debilidades de los sistemas de información, esto incluye:

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAYPE</b> <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
			página			17 de 24

Información que se proporciona en presentaciones, discusiones, o es tratada en diferentes foros que incluya aspectos técnicos de infraestructura.

## 16. DE MONITOREO Y EVALUACIÓN DEL CUMPLIMIENTO

- COOPEAYPE se reserva el derecho de monitorear o inspeccionar en cualquier momento todos los sistemas de información de la entidad. Esta evaluación puede tener lugar con el consentimiento, presencia o conocimiento del jefe inmediato de los funcionarios involucrados. Los sistemas de información sujetos a tal examen incluyen, pero no están limitados a, sistemas de archivo de correo electrónico, archivos en discos duros de computadores personales, archivos de correo de voz, archivos en colas de impresión.
- Debido a que los sistemas de cómputo y comunicaciones suministrados por COOPEAYPE se emplean únicamente para propósitos de la entidad, los funcionarios, contratistas y terceras partes no deben tener expectativas de privacidad asociadas con la información que ellos almacenan o envían a través de estos sistemas de información.
- El personal técnico asignado a un proceso contractual deberá reportar los incidentes de seguridad de acuerdo con las tareas establecidas para dar cumplimiento a las especificaciones del contrato.
- COOPEAYPE se reserva el derecho de interceptar o vigilar cualquier tráfico de información que pase a través del sistema de la entidad como parte de sus actividades de vigilancia, mantenimiento, investigación, auditoría o seguridad del desempeño del sistema. Todo el personal debe estar consciente de esto cuando use los sistemas de tecnologías de información de la entidad.

## 17. DE PANTALLA DESPEJADA Y ESCRITORIO LIMPIO

- Todos los equipos de COOPEAYPE, deberán ser bloqueados automáticamente después de cinco (5) minutos de inactividad, además los funcionarios, contratistas y terceros deben tener conocimiento de los procedimientos para proteger los equipos desatendidos.
- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren de la misma, de forma tal que solo se pueda desbloquear con la contraseña de usuario.
- Cuando finalice la jornada laboral, se deben cerrar todas las aplicaciones y dejar los equipos apagados o en hibernación.
- Los funcionarios y contratistas de COOPEAYPE deben conservar su escritorio físico libre de información que pueda ser alcanzada, copiada o utilizada por

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Aipuna</i>	PROCESO	GESTIÓN DE SISTEMAS			
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS			
	Código	SI-PO-1	Versión	1	Emisión Abril/2022 pagina 18 de 24

terceros o personal sin autorización, cada vez que se vayan a retirar de sus puestos de trabajo.

- Cualquier equipo portátil debe ser debidamente asegurado si se va a dejar desatendido. Es necesario guardarla bajo llave y/o utilizar una guaya de seguridad.
- Se deben utilizar restricciones para los tiempos de conexión en los servidores de la plataforma tecnológica de COOPEAIPÉ, después de un período de tiempo de inactividad el sistema solicitará nuevamente las credenciales.
- Cuando los funcionarios no se encuentren en su puesto de trabajo, deben guardar cualquier información que utilicen para el desarrollo de sus labores y sea considerada “reservada” de acuerdo con la clasificación. Así mismo, deben asegurar en forma apropiada dicha información.
- El usuario no debe abandonar su PC, terminal o estación de trabajo sin antes salirse de los sistemas o aplicaciones pertinentes o bloquear la estación de trabajo con el comando Windows + L.

## 18. DE RESPALDO DE DATOS

- Toda la información de COOPEAIPÉ debe almacenarse de forma segura, de acuerdo con los requerimientos de tiempo determinados y de conformidad a las normas expedidas.
- COOPEAIPÉ, debe realizar copias de respaldo de la información y pruebas de éstas.
- Se deben realizar registros exactos y completos de las copias de respaldo, y procedimientos de restauración.
- Se debe realizar seguimiento a la ejecución de las copias de respaldo y se deben registrar las fallas de las copias de respaldo programadas, con el fin de certificar su validez y correcto funcionamiento.
- Los medios de respaldo se ponen a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; esto se combina con una prueba de los procedimientos de restauración, y se verifica contra el tiempo de restauración requerido. La prueba de la capacidad para restaurar datos respaldados se hace en medios de prueba dedicados, no sobrescribiendo el medio original, para evitar que en caso de que el proceso de elaboración de copias de respaldo o de restauración falle, cause daño o pérdida de datos irreparable.
- El período de retención de la información esencial del negocio está dado por las Tablas de Retención Documental.

