



COOPERATIVA DE AHORRO Y CRÉDITO DE TENJO
COOPTENJO

CONSEJO DE ADMINISTRACIÓN

ACUERDO No. 118
(agosto 26 de 2026)

“Por medio del cual se actualiza la Política Integral De Seguridad De La Información Y Ciberseguridad de COOPTENJO y se articula formalmente con el Sistema de Gestión de Seguridad de la Información SGSI.”

El Consejo de Administración de la COOPERATIVA DE AHORRO Y CREDITO DE TENJO, "COOPTENJO", en uso de las facultades que le confieren las disposiciones legales, el Estatuto y el Reglamento del Sistema Integrado de Administración de Riesgos-SIAR de la Cooperativa, y

CONSIDERANDO:

- 1º. Que por su actividad financiera COOPTENJO en el desarrollo de sus operaciones se encuentra expuesta al riesgo de Crédito.
- 2º. Que, de conformidad con las disposiciones legales, las directrices de la Superintendencia de la Economía Solidaria y el Sistema Integrado de Administración de Riesgos – SIAR, desarrollado e implementado, COOPTENJO debe realizar una efectiva gestión y administración del Riego de Crédito.
- 3º. Que mediante Circular Externa No. 036 de enero de 2022, la Superintendencia de la Economía Solidaria actualizó la Circular Básica Contable y Financiera, la cual en el Capítulo IV del Título IV, establece en forma obligatoria para las organizaciones vigiladas, implementar el Sistema de Gestión de Seguridad de la Información.
- 4º. Que COOPTENJO publicó el Sistema de Gestión de Seguridad de la Información SGSI el 17 de enero de 2024, razón por la cual se requiere actualizar la política vigente para integrarla formalmente a dicho sistema y fortalecer los controles de seguridad, ciberseguridad y protección de la información.

 ENTIDAD COOPERATIVA DE AHORRO Y CRÉDITO	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 2 de 42

ACUERDA:

Actualizar la política de seguridad informática y tecnología de la información, en los términos expresados en el siguiente texto:

POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD

1. OBJETIVO

Establecer los lineamientos, responsabilidades y controles para proteger la información, los datos personales, los activos tecnológicos, los sistemas de información, las comunicaciones y los servicios digitales de COOPTENJO, preservando su confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y cumplimiento normativo, en el marco del SGSI.

2. ALCANCE

Esta política es de obligatorio cumplimiento para órganos de administración y control, directivos, trabajadores, aprendices, proveedores, contratistas, encargados del tratamiento, terceros y demás personas que accedan, consulten, procesen, almacenen, transmitan o administren información de COOPTENJO.

3. AREAS INVOLUCRADAS

- a. Consejo de Administración.
- b. Gerencia General.
- c. Control interno.
- d. Riesgos y Calidad.
- e. Tecnología Informática.

4. NORMATIVIDAD

La presente política se fundamenta en la normatividad aplicable a COOPTENJO, incluyendo Ley 1273 de 2009, Ley 1581 de 2012, Decreto 1377 de 2013, normas y circulares aplicables de la Superintendencia de la Economía Solidaria, SIAR/SARO, buenas prácticas de seguridad y ciberseguridad, ISO/IEC 27001 2013-2022, ISO/IEC y el SGSI publicado el 17 de enero de 2024.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 3 de 42

5. LINEAMIENTOS GENERALES

La información es un recurso que como el resto de los importantes activos comerciales tiene valor para una organización 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 tecnológica, 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:

- Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
- Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- 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 organización.

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. 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, inundación, ataques mediante virus informáticos, "hacking" y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 4 de 42

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.

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 funcionarios de la organización. También puede requerir la participación de proveedores y asociados. 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 COOPTENJO Cooperativa de Ahorro y Crédito contempla los siguientes temas:

- a. Principios Básicos.
- b. Derechos de Propiedad Intelectual.
- c. Seguridad Lógica.
- d. Seguridad del Software y el Hardware.
- e. Control de Cambios y desarrollo de software.
- f. Clasificación y Acceso a los Datos.
- g. Seguridad en Comunicaciones.
- h. Seguridad Física.

6. PROCEDIMIENTO DESCRIPTIVO

6.1. PRINCIPIOS DE SEGURIDAD INFORMATICA

Los principios sobre los cuales se establece la seguridad informática para COOPTENJO Cooperativa de Ahorro y Crédito son:

- a. **Confidencialidad:** Consiste en velar por la privacidad de la información, haciéndola

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 5 de 42

accesible únicamente a usuarios autorizados.

- b. **Integridad:** Se debe garantizar que la información no ha sido alterada interna o externamente al sistema.
- c. **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.
- d. **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 institucional

COOPTENJO se compromete a gestionar los riesgos de seguridad de la información, ciberseguridad, privacidad, continuidad tecnológica y protección de datos personales, mediante controles preventivos, detectivos, correctivos y de mejora continua, articulados al SGSI/SIAR.

6.2.2. Roles y responsabilidades frente al Sistema de Gestión de Seguridad de la Información SGSI y normativa vigente (circular 36 anexo 2).

La administración, implementación, seguimiento y mejora continua de la seguridad de la información en COOPTENJO deberá contar con roles y responsabilidades claramente definidos, de acuerdo con la estructura de gobierno de la Cooperativa, el Sistema de Gestión de Seguridad de la Información SGSI, el SIAR/SARO y las disposiciones regulatorias aplicables.

6.2.2.1. Consejo de Administración.

El Consejo de Administración será responsable de aprobar la Política Integral de Seguridad de la Información y Ciberseguridad, así como sus modificaciones. En materia de seguridad de la información le corresponde:

- a) Definir y promover la dirección estratégica para la seguridad de la información.
- b) Proporcionar los recursos necesarios para la adecuada implementación, mantenimiento y mejora del SGSI.
- c) Velar y apoyar la implementación del Sistema de Gestión de Seguridad de la Información.
- d) Autorizar, facilitar e integrar la puesta en operación del SGSI mediante mecanismos de supervisión y seguimiento por parte de los líderes de proceso.
- e) Velar por el cumplimiento de las obligaciones regulatorias en materia de seguridad de la

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 6 de 42

información, ciberseguridad y protección de datos personales.

f) Velar por la disponibilidad de los recursos y su uso apropiado.

g) Designar o aprobar los responsables de la implementación del SGSI.

h) Pronunciarse y hacer seguimiento a los informes trimestrales presentados por el Representante Legal, dejando constancia en las actas respectivas.

i) Aprobar o conocer, según corresponda, las evaluaciones de riesgo de seguridad de la información y los planes de tratamiento resultantes.

j) Revisar que la estrategia de seguridad de la información esté alineada con los objetivos institucionales y estratégicos de COOPTENJO.

k) Revisar y aprobar las actualizaciones relevantes del SGSI para garantizar su conveniencia, idoneidad y efectividad.

l) Establecer prioridades sobre proyectos e iniciativas relacionadas con seguridad de la información, ciberseguridad, continuidad tecnológica y protección de la información.

6.2.2.2. Representante Legal / Gerencia General

Sin perjuicio de las funciones asignadas en otras disposiciones internas, al Representante Legal o Gerencia General le corresponde:

a) Velar por el desarrollo de los objetivos estratégicos de seguridad de la información definidos por el Consejo de Administración.

b) Velar por la implementación de la presente política y de los controles asociados al SGSI.

c) Facilitar la integración entre los diferentes líderes de proceso para la implementación del modelo de seguridad de la información.

d) Gestionar la disponibilidad de los recursos requeridos y su uso apropiado.

e) Velar por la correcta aplicación de los controles de seguridad para reducir los riesgos de seguridad de la información.

f) Velar por la designación de los responsables de implementar la política y los controles del SGSI.

g) Presentar al Consejo de Administración, como mínimo trimestralmente, informe sobre la evolución y aspectos relevantes de la seguridad de la información, incluyendo acciones preventivas y correctivas, resultados de mediciones, incidentes relevantes, cumplimiento de objetivos, riesgos identificados y planes de mejora.