 <b>COOPEAIPE</b> <i>Empresa de Proyección Aipuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
			página		19 de 24	

- Las copias de respaldo se guardan únicamente con el objetivo de restaurar información cuando por situaciones como borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o equipos de cómputo, o por requisitos legales, sea necesario recuperarla.
- Los datos críticos que hayan sido respaldados no deben utilizarse directamente para restaurar datos, a menos que exista otra copia de respaldo de estos en un medio de almacenamiento diferente (cinta, disco, memorias USB, smart-card, CD-ROM, etc.). Si se sospecha la existencia de virus u otro problema de software, la copia de respaldo adicional debe realizarse en una computadora diferente. Esta política previene que la única copia de respaldo de datos críticos sea dañada inadvertidamente en el proceso de restauración.
- Deberá existir un lugar de almacenamiento de medios, externo con información crítica de la entidad para propósitos de recuperación contra desastres, con los estándares de seguridad y conservación adecuados en sus instalaciones, para custodiar los medios magnéticos de la entidad. De la misma forma un acuerdo de confidencialidad de información debe ser firmado por la empresa que hace la custodia de la información.
- Los respaldos de información sensible, crítica y valiosa deben almacenarse en un sitio protegido contra inclemencias del medio ambiente y con controles estrictos de acceso que se encuentre a una distancia razonablemente fuera del alcance de un evento en la zona original.

## 19. DE ACCESO LÓGICO

- COOPEAIPE debe contar con un control efectivo para el cuidado de la información que reside en los sistemas informáticos de la entidad, que tenga lineamientos y políticas que restrinjan el acceso de los usuarios a las aplicaciones y sistemas de la entidad. Adicionalmente se debe contar con un bloqueo automático de los equipos de cómputo, cuando transcurre un tiempo de inactividad superior a 5 minutos.

## 20. DE CONTROL DE ACCESO

- Todos los sistemas conectados a la red de COOPEAIPE deben solicitar el usuario de acceso a la red y contraseña, la cual tendrá máximo tres (3) intentos fallidos. Se debe buscar que información específica como el nombre de la entidad, el sistema operativo, el nombre de la aplicación y otros aspectos relevantes no aparezcan hasta que el usuario tenga acceso exitosamente al sistema.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <p><b>COOPERATIVA DE AHORRO Y CRÉDITO</b>  <b>COOPEAIPÉ</b>  <i>Empresa de Proyección Alpuna</i></p>	<b>PROCESO</b>	<b>GESTIÓN DE SISTEMAS</b>				
	<b>POLÍTICA</b>	<b>POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS</b>				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022

pagina 20 de 24

- Las novedades (vacaciones, enfermedades, viajes largos, entre otros) de las cuentas de usuario notificadas por los procesos de gestión humana y administrativa se deshabilitarán de todos los sistemas a los cuales tienen acceso.
- Los usuarios deben tener acceso sólo a la información que sea necesaria para el desarrollo de sus actividades y para la cual tengan autorización.
- El acceso de usuarios remotos debe ser autorizado por Gerente al área de sistemas.
- El acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro, de acuerdo con los perfiles que se hayan asignado a los usuarios de cada aplicación. Además, sólo los usuarios administradores podrán tener acceso a los sistemas operativos.
- Se deben revisar al menos cada seis (6) meses los derechos de acceso de los usuarios a los datos y a los servicios de información, para mantener un control eficaz por el área de sistemas.

## 21. DE CONFLICTOS LEGALES

- Las políticas de seguridad de información de COOPEAIPÉ fueron diseñadas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones. Si algún funcionario y/o tercero de COOPEAIPÉ considera que alguna política de seguridad de información está en conflicto con las leyes y regulaciones existentes, lo debe reportar en forma inmediata a la gerencia y área de sistemas de la cooperativa.

## 22. DE TRANSFERENCIA DE INFORMACIÓN

- La transferencia de información deberá realizarse protegiendo la Confidencialidad e Integridad de los datos de acuerdo con la clasificación del activo tipo información involucrada.
- Se firmará actas de confidencialidad con los funcionarios y/o Contratistas que por diferentes razones requieran conocer o intercambiar información clasificada y reservada. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes del acceso o uso de dicha información.
- La transferencia e intercambio de datos e información sensible (información pública clasificada, información pública reservada y sobre todo aquella que contenga datos personales) solamente puede hacerse a través de la red o copiarse a otro medio de almacenamiento, siempre que la confidencialidad e integridad de los datos se garantice.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPEAIPÉ</b> <i>Empresa de Proyección Aipuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022
			página			21 de 24

- Se deben usar mecanismos criptográficos para garantizar la confidencialidad, integridad y disponibilidad de la información durante su transferencia, de acuerdo con su nivel de clasificación.
- Se debe transferir información únicamente a receptores autorizados, quienes garanticen por escrito la confidencialidad de la información que se les vaya a suministrar, por medio de acuerdos de confidencialidad.
- No se permite el intercambio de información por medios no autorizados por la Entidad.
- Los emisores deben verificar previamente al envío, el nombre de los destinatarios de la información clasificada como reservada, con el fin de reducir la posibilidad de envío de este tipo de datos, a destinatarios no deseados.
- Se prohíbe el envío de archivos que contengan extensiones ejecutables y otras que puedan ser utilizadas para envío de códigos maliciosos, por medio del correo electrónico de la Entidad.
- Antes de transferir cualquier información, se debe revisar con un software antivirus y antimalware, para garantizar que no esté comprometida con algún código malicioso.

### 23. GESTIÓN DE ACCESO A USUARIOS.

- Se evalúan los controles de accesos de los usuarios a las plataformas de procesamiento informático y a los datos que éstas gestionan.
- **Permisos:** Es la Gerencia la que autoriza la asignación al área de sistemas a cada usuario a un grupo determinado o área. Los sistemas informáticos están desglosados en varios módulos diferentes, donde cada uno de ellos es un programa en sí mismo. De esta manera cada usuario del sistema, según el grupo al que pertenece en la Cooperativa, dispone de los accesos directos a los programas que corresponden a su área.
- **Asignación de Usuarios:** Cuando un usuario nuevo ingresa a la empresa, la gerencia informara al área de sistemas si este usuario necesita del sistema informático y se genera el alta del usuario al sistema o los sistemas. Los datos que se ingresan en la cuenta son los siguientes:
  - **ID de usuario:** Nombre que identifica al usuario, por regla general siempre se debe colocar el nombre o iniciales, esto con el fin de poder identificarlos en los Log de auditoría de los diferentes programas.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 <b>COOPERATIVA DE AHORRO Y CRÉDITO</b> <b>COOPEAIPE</b> <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código   SI-PO-1	Versión   1	Emisión   Abril/2022	pagina	22 de 24	

- **Password:** Estas las crea el usuario, deben ser contraseñas seguras y deben de tener unas características especiales (mínimo cinco (5) caracteres, letras, números y caracteres especiales) sin importar el orden en que se realice.
- **Cancelación de usuarios:** Las cuentas de los usuarios se deben deshabilitar cuando las personas estén de vacaciones, licencia, permisos o terminación del contrato laboral. Se debe estar monitoreando a los usuarios con el fin de poder cambiarle el perfil en caso de que este ya no utilice todos los módulos autorizados o entre a realizar operaciones no relacionadas para su perfil.
- **Mantenimiento de Contraseña:** Se debe configurar el sistema de administración de usuarios para que exija cambio de claves al menos una vez cada mes y que la longitud de esta clave tenga al menos 5 caracteres distintos incluido un carácter especial, adicionalmente se controle que la contraseña no se repita durante al menos 2 veces. Esta función estará a cargo del área de sistemas.
- **Inactividad:** Si el usuario permanece un período de tiempo logeado sin actividad, o se ausenta del área de labores, se debe advertir a los usuarios sobre la necesidad de no dejar las máquinas logeadas e inactivas. Los equipos de cómputo deben tener instalado un protector de inicio de sesión con contraseña.
- **Cuentas de usuario** Los usuarios de COOPEAIPE deben ser identificados en forma personal y no usar el mismo nombre y contraseña para ingresar al sistema informático. Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros. Así mismo, no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- **Control de Aplicaciones en Equipos de cómputo:** Se debe informar a los usuarios sobre las restricciones con respecto a la instalación de programas en sus respectivos puestos de trabajo, ya que la instalación indiscriminada de aplicaciones puede traer problemas con relación a las licencias de los programas y virus, y lo más importante es acarrear sanciones para la Cooperativa por violación a la ley 603 de 2000 de derechos de autor. En la Ley 603 de 2000, se establece que las compañías deben declarar en los Informes de Gestión de cada año, si cumplen o no con las Leyes de protección a los Derechos de Autor y la Propiedad Intelectual; y faculta a las autoridades supervisoras correspondientes (DIAN o SES) para que en el ejercicio de sus funciones verifiquen el cumplimiento de la norma.