6.2.2.3. Auditoría Interna o Control Interno

Auditoría Interna o quien ejerza Control Interno deberá:

a) Mantener conocimiento apropiado sobre seguridad de la información, SGSI y normativa aplicable.

b) Evaluar periódicamente la efectividad y cumplimiento de las etapas, controles y elementos clave del SGSI.

c) Identificar deficiencias, oportunidades de mejora y posibles soluciones.

d) Informar los resultados de sus evaluaciones al Consejo de Administración, Gerencia General y demás instancias competentes, según corresponda.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 7 de 42
	Dirección de Tecnología Informática	

e) Realizar seguimiento a los planes de acción derivados de auditorías, evaluaciones, revisiones regulatorias o incidentes de seguridad.

6.2.2. COOPTENJO Cooperativa de Ahorro y Crédito 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.

6.2.3. Cada agencia de COOPTENJO Cooperativa de Ahorro y Crédito 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 asegurar que todas las personas de la empresa tengan presente la importancia y la necesidad de contar con un ambiente seguro.

6.3. 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 COOPTENJO, incluyendo a los organismos directivos, asociados, funcionarios y terceros que estén realizando labores o tenga algún manejo y gestión de la información de la cooperativa.

Todas las descripciones de cargos deben contener detalles referentes a las responsabilidades específicas para el cumplimiento de las Políticas de seguridad de la organización.

Tener acceso a un sistema de información trae consigo 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 COOPTENJO de evitar brechas de seguridad. Estas responsabilidades deben ser claras para el usuario al momento de autorizársele el acceso, para así asegurar que todos los usuarios de la información y de los recursos tecnológicos de la entidad, cumplan con

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 8 de 42

las políticas de seguridad establecidas.

6.4. USUARIOS

Los usuarios responsables de la información y equipos de COOPTENJO deben:

- Aceptar cumplir las Políticas de seguridad de la empresa.
- Aceptar la responsabilidad personal de proteger los equipos de cómputo y la información de COOPTENJO contra pérdida, modificaciones no autorizadas y accesos de terceras personas.
- Los trabajadores de COOPTENJO deben firmar un documento especificando que aceptan la responsabilidad de cumplir las Políticas de Seguridad Informática de la empresa.
- Los acuerdos firmados por los funcionarios de COOPTENJO deben ser claros, fáciles de entender y deben incluir ejemplos de lo que constituye una violación de seguridad.

6.5. ASUNTOS OPERACIONALES Y DE MANEJO

Para que las Políticas y estándares de seguridad sean efectivos, COOPTENJO debe utilizar métodos de trabajo, prácticas de negocios y procedimientos en el contexto de cumplir con las estrategias de la Cooperativa. 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 COOPTENJO.

El Consejo de Administración es el encargado de establecer y aprobar políticas, los controles de manera que protejan la infraestructura tecnológica y la información de la entidad. Todas las acciones tomadas deben estar encaminadas a proveer un servicio de calidad, cumpliendo con los objetivos estratégicos y mejorando su ventaja competitiva.

6.6. RESPONSABILIDAD EN EL USO DE LA INFORMACIÓN Y RECURSOS

La Cooperativa COOPTENJO 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 las mismas.

Los funcionarios que tengan conocimiento de cualquier uso indebido de la información usada en COOPTENJO, deben notificarlo al Departamento de Tecnología y Informática.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Dirección de Tecnología Informática

Los funcionarios deben utilizar la información de COOPTENJO exclusivamente para fines relacionados con la Cooperativa, quedando prohibido explícitamente cualquier uso comercial y/o privado no autorizado.

Cada funcionario y/o tercero que tenga a su cargo un computador o conexión a COOPTENJO 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 la instalación y el uso indebido de cualquier software no autorizado por COOPTENJO.

Cada funcionario y/o tercero que interactúe con COOPTENJO 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 COOPTENJO 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 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, COOPTENJO responsabilizará al propietario de la misma.

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

6.7. USO SEGURO DE INTELIGENCIA ARTIFICIAL

El uso de herramientas, plataformas o servicios de inteligencia artificial deberá ser autorizado por COOPTENJO y estar alineado con el SGSI, la protección de datos personales, la confidencialidad de la información y la gestión de riesgos y política IA. Se prohíbe ingresar, cargar, copiar o procesar en herramientas de IA no autorizadas información confidencial, restringida, sensible, datos personales, información financiera, información de asociados, credenciales, código fuente, documentos internos o cualquier información de COOPTENJO que no haya sido expresamente aprobada para dicho uso. Todo uso institucional de IA deberá contar con evaluación del comité.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 10 de 42

6.8. PROPIETARIOS Y USUARIOS DE INFORMACIÓN

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

6.8.1. Usuarios de la información

Son usuarios de información todas las personas que directa o indirectamente, tengan algún tipo de relación con COOPTENJO, dándole esta característica el uso de los recursos de la Cooperativa, tomando en cuenta esta definición, son usuarios: los asociados, funcionarios, proveedores, aliados estratégicos, directivos y delegados.

Al tener el calificativo de usuario de información de COOPTENJO, deben cumplir con todas y cada una de las políticas y estándares expuestos por la entidad en lo que a seguridad informática y de la información se refiere.

6.8.2. Los Propietarios de la Información

Son propietarios de información, todas aquellas personas que trabajan en COOPTENJO. Por lo tanto, son responsables de protegerla adecuadamente, clasificarla y 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).

6.8.3. Los Propietarios de Infraestructura

Son propietarios de infraestructura, todos los funcionarios que dependiendo su grado de administración, utilicen recursos 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 la entidad.

 ENTIDAD COOPERATIVA DE AHORRO Y CRÉDITO	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 11 de 42

7. POLITICAS PARA COOPTENJO

7.1. POLÍTICAS QUE REGULAN LA ACTIVIDAD DE LOS USUARIOS

7.1.1. Responsabilidad del personal

Todas las personas que laboran para COOPTENJO son responsables del cumplimiento de las políticas, normas, procedimientos y estándares vigentes en materia de Seguridad Informática y de la información.

7.1.2. Validez de la información

Toda información, enviada, recibida, guardada electrónicamente dentro del COOPTENJO, debe y será considerada válida para cualquier proceso de carácter legal dentro y fuera de la Cooperativa.

7.1.3. Entrenamiento y difusión de las políticas de Seguridad Informática

Todas las personas que laboran para COOPTENJO y terceros que trabajen para la Cooperativa deberán ser capacitadas en lo que se refiere a las políticas, normas, procedimientos y estándares de Seguridad Informática.

7.1.4. Sistema de administración y monitoreo de usuarios

Todas las personas que laboran para COOPTENJO y terceros que trabajen para el mismo, deberán ser identificadas y autorizadas por el sistema central de administración de usuarios de la organización.

7.1.5. Uso de los recursos informáticos e información

Las personas que laboran para COOPTENJO deben ser responsables de utilizar de manera segura y en beneficio de la empresa la información y todos los recursos informáticos a su disposición.

7.1.6. Uso de herramientas que comprometen la seguridad

El uso de herramientas especializadas de intrusión y diagnóstico de seguridad está restringido a labores de administración de seguridad, en caso de requerirse su utilización deberá ser aprobada por el Departamento de Tecnología Informática.

7.1.7. Acceso a los sistemas de información

Las personas que laboran para el COOPTENJO deben tener acceso monitoreado y

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 12 de 42

controlado a los sistemas de información para el desarrollo de sus actividades.

7.1.8. Responsabilidad sobre la identidad de usuarios

Los identificadores de usuario y las contraseñas definidas en los sistemas de información de COOPTENJO son de exclusiva responsabilidad de la persona a la cual fueron asignados. Es por eso, que su carácter es personal e intransferible y el usuario debe seguir las recomendaciones emitidas para la creación de contraseñas seguras.

7.1.9. Personal con acceso privilegiado

Todos los funcionarios que por sus funciones tienen acceso privilegiado a los Sistemas de información, deben actuar de acuerdo con las funciones para las cuales fueron asignados.

7.1.10. Protección contra virus

La Cooperativa debe proveer las herramientas necesarias para la protección de los recursos informáticos y la información de propiedad de COOPTENJO contra los virus informáticos y cualquiera de sus variantes que atenten contra la integridad, confidencialidad y disponibilidad de la información y de la infraestructura informática.

Los usuarios de los recursos informáticos e información de propiedad de COOPTENJO son responsables de utilizar estas herramientas para impedir el ingreso de esta clase de programas a la infraestructura informática de COOPTENJO.

7.2. POLÍTICAS QUE REGULAN LA OPERACIÓN DE LOS SISTEMAS DE INFORMACIÓN Y LAS PLATAFORMAS TECNOLÓGICAS

7.2.1. Roles, responsabilidades y procedimientos

La dirección de tecnología informática es responsable de crear los roles y perfiles que posteriormente el líder de cada área y propietario de la información definirán responsabilidades y accesos que tendrán los funcionarios a su cargo. La dirección de tecnología informática también creará procedimientos operativos que aseguren un ambiente de control y seguridad.

7.2.2. Cambios Tecnológicos

Todo cambio a un sistema de información debe ser aprobado formalmente por la Dirección de Tecnología Informática.

Los cambios que afecten la plataforma tecnológica deben ser formalmente aprobados por la Dirección de Tecnología Informática y debe velar por que este cambio contribuya y mantenga la seguridad existente.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 13 de 42

Bajo ninguna circunstancia el cambio a un sistema de información o una plataforma tecnológica puede ser aprobado, desarrollado e implantado por la misma persona.

Los cambios técnicos en los sistemas de información o en las plataformas tecnológicas deben ser documentados por el Departamento de Tecnología Informática y aprobados de acuerdo con la metodología de documentación aprobada por la Cooperativa.

7.2.3. Cambios laborales

Gestión Humana, líderes de proceso y Tecnología deberán coordinar el retiro, suspensión o modificación inmediata de accesos por ingreso, traslado, retiro, vacaciones, licencias, terminación contractual o cambio de funciones, conservando evidencia de la gestión realizada.

7.2.4. Documentación de los sistemas de información

Todos los sistemas de información deben contar con la documentación suficiente para mantener y dar continuidad a la Seguridad Informática y la operación. La responsabilidad de esta actualización recae sobre el Líder del sistema de información.

7.2.5. Legalización del software

Todo el software utilizado en plataformas propias o alquiladas administradas por COOPTENJO tendrá contrato formal de propiedad o licencia de uso.

7.2.6. Procesamiento y almacenamiento de la información

La plataforma tecnológica y los sistemas de información, bajo la administración de COOPTENJO, que procese o almacene información de la Cooperativa, debe cumplir con las políticas de Seguridad Informática.

En caso de ser un servicio prestado por terceros, se debe evaluar en el área de Seguridad Informática las posibles desviaciones en su cumplimiento.

8. POLÍTICAS QUE APOYAN LA CONTINUIDAD Y OPERACIÓN DEL NEGOCIO.

8.1. CONTINUIDAD DE NEGOCIO.

Cooptenjo debe garantizar la prestación del servicio y la protección de los derechos de los asociados cuando se presenten interrupciones del servicio por causas ajenas a la voluntad y que afectan directamente la venta y el servicio.

Cooptenjo debe realizar un plan de continuidad de negocio (PCN) donde se tengan en

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 14 de 42

cuenta:

- La identificación de los procesos críticos de la organización y los recursos necesarios para mantener los operativos.
- Planificación y documentación de los procedimientos para la recuperación de los procesos críticos.
- Identificación y capacitación del personal responsable de la implementación del plan de continuidad del negocio.
- Implementación de medidas de seguridad y control de acceso para asegurar la protección de los datos y recursos de la organización durante el proceso de recuperación.
- Pruebas y actualizaciones periódicas del plan de continuidad del negocio para garantizar su eficacia y relevancia.

Es importante que la política de continuidad del negocio se actualice periódicamente para asegurar que cumpla con los requisitos cambiantes de la organización y las mejores prácticas de seguridad informática.

8.2. CONTINUIDAD DE LA PLATAFORMA TECNOLÓGICA

La plataforma tecnológica y los sistemas de información de COOPTENJO o de terceros en los cuales se soportan los procesos críticos del negocio, deben poseer planes de contingencia y los recursos necesarios que aseguren su continuidad. Estos son responsabilidad de la dirección de Tecnología Informática con apoyo del equipo del departamento.

En caso de que estos sistemas de información y plataformas tecnológicas sean administrados por un tercero, dichas exigencias deben ser consideradas en el contrato de servicios con COOPTENJO.

8.3. SEGURIDAD FÍSICA

Las instalaciones y equipos informáticos propios o de terceros en los cuales se procese o almacene información de COOPTENJO deben contar con mecanismos de seguridad física que garanticen la protección de los recursos informáticos en lo referente al acceso físico y las condiciones mínimas de operación que garanticen la disponibilidad, confidencialidad e integridad de la información.

8.4. PROPIEDAD DE LA INFORMACIÓN

La información relacionada con el negocio de COOPTENJO que se encuentre almacenada en recursos informáticos a su servicio, pertenece a COOPTENJO, a menos que, un contrato formal escrito exprese lo contrario.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 15 de 42

8.5. CONFIDENCIALIDAD DE LA INFORMACIÓN

Toda la información de COOPTENJO debe estar clasificada como: confidencial, restringida o pública, de acuerdo con el dueño del proceso que la genera. Esta clasificación debe verse reflejada en el sistema de gestión de seguridad de la información. Los funcionarios deben dar un buen uso de acuerdo con su clasificación, en caso de duda, la información debe ser considerada como confidencial.

La información generada, recibida, procesada, almacenada o transmitida en desarrollo de actividades institucionales pertenece a COOPTENJO o se encuentra bajo su responsabilidad, salvo disposición legal o contractual en contrario. Su uso deberá limitarse a finalidades autorizadas.

9. POLÍTICAS QUE REGULAN EL INTERCAMBIO Y PROTECCIÓN DE LA INFORMACIÓN

Cualquier información que entre o salga de COOPTENJO por medio magnético, transmisión electrónica o hardware, deberá tener los mecanismos de autenticación, autorización y registro de eventos que aseguren la confidencialidad, integridad, auditabilidad y disponibilidad de esta información.

9.1. ALIANZAS O CONVENIOS CON PROVEEDORES O PERSONAL EXTERNO

Cualquier alianza o convenio de procesamiento de información con proveedores o personal externo debe contar con los mecanismos de seguridad, integridad y auditabilidad, de tal forma que cumplan los estándares y políticas definidas por la entidad.

Para todo el intercambio de información confidencial y restringida se deben establecer acuerdos de confidencialidad.

10. POLÍTICAS DE ADMINISTRACIÓN DEL MODELO DE SEGURIDAD

10.1. GRUPO DE SEGURIDAD INFORMÁTICA

Se debe crear el grupo de Seguridad Informática de COOPTENJO designado por la gerencia general. Este grupo se reunirá cuando las circunstancias lo ameriten para:

- a. Realizar seguimiento al cumplimiento de políticas.

 ENTIDAD COOPERATIVA DE AHORRO Y CRÉDITO	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 16 de 42

- b. Analizar el impacto de incidentes de seguridad.
- c. Servir como garante de los proyectos de seguridad Informática.
- d. Revisar o realizar actualizaciones al Modelo de Seguridad Informática.

10.2. IMPLANTACIÓN DE LA SEGURIDAD

Los encargados de administrar las plataformas tecnológicas y los sistemas de información por parte de COOPTENJO son los responsables de implantar las medidas de seguridad aprobadas por el grupo de Seguridad Informática y de ejecutar las acciones necesarias para su mantenimiento.

10.3. CUMPLIMIENTO DE REGULACIONES

Las definiciones del Modelo de Seguridad Informática deberán cumplir con las regulaciones que al respecto sean emitidas por organismos de regulación colombiana.

11. POLÍTICAS DE SEGURIDAD

11.1. POLÍTICAS DE CONOCIMIENTO GENERAL

Se denominan políticas de conocimiento general, todas aquellas políticas, implícitas en todas y cada una de las tareas desarrolladas dentro del COOPTENJO.

Dentro de este nivel de políticas se encuentran:

- a. Todos los usuarios, son responsables por garantizar la Confidencialidad, integridad, y disponibilidad de la formación que se les ha sido entregada.
- b. 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.
- c. Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.
- d. El correo electrónico no se usará para: envío de materiales de uso no relacionado con el trabajo asignado, envío de material masivo, envío de material que atente contra la dignidad. (Entiéndase por material masivo todo aquel que sea ajeno a la Cooperativa, tal

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	
	Junio 2026	
	Dirección de Tecnología Informática	Página 17 de 42

como cadenas, publicidad y propaganda comercial, política o social, etc.).

- e. Para reforzar la seguridad de la información, el usuario conforme su criterio, deberá hacer respaldos de su información o en su efecto pedir al Departamento de Tecnología Informática que se realice un respaldo dependiendo de la importancia y frecuencia de modificación de la misma.
- f. Queda estrictamente prohibido inspeccionar, copiar y almacenar; hardware, software y demás fuentes que violen la ley de derechos de autor.
- g. Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red de COOPTENJO, de acuerdo con las políticas que en este documento se mencionan.
- h. Los usuarios deberán solicitar apoyo al Departamento de Tecnología Informática, para cualquier problema relacionado con la violación de alguna de las políticas de seguridad.
- i. El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud del Departamento de Tecnología Informática, con el fin de contribuir a la seguridad de los recursos de administración de la información.
- j. El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.
- k. Si el usuario hace uso de medios de almacenamiento personales, éstos serán controlados por la Solución Antivirus en la computadora del usuario o por el equipo designado para tal efecto.
- l. El usuario deberá comunicarse con el Departamento de Tecnología Informática en caso de problemas de virus para buscar la solución.

11.2. IDENTIFICACIÓN Y AUTENTICACIÓN

COOPTENJO maneja un único dominio de autenticación de usuarios, la administración de las políticas, estándares, procedimientos de seguridad toman como base el dominio, todos los usuarios de información en COOPTENJO, deben ser autenticados por el dominio antes de hacer uso de cualquier recurso.

Identificación: Es el proceso cuando el usuario se da a conocer en el sistema, para esto se utiliza un identificador único, los nombres posibles para este identificador único son:

- a. ID, cuenta, usuario, login.

Autenticación: Es la verificación del usuario ante el sistema, para esto se utiliza la clave

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 18 de 42

(password).

11.2.1. Administración de cuentas

Las cuentas de usuario deben ser administradas así:

- Asignación de acuerdo a el rol que cumple el usuario.
- Debe ser asignada con un horario determinado para el cargo y rol que cumple el responsable de la cuenta.
- Los sistemas en los cuales estas cuentas sirven de identificación deben proveer los mecanismos de Auditabilidad, que permitan el monitoreo constante de las cuentas.
- Todas las cuentas deben tener un periodo de vigencia que va de acuerdo con la labor desempeñada por el usuario, esta labor está ligada al tiempo de la tarea o proyecto.

11.2.2. Cuentas Inactivas/ ID de usuarios Inactivos

Una cuenta inactiva no puede proveer acceso autorizado a los sistemas de información de COOPTENJO.

Una cuenta puede estar inactiva por varias razones:

Ausencia del usuario autorizado (licencias médicas, viajes de negocios)

- Cuando el usuario autorizado deja de trabajar en la organización.
- El acceso ya no es necesario para ese usuario.
- Cuando una cuenta "temporal" se deja habilitada.
- Cuentas especiales se dejan habilitadas para usos específicos (mantenimiento, pruebas, consultor).

El Departamento de Tecnología Informática y los designados como administradores son responsables de realizar la inactivación o activación de las cuentas según sea requerido por el área de Gestión Humana.

11.2.3. Uso y protección de claves

Las claves son el medio principal de autenticar el acceso de un usuario a un dispositivo, una aplicación o a información privilegiada, por esta razón deben ser cuidadosamente controlados.

Todos los puntos de acceso COOPTENJO deben ser controlados por claves, incluyendo:

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 19 de 42

- a. Datos
- b. Sistemas de información
- c. Sistemas de correo
- d. Equipos de red (routers, bridges, firewalls, switch's y equipos de control utilizados en la red, pero no de acceso directo por los usuarios).
- e. Las claves que se utilicen deben cumplir con los estándares mínimos definidos para cada plataforma.

11.2.4. Usos no permitidos

- a. No tener una única clave asignada para todas las tareas desempeñadas dentro de COOPTENJO.
- b. No debe obtener la contraseña de acceso de una cuenta de usuario sin la autorización del propietario.
- c. No debe divulgar la clave personal a otros usuarios.
- d. No debe recibir la contraseña de otro usuario.
- e. No debe dejar escrita la clave o claves en lugares visibles o de fácil acceso (notas, papeles, cuadernos, libretas etc...)

11.3. DERECHOS DE PROPIEDAD INTELECTUAL

Esta Política aplica para cualquier elemento de software usado por COOPTENJO, el cual sea:

- a. Desarrollado internamente para uso en COOPTENJO.
- b. Diseñado para cumplir las necesidades específicas de un proyecto o compromiso adquirido.
- c. Licenciado por una tercera persona o entidad para el uso de COOPTENJO.
- d. En equipos de COOPTENJO.
- e. Por sus funcionarios durante su estancia en COOPTENJO (este derecho a la propiedad intelectual debe estar incluido en los contratos de empleo).
- f. Externamente por el personal de COOPTENJO.

 ENTIDAD COOPERATIVA DE AHORRO Y CRÉDITO	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 20 de 42

g. Para uso de COOPTENJO o pagado por COOPTENJO.

Las aplicaciones desarrolladas por funcionarios de COOPTENJO para uso interno deben ser desarrolladas usando software de propiedad, licenciado o autorizado a COOPTENJO.

La Dirección de Tecnología Informática deben autorizar cualquier desarrollo de software para COOPTENJO.

Todo el software utilizado por COOPTENJO para trabajar o desarrollar debe estar licenciado por COOPTENJO y debe ser usado únicamente bajo los términos y condiciones definidos en las licencias.

Todo el software obtenido desde fuentes externas o no autorizadas debe ser usado con precaución. Este software no debe ser utilizado en equipos del COOPTENJO o para uso COOPTENJO (por ejemplo, software no solicitado a vendedores) sin antes haber obtenido autorización el Departamento de Tecnología Informática.

Uso restringido de software con licencia temporal de uso o “Shareware”.

11.4. CORREO ELECTRÓNICO (E-MAIL) COORPORATIVO

El e-mail debe ser utilizado únicamente con propósitos de negocios, usando términos consistentes con las políticas de la organización. Los archivos anexos al e-mail deben permitirse únicamente después de haber determinado las características de la información, pertinencia del receptor (cliente interno y/o tercero,) y permisos correspondientes en caso de no hacer parte de las funciones del cargo. Siempre se debe revisar que los archivos que se van a enviar estén libres de código malicioso y que además no contengan información inapropiada.

11.4.1. Validez de la información enviada y recibida por medio del correo electrónico

Toda la información que se envíe y reciba por medio de correo electrónico, debe ser tratada como un documento válido y real, para trámites internos, cualquier información que se envíe o reciba será salvaguardada por la seguridad de la información de COOPTENJO.

11.4.2. E-mail entrante

Los e-mails entrantes deben tratarse con gran cuidado debido a que son un riesgo de seguridad. Los archivos que vengan anexos a los e-mails únicamente deben ser abiertos después de haber sido revisados por la herramienta antivirus instalada y permitida por la cooperativa, para minimizar el riesgo del código malicioso y de virus.

11.4.3. Intervalo de retención de e-mail

El intervalo de tiempo que deben ser almacenados los e-mails debe ser definido de acuerdo a las

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 21 de 42

reglamentaciones legales e internas vigentes y debe ser cumplido por todos los miembros de COOPTENJO.

11.4.4. Información no solicitada

Los e-mails que contengan información no solicitada o sospechosa deben ser tratados con gran cuidado y alineados al manual de correos maliciosos.

11.4.5. Cadenas de favores y listas de distribución

Los recursos de correo electrónico asignados por COOPTENJO no pueden ser empleados para el reenvío de e-mail en cadenas de favor, también se prohíbe utilizar estos recursos para la inscripción en listas de distribución.

11.4.6. Uso exclusivo del correo electrónico corporativo

- a. Todos los empleados deben utilizar únicamente el correo electrónico corporativo proporcionado por la empresa para llevar a cabo cualquier actividad relacionada con el trabajo.
- b. Prohibición del uso del correo electrónico personal: los empleados no tienen permitido utilizar su correo electrónico personal para enviar o recibir correos electrónicos relacionados con su trabajo. Cualquier uso de correo electrónico personal para fines laborales puede dar lugar a consecuencias disciplinarias
- c. Sensibilización de los empleados: todos los empleados deben ser informados y capacitados sobre las buenas prácticas de seguridad de correo electrónico y de seguridad de la información en general.
- d. Monitoreo y auditoría: la cooperativa se reserva el derecho de monitorear y auditar el uso del correo electrónico corporativo por parte de los empleados para garantizar el cumplimiento y el buen uso del servicio con el fin de proteger la información crítica y sensible de la cooperativa.

11.5. SEGURIDAD FÍSICA

Todas las instalaciones físicas, equipos, componentes relacionados y recursos de COOPTENJO deben estar protegidos de accesos físicos no autorizados, daños, robos y otros riesgos.

Se debe proveer seguridad adecuada en las instalaciones y estas deben estar bien mantenidas y limpias.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 22 de 42

11.5.1. Manejo Del Hardware

Todos los funcionarios de COOPTENJO deben tener en cuenta que se prohíbe:

- a. El daño físico de los equipos o el daño en la infraestructura física, lógica o eléctrica.
- b. Conexión, desconexión o reubicación de equipos o cambios de configuración de los mismos sin autorización expresa. Así como la conexión de medios externos y/o equipos que no pertenecen a la Entidad.
- c. Instalación de dispositivos y tarjetas de acceso remoto, módems, RDSI, routers o cualquier otro dispositivo de comunicaciones en servidores y estaciones de trabajo o redes de COOPTENJO, sin autorización expresa.
- d. Instalación de equipos de comunicaciones para intercambio de información (switches, redes) entre ordenadores de red de la Cooperativa y otros ajenos a dicha red, sin autorización expresa.
- e. Uso de la red o servidores de la Cooperativa para conseguir acceso no autorizado a cualquier estación de trabajo.
- f. Realizar con conocimiento de causa cualquier acto que interfiera en el correcto funcionamiento de los servidores o estaciones de trabajo, terminales, periféricos, red de comunicaciones, etc.
- g. Agregar o quitar programas sin previa autorización.
- h. Cambiar la configuración predeterminada de los equipos clientes o servidores sin previa autorización.
- i. El equipo debe ser bloqueado por ausencia temporal o permanente del usuario durante la jornada laboral.
- j. El equipo a cargo del funcionario debe ser entregado al área de tecnología cuando este tenga su periodo de vacaciones, licencia, sanciones u otro evento que no represente una labor de sus funciones contratadas.
- k. Se prohíbe adherir stickers, calcomanías, etiquetas no institucionales, cintas, marcas, adhesivos decorativos o cualquier elemento físico sobre los equipos tecnológicos asignados por COOPTENJO, salvo autorización expresa de la Dirección de Tecnología Informática. Solo se permitirán etiquetas institucionales de inventario (plaqueta activo fijo), identificación, control patrimonial, seguridad o soporte técnico definidas por la Cooperativa.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 23 de 42

- I. El usuario deberá conservar los equipos asignados en buen estado físico, sin alteraciones, marcas, adhesivos, rayones, modificaciones externas o internas no autorizadas.

11.5.2. Protección contra virus

Los virus son programas diseñados para propagarse a través de computadoras y redes típicamente afectan el procesamiento normal y los servicios dañando, corrompiendo o borrando archivos e información.

COOPTENJO tiene el riesgo de recibir virus y como resultado de esto puede afectar inadvertidamente a clientes o terceros.

Los usuarios deben usar versiones aprobadas de software antivirus. La versión más actualizada de software antivirus debe ser instalada y usada en todos los computadores personales y servidores para revisar y vacunar archivos y discos antes de que la información sea usada y antes de que sea enviada a clientes o terceros.

Los funcionarios de COOPTENJO deben seguir estrictamente las instrucciones sobre el uso de antivirus en cada equipo, así como en el reporte de incidentes, por lo problemas presentados por virus que se presenten en la información que les ha sido encomendada.

COOPTENJO por medio del Departamento de Tecnología Informática, debe proveer los procedimientos para: prevención, detección y recuperación en caso de problemas con virus.

Los usuarios de COOPTENJO deben utilizar los procedimientos, herramientas y demás medios expuestos por COOPTENJO para el manejo de incidentes, por ningún motivo los usuarios deben hacer uso de procedimientos, herramientas y medios de personas ajenas a COOPTENJO para la solución de problemas.

11.6. SEGURIDAD DE BASES DE DATOS

Una base de datos es "Un conjunto de datos integrados, adecuado a varios usuarios y a diferentes usos", es el propio uso concurrente de los datos el que plantea problemas de seguridad que el funcionario encargado (administrador de la base de datos DBA) debe lidiar con las facilidades que le proporciona el Sistema de Gestión de bases de datos (SGBD).

Las políticas de seguridad de bases de datos se refieren a los aspectos que implican:

- a. El Sistema de gestión de Bases de datos (SGBD)
- b. El administrador de la base de datos (DBA),
- c. La seguridad física
- d. La seguridad lógica de los datos y el control de acceso
- e. La documentación

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 24 de 42

11.6.1. El Sistema de gestión de Bases de datos (SGBD)

Es un paquete generalizado de software, que se ejecuta en un sistema computacional anfitrión, centralizando los accesos a los datos y actuando de interfaz entre los datos físicos y el usuario. Las principales funciones que debe cumplir un SGBD se relacionan con la creación y mantenimiento de la base de datos, el control de accesos, la manipulación de datos de acuerdo con las necesidades del usuario, el cumplimiento de las normas de tratamiento de datos, evitar redundancias e inconsistencias y mantener la integridad. El SGBD facilita normalmente mecanismos para prevenir los fallos (subsistema de control), para detectarlos una vez que se han producido (subsistema de detección) y para corregirlos después de haber sido detectados (subsistema de recuperación).

En COOPTENJO, cualquier sistema de información que se diseñe y maneje bases de datos, debe contar con un sistema de gestión de bases de datos.

11.6.2. El administrador de la base de datos (DBA)

El Administrador de bases de datos es el funcionario que coordina todas las actividades del sistema de bases de datos tiene un buen conocimiento de los recursos y necesidades de información de la organización.

Las funciones del administrador de bases de datos incluyen:

- Definición de esquemas y mantenimiento de las bases de datos
- Definición de métodos de acceso y estructuras de almacenamiento
- Modificación de esquemas y organización física
- Definición de acceso a la base de datos
- Especificar restricciones de integridad
- Actuar como enlace con los usuarios
- Monitoreo y optimización de las bases de datos

En COOPTENJO, debe existir un grupo administrador de bases de datos que se responsabilice de las funciones de administración de bases de datos. Este grupo debe mantener una estructura funcional acorde a la plataforma técnica establecida.

11.6.3. La seguridad física de los datos

Se refiere a la protección de los datos que deberá llevarse a cabo contra fallos físicos, fallos lógicos y fallos humanos (intencionales o no). Estos fallos pueden alterar indebidamente los datos y dañarlos con lo que la base de datos, ya no puede servir a los fines para los que fue creada. Involucra aspectos como:

- Los mecanismos para prevenir los fallos (subsistema de control).

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 25 de 42

- b. Para detectarlos una vez que se han producido (subsistema de detección).
- c. Los mecanismos para corregirlos después de haber sido detectados (subsistema de recuperación y copias de seguridad).

11.6.4. La seguridad lógica de los datos

Se refiere al control de acceso a las bases de datos. El Sistema de Gestión de la Bases de Datos debe proveer técnicas y mecanismos que permitan al administrador de la base de datos (DBA) el control de acceso a los datos, de tal manera que se garantice la integridad, la confidencialidad y la disponibilidad de la información en los ambientes de trabajo existentes (producción, pruebas y desarrollo). Esto involucra aspectos como:

- a. Definición de usuarios y roles
- b. Autorizaciones de acceso a los datos
- c. Registros de actividades de los usuarios
- d. Operaciones y opciones de auditoría

Es función del administrador de la base de datos, lo que corresponde a la creación de cuentas de usuarios, la concesión y revocación de privilegios y la asignación de niveles de acceso a los datos para los diferentes usuarios (desarrolladores, usuarios de pruebas y usuarios finales, administradores y personal de seguridad).

11.6.5. La documentación

Existe una estrecha relación entre el sistema de gestión de bases de datos (SGBD) y la administración de las bases de datos (DBA), que se soporta por la documentación técnica. Esta información es necesaria para evaluar el impacto del mantenimiento, actualización y administración de las bases de dato, así como para contemplar el esfuerzo de las tareas que se deben estructurar por parte del área de administración.

Para todo sistema de información que utilice el concepto de Bases de datos y que sea desarrollado internamente dentro de la Cooperativa o contratado a terceros, es requisito contar con la siguiente documentación:

- a. La estructura de la base de datos.
- b. El diccionario de la base de datos.
- c. Modelos de entidad-relación
- d. Diseños físicos
- e. Diseños lógicos
- f. Características operativas.
- g. Diseño funcional y las interfaces con otros procesos.
- h. Controles existentes.
- i. Procesos de respaldo.
- j. Procesos de recuperación

 ENTIDAD COOPERATIVA DE AHORRO Y CRÉDITO	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 26 de 42

k. Esquemas de seguridad lógica

11.7. CLASIFICACIÓN Y ACCESO A LOS DATOS

La clasificación de la información determina los controles y el nivel de protección requeridos. La responsabilidad de clasificar la información, el nivel y el costo de su protección recae en los propietarios de la información, propietarios de infraestructura y grupo de tecnología informática

Esquema de clasificación de la información

COOPTENJO tiene tres grandes categorías de información:

- Sensible/Restringida
- Privada/Confidencial
- Interna/No Restringida/Pública

11.7.1 Sensible/Restringida (alto riesgo, alto costo de protección)

El acceso no autorizado a la información Sensible/Restringida puede traer riesgos muy graves para COOPTENJO, por lo que se deben aplicar muchos más controles.

Dentro de la información que puede ser considerada como Sensible/Restringida se incluye:

- Importante comercialmente o privada (que brinda ventaja competitiva)
- Registros financieros de COOPTENJO (toda la información financiera interna)
- Información de Recursos Humanos (Personal que labora en COOPTENJO)
- Información privada de los asociados
- Propuestas y contratos

De manera permanente en computadores portátiles no debe almacenarse información restringida, cuando esto no es posible. Deben definirse límites para la retención de información restringida en computadores portátiles.

Deben instalarse productos de encriptación y auditoria de la información para reducir las posibilidades de acceso a información restringida.

También debe ejecutarse la destrucción segura de los discos duros y medios magnéticos que contengan o hayan contenido información restringida. por medio del método aprobado por

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 27 de 42

COOPTENJO.

Los funcionarios de tecnología informática de COOPTENJO deben ejecutar estos procedimientos.

11.7.2. Información Privada/Confidencial (Riesgo Medio, Costo de protección medio a bajo)

Los accesos no autorizados a información Privada/Confidencial pueden dar como resultado aumento en los costos, pérdida de negocios y problemas legales para COOPTENJO. La mayoría de la información de COOPTENJO puede considerarse como Privada/Confidencial y no debe estar disponible para personas no autorizadas. Los derechos de acceso deben ser limitados/controlados para prevenir el acceso a información confidencial por parte de personas no autorizadas.

Deben instalarse productos de encriptación y auditoria de la información para reducir las posibilidades de acceso a información privada/confidencial.

También se debe ejecutarse la destrucción segura de los discos duros y medios magnéticos que contengan o hayan contenido información restringida por medio del método aprobado por COOPTENJO.

Dentro de la información que puede ser considerada como restringida se incluye:

- a. Información general de trabajo acerca de COOPTENJO, planes de mercadeo y clientes
- b. Información detallada de cartera
- c. Papeles de trabajo

11.7.3. Información Interna/Sin Restricción/Publica (Bajo riesgo, costo de protección bajo a medio)

Parte de la información de COOPTENJO es solamente para uso interno, pero no tendría consecuencias indeseables si es conocida por usuarios no autorizados. Otra parte de la información es considerada del dominio público. Los tenedores de información de dominio público no necesitan tener precauciones de seguridad especiales para prevenir el acceso no autorizado dado que todos los accesos a la información están autorizados. Sin embargo, la naturaleza de la información que es de dominio público requiere un cuidadoso escrutinio de su contenido.

Se debe ser cuidadoso para asegurarse que los derechos de acceso para usuarios que no laboren en COOPTENJO, que sean trabajadores temporales, contratistas y clientes y puedan tener acceso a las instalaciones y las redes de COOPTENJO, estén restringidos a la información Interna/No Restringida/Publica

 ENTIDAD COOPERATIVA DE AHORRO Y CRÉDITO	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 28 de 42

Dentro de la información que puede ser considerada como interna/sin restricción/pública se incluye:

- a. Información utilizada para el mercadeo de COOPTENJO
- b. Información (no financiera) referente a COOPTENJO

11.8. ACCESO A LA INFORMACIÓN EN EQUIPOS DE COOPTENJO

COOPTENJO se reserva el derecho de acceder toda la información usada por las personas que laboran en la organización, de acuerdo con las reglas definidas por los propietarios de la información e infraestructura, incluyendo la información de:

- a. Asociados, personas que laboran en la empresa, organizaciones externas
- b. Contenida en computadores, servidores, dispositivos de red y sistemas de correo electrónico localizados dentro o fuera de las instalaciones de COOPTENJO.
- c. Guardada en equipos de COOPTENJO o en equipos que se encuentren en las instalaciones de la entidad.
- d. Almacenada en archivos de datos de los sistemas de COOPTENJO.
- e. Almacenada por el personal que labora en COOPTENJO.
- f. Almacenada en backups o en copias de archivos.

En particular esta regla cubre:

- a. Información de COOPTENJO que esté almacenada en equipos que pertenezcan a contratistas o a personal que labora en o para COOPTENJO.
- b. Información de asociados usada y almacenada por COOPTENJO en equipos de proveedores o asociados.

Los usuarios deben dar acceso a su información si así lo requiere la persona indicada (Departamento de Tecnología Informática). En estos casos puede requerirse del uso de la clave del usuario para permitir el acceso para poder acceder a la información.

 ENTIDAD COOPERATIVA DE AHORRO Y CRÉDITO	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 29 de 42

11.9. ACCESO DE USUARIOS A LA INFORMACIÓN DE COOPTENJO

La información es un activo muy importante para COOPTENJO y como tal debe ser protegido siempre. El acceso no autorizado, el uso o la divulgación de información inciden en la competitividad de COOPTENJO, impactando los ingresos y destruyendo el valor de la información para la entidad.

El acceso de los usuarios a los sistemas, a la información, a las aplicaciones, o a los recursos de COOPTENJO debe ser limitado a las áreas directamente relacionadas con sus responsabilidades y tareas.

Las autorizaciones deben ser dadas por medio de un procedimiento formal y deben quedar documentadas. Los usuarios deben usar sus privilegios de acceso de una manera responsable y no debe realizar o intentar acceder a información para la cual no está autorizado.

11.9.1. Seguridad en las Comunicaciones de COOPTENJO

11.9.1.1. Conexiones Electrónicas

Las conexiones electrónicas de COOPTENJO con el exterior deben establecerse de acuerdo con las normas de seguridad informática definidas y con los mecanismos que aseguren, tanto la identidad de quienes realizan la conexión, como la confidencialidad, integridad, auditabilidad y disponibilidad de la misma.

COOPTENJO provee a sus trabajadores con la tecnología disponible en las áreas de telefonía IP, correo electrónico, VPN, bases de datos y otros sistemas informáticos para permitirles servir a los asociados de una manera más efectiva. El uso de estas herramientas tecnológicas brinda ventajas competitivas, pero al mismo tiempo presenta riesgos como virus, corrupción de información, brechas de seguridad y pérdida de la privacidad y la confidencialidad de la información del COOPTENJO y de sus asociados. Esta política define la posición de COOPTENJO respecto a:

11.9.1.2. Usos aprobados y prohibidos de estas tecnologías

Acceso a comunicaciones electrónicas enviadas o recibidas usando los recursos de COOPTENJO o almacenadas en los equipos de la organización.

11.9.1.3. Usos Aprobados

Las comunicaciones electrónicas en COOPTENJO deben ser utilizadas exclusivamente para los fines de la Cooperativa. El uso ocasional para fines personales es permitido mientras no interfiera con la productividad laboral. Toda la información y los mensajes almacenados dentro de los sistemas y equipos del Cooperativa serán tratados como si fueran relacionados con los negocios de COOPTENJO y deben estar de acuerdo a los estándares de contenido definidos por la

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 30 de 42

entidad.

Los sistemas de comunicaciones electrónicas y todos los mensajes procesados o generados por sistemas de comunicaciones, incluyendo las copias de respaldo, son considerados como propiedad de COOPTENJO.

11.9.1.4. Comunicaciones electrónicas con clientes

Las políticas que se aplican a las comunicaciones escritas también se aplican a las comunicaciones electrónicas y deben ser consistentes con los estándares de COOPTENJO. Material confidencial no debe ser transmitido utilizando Internet sin algún tipo de mecanismo de encriptación.

11.9.1.5. Acceso de los funcionarios de COOPTENJO a los sistemas de comunicación electrónica

COOPTENJO se reserva el derecho de examinar las comunicaciones electrónicas utilizando un muestreo estadístico y se reserva el derecho de utilizar herramientas automatizadas para buscar palabras o frases con el fin de localizar mensajes que vayan en contra de las políticas de la organización. El contenido y el uso de las comunicaciones electrónicas pueden ser monitoreados para actividades de investigación, seguridad o rutina, sin consentimiento o consentimiento previo del usuario. El acceso a esta información se hará con las políticas de tratamiento confidencial de la información.

Nadie puede leer las comunicaciones electrónicas de otra de las personas que labore en el COOPTENJO sin la autorización correspondiente.

Todas las comunicaciones electrónicas que se hagan utilizando los equipos del COOPTENJO son consideradas en posesión, custodia o control de la entidad. Como resultado, terceras personas, como dependencias del gobierno que realicen investigaciones en COOPTENJO, pueden acceder a esas comunicaciones electrónicas.

11.9.1.6. Usos prohibidos

Los empleados deben recordar que los recursos de COOPTENJO no deben ser utilizados de forma inapropiada. La suplantación de la identidad de otro usuario es prohibida. El nombre de usuario, la dirección de correo electrónico y la información relacionada debe reflejar su verdadero origen.

Reenviar información que provenga del correo interno de COOPTENJO a Internet o a terceras personas sin la debida autorización está prohibido.

COOPTENJO prohíbe explícitamente el uso de las comunicaciones electrónicas para cualquiera de los siguientes propósitos:

 ENTIDAD COOPERATIVA DE AHORRO Y CRÉDITO	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 31 de 42

- a. Realizar actividades criminales.
- b. Realizar negocios personales.
- c. Obtener acceso no autorizado a cualquier computador o entidad.
- d. Diseminación de cadenas de mensajes.
- e. Transmitir mensajes amenazantes.
- f. Diseminar, ver, bajar, almacenar, guardar o reenviar material que contenga información sexualmente explícita o material ofensivo.
- g. Bajar o almacenar materiales (incluyendo software) protegido por leyes de copyright.
- h. Diseminar de manera no autorizada documentos internos de COOPTENJO.
- i. Hacer comentarios negativos de COOPTENJO o sus asociados.
- j. Diseminar de forma intencional información que no sea veraz.

La violación de estas políticas puede llevar a la toma de acciones disciplinarias incluyendo el despido o la acción legal por parte de las autoridades competentes.

11.10. CONFIGURACIÓN DE LA RED

La red debe ser configurada y diseñada para tener un alto nivel de desempeño y seguridad al proveer control de los recursos y al acceso a la información.

11.10.1. Administración de la Red

El personal que se encargue del control de la red debe estar capacitado de una manera adecuada y será el encargado de preservar la estabilidad e integridad de los recursos de la red.

11.10.2. Acceso Remoto a la Red

El acceso remoto a la red y a sus recursos se dará únicamente después de que los usuarios hayan sido autenticados. La información debe viajar encriptada a través de la red y además los usuarios deben tener permisos de acuerdo a su cargo o funciones que desempeñen.

11.10.3. Defensa de la Red de Ataques Maliciosos

El hardware del sistema, el software, los sistemas operativos, las redes y los sistemas de comunicaciones, deben estar configurados adecuadamente y salvaguardado contra ataques

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 32 de 42

físicos e intentos de accesos no autorizados a través de la red.

11.10.4. Gestión de vulnerabilidades

COOPTENJO deberá identificar, evaluar, priorizar y tratar vulnerabilidades técnicas en sistemas, aplicaciones, infraestructura, comunicaciones y servicios críticos, mediante revisiones periódicas, actualizaciones, parches, hardening, pruebas controladas y seguimiento a planes de remediación

11.11. SEGURIDAD PARA INTERNET

- Solo se debe acceder a Internet por el canal contratado y aprobado por el COOPTENJO, está prohibido hacer conexiones no controladas ni autorizadas hacia Internet.
- Los usuarios de COOPTENJO sin excepción, deben solicitar por escrito, el permiso para conectarse a paginas diferentes a las autorizadas.
- Está prohibido enviar o recibir información confidencial de COOPTENJO sin una autorización previa.
- Todas las conexiones a Internet son monitoreadas y controladas por COOPTENJO.
- La Cooperativa puede deshabilitar cualquier cuenta de Internet en el momento que considere que la seguridad de la información ha sido violada.

11.12. AUDITORIA/MONITOREO

COOPTENJO debe realizar, mantener y demostrar control sobre el acceso y uso de recursos de los sistemas informáticos, manteniendo log's y registros de control que estén disponibles para su inspección. El Departamento de Tecnología Informática son los responsables de implementar todas las funciones de seguridad que sean requeridas para controlar el acceso y rastrear el uso del sistema. Esto incluye la inspección frecuente de los log's de auditoría y de los registros de control y el monitoreo diario de:

- Transmisiones de archivos
- Accesos al sistema desde cuentas de usuarios privilegiados
- Accesos a información sensible.
- Acceso a sistemas no autorizados.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 33 de 42

- e. Patrones no usuales, como accesos fuera del horario normal de trabajo e intentos no exitosos de entrada al sistema (detección de intrusos)

Las revisiones de auditoría enfocadas a cada una de las plataformas técnicas y a las instalaciones físicas deben ser hechas por los propietarios de la información con una frecuencia determinada para asegurar que se esté cumpliendo con las Políticas de Seguridad, estas revisiones deben ser informadas al área de seguridad del COOPTENJO.

11.13. POLÍTICAS DE RESPALDO DE INFORMACIÓN DE AUDITORIAS

Se denominan políticas de respaldo de información de auditorías, todas aquellas políticas tendientes a salvaguardar la información de control, de cualquier tipo y de cualquier aplicativo en funcionamiento dentro de COOPTENJO.

COOPTENJO debe realizar, mantener y demostrar control sobre el acceso y uso de recursos de los sistemas informáticos, manteniendo log's y registros de control que estén disponibles para su inspección.

11.13.1. Normas Generales de respaldo de Log's

Generalmente, todos los sistemas que entregan los proveedores cuentan con archivos de auditorías y log's, que, a decisión de los administradores de sistemas asignados, pueden habilitarse o deshabilitarse para que registren los sucesos sobre los sistemas mismos. Es política obligatoria y hasta tanto no se defina qué información es requerida, mantener habilitadas las máximas opciones de log's y auditorías permitidas, y crear el procedimiento de respaldo de estos archivos en su totalidad.

- a. Los Administradores del Sistema son responsables de implementar todas las funciones de seguridad que sean requeridas para controlar el acceso y rastrear el uso del sistema. Esto incluye la inspección frecuente de los log's de auditoría y de los registros de control y el monitoreo diario de los aplicativos en funcionamiento.
- b. Los Administradores del Sistema deben garantizar la disponibilidad y seguridad de la información correspondiente a las auditorías, log's y registros de control que existan en cada sistema de información.
- c. Los Administradores del Sistema son responsables, de garantizar el respaldo de la información correspondiente a las auditorías, log's y registros de control que existan en cada sistema de información.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 34 de 42

Los Administradores del Sistema deben garantizar la copia del contenido lógico y físico, de los sistemas de control informático correspondiente a las auditorías y log's, a un medio que cumpla con una serie de exigencias, tales como:

- a. Ser confiable: Minimizar las probabilidades de error.
- b. Estar en un lugar seguro: El medio que almacena los respaldos debe estar en un lugar seguro desde el punto de vista de sus requerimientos técnicos como humedad, temperatura, campos magnéticos, como de su seguridad física y lógica.
- c. La forma de recuperación sea rápida y eficiente: los administradores de los sistemas deben probar la confiabilidad del sistema de respaldo, no sólo para respaldar, sino que también para recuperar.

Mecanismos de comprobación. Se deben definir mecanismos de comprobación de las copias de seguridad, aunque los propios programas que las efectúan suelen disponer de ellos para verificar el estado de la copia, es conveniente planificar dentro de las tareas de seguridad, la restauración de una parte de la copia o de la copia completa periódicamente, como mecanismo de prueba y garantía.

La Nomenclatura de los respaldos debe identificar completamente el orden cronológico del respaldo, el nombre del sistema al cual pertenece, el tipo de archivo respaldado y precedencia o secuencia del archivo.

11.13.2. Frecuencia de realización de copias de seguridad de los datos correspondiente a las auditorías y log's

La realización de copias de seguridad ha de realizarse diariamente, éste es el principio que debe regir la planificación de las copias, sin embargo, existen condicionantes, tales como la frecuencia de actualización de los datos y el volumen de datos modificados, que pueden hacer que las copias se realicen cada más o menos tiempo.

11.13.3. Planificación de la copia

Las copias de seguridad se pueden realizar en diferentes momentos del día, incluso en diferentes días, pero siempre se han de realizar de acuerdo a un criterio, si es posible, la copia se debe realizar de forma automática por un programa de copia, y según la configuración de éste, se podrá realizar un día concreto, diariamente, semanalmente, mensualmente, a una hora concreta, o cuando el sistema esté inactivo. Todos estos y muchos más parámetros pueden estar presentes en los programas que realizan las copias de seguridad y deben permitirnos la realización únicamente de las tareas de supervisión.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 35 de 42

11.13.4 Tiempo disponible para efectuar la copia.

El tiempo disponible para efectuar la copia de seguridad de los datos correspondiente a las auditorias, log's, es importante, ya que el soporte utilizado, unidad de grabación y volumen de datos a almacenar, puede hacer que el proceso de grabación de los datos dure horas, y teniendo en cuenta que mientras se efectúa el proceso es conveniente no realizar accesos o modificaciones sobre los datos objeto de la copia, este proceso ha de planificarse para que suponga un contratiempo en el funcionamiento habitual del sistema de información.

11.13.5. Seguridad física y lógica

Respecto a las copias de seguridad de los datos correspondiente a las auditorias, log's. Se deben tener en cuenta los siguientes puntos:

- a. Deberá existir un administrador, entre cuyas funciones esté la de verificar la correcta aplicación de los procedimientos de realización de las copias de respaldo y recuperación de los datos.
- b. Los procedimientos establecidos para la realización de las copias de seguridad deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse el respaldo.

La realización de las copias de seguridad se basará en un análisis previo del sistema de información, en el que se definirán las medidas técnicas que puedan condicionar la realización de las copias de seguridad, entre los que se encuentran:

- a. Volumen de información a copiar. Compuesto por el conjunto de datos que deben estar incluidos en la copia de seguridad. Se debe realizar una copia completa de todos los archivos de log's y auditorias de todos los sistemas.

11.13.7. Dispositivo de almacenamiento

El respaldo de la información correspondiente a las auditorias y Log's, debe realizarse en dispositivos de almacenamiento con capacidad de mantener altos volúmenes de información. Es responsabilidad del Departamento de Tecnología Informática, determinar los medios requeridos en función de las necesidades y al volumen de información que se maneje.

Es recomendable que exista un servidor de respaldo con copias en medios ópticos o magnéticos de gran velocidad en su grabación y recuperación.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
	Dirección de Tecnología Informática	Página 36 de 42

12. POLITICA DE DISPOSITIVOS MOVILES

12.1. GENERALIDADES

Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, el Departamento de Tecnología Informática debe implementar controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

COOPTENJO pone a disposición de los funcionarios dispositivos móviles institucionales para facilitar el desempeño de sus labores y propende porque dichos funcionarios hagan un uso responsable de ellos.

Con el fin de dar cumplimiento al tratamiento definido para los activos de información, todos los involucrados en el alcance deben cumplir las siguientes directrices:

12.2 DIRECTRICES DE SEGURIDAD PARA EL USO DE DISPOSITIVOS MÓVILES QUE ACCEDAN A INFORMACIÓN DE COOPTENJO.

- El personal que haga uso del dispositivo móvil para almacenar o acceder a la información de los diferentes softwares de COOPTENJO, deberá:
- Solicitar a el Departamento de Tecnología Informática la autorización para ello, aceptando el cumplimiento de la política de dispositivos móviles.
- Aceptar las configuraciones de seguridad del dispositivo, y estas no podrán modificarse mientras se acceda o almacene información de la Cooperativa.
- Instalar y configurar un software de antivirus.
- Establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.
- Configurar el bloqueo de pantalla para un mínimo de 3 minutos de inactividad.
- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.
- Es de ser posible realizar el cifrado del dispositivo móvil.

12.3. DIRECTRICES DE SEGURIDAD PARA DISPOSITIVOS MÓVILES DE PROPIEDAD DE COOPTENJO.

- Está prohibido almacenar información personal en los dispositivos móviles asignados por COOPTENJO.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 37 de 42

- b. Está prohibido realizar instalación de aplicaciones no autorizadas por el Departamento de Tecnología Informática.
- c. Está prohibido hacer volcado de pila o reinstalación del sistema operativo por parte del usuario en el dispositivo.

12.4. DIRECTRICES DE SEGURIDAD PARA EL PERSONAL ENCARGADO DE CONFIGURAR LOS DISPOSITIVOS MÓVILES.

- a. Cumplir con los lineamientos dados en la presente política respecto a la configuración de los dispositivos móviles.
- b. Configurar sólo las cuentas organizacionales en los dispositivos de la COOPTENJO que tendrán acceso a la información de la Entidad.
- c. Para aquellos dispositivos que no son entregados por COOPTENJO, deben recibir correo de la persona que envió solicitud