 <p>COOPERATIVA DE AHORRO Y CRÉDITO <b>COOPEAIPE</b> Empresa de Proyección Alpuna</p>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abril/2022

pagina 23 de 24

## 24. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

- Se debe generar y ejecutar por lo menos una vez al año un plan de análisis de vulnerabilidades y/o hacking ético para las plataformas críticas de COOPEAIPE, cuya viabilidad técnica y de administración lo permita.

## 25. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

- Los empleados y terceros de COOPEAIPE están en la obligación de reportar tan pronto sean de su conocimiento todos los incidentes de seguridad de la información que puedan afectar leve o gravemente la seguridad de la información, entendida como la integridad disponibilidad, confidencialidad o usabilidad de los activos de información de la entidad.
- Los empleados y terceros de COOPEAIPE están en la obligación de reportar tan pronto sean de su conocimiento todas las vulnerabilidades o debilidades de seguridad de la información que puedan atentar contra la seguridad de la información,
- COOPEAIPE cuenta con canales expeditos, adecuados, y si es el caso anónimo para reportar la ocurrencia de algún incidente o una vulnerabilidad de forma inmediatamente.
- COOPEAIPE cuenta con las metodologías para identificar las causas y orígenes de posibles incidentes de seguridad de la información, mediante el monitoreo constante y la detección temprana de anomalías en la operación diaria.
- Toda violación de estas políticas se debe notificar inmediatamente al área de sistema y al jefe inmediato y/o Gerente, de modo que se pueda resolver debidamente el incidente. Con lo anterior se busca reducir los riesgos de seguridad de la información, protegiendo a todas las personas, así como a la entidad. Así mismo, se deben reportar los eventos de seguridad de la información identificados.
- Se deben notificar situaciones tales como: personas ajenas a COOPEAIPE en oficinas y centros de cómputo, correos maliciosos, sospechas de equipos infectados, reinicio de los equipos de cómputo o enrutadores, mala utilización de recursos, uso ilegal del software, mal uso de información Corporativa, alteración de información, entre otros. Esta función la realizará el área de sistemas de la cooperativa.

## 26. RESPONSABILIDAD DE LOS USUARIOS

- Todos los empleados de COOPEAIPE son responsables de:

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

<b>COOPERATIVA DE AHORRO Y CRÉDITO</b>  <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	POLÍTICA	POLÍTICAS DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-PO-1	Versión	1	Emisión	Abri/2022
		página	24 de 24			

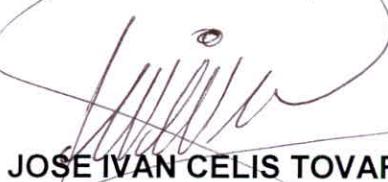
- Mantener sesiones documentos o aplicaciones abiertas de los equipos de cómputo que les han sido asignados para la ejecución de sus actividades cuando deban alejarse de ellos así sea por un tiempo mínimo.
- Mantener su área de trabajo libre de documentos o información que pueda ser vista por otras personas no autorizadas.
- Mantener el escritorio de su estación de trabajo asignada libre de documentos o información que pueda ser accedida fácilmente por personas no autorizadas
- Cumplir las instrucciones de adecuada Comunicación y Buen Uso de los Equipos de Cómputo.
- Los empleados de COOPEAIPe serán responsables por cualquier operación que se efectúe con sus usuarios

**El MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS**, será revisado y actualizado con la regularidad que se requiera, teniendo en cuenta las reglamentaciones expedidas y las necesidades propias de COOPEAIPe

El presente manual entrará en vigor a partir de su aprobación por parte del Consejo de Administración y publicación respectiva; deroga todas las disposiciones anteriores y todas aquellas normas que le sean contrarias.

**Comuníquese y Cúmplase,**

En constancia firman, en Aipe, Huila a los 02 días del mes de abril del año 2022.



**JOSE IVAN CELIS TOVAR**  
Presidente Consejo Administración



**AGUSTIN CHARRY CHARRY**  
Secretario Consejo Administración

Control de Cambios	
Versión	Observación
1	Aprobación inicial ACUERDO No 39 del 02 de abril de 2022

El presente Manual, fue socializado y aprobado por el Consejo de Administración, en uso de sus facultades legales, estatutarias y reglamentarias, en reunión del día 02 del mes abril del año 2022, y según consta en el acta extraordinaria número 07 de 2022.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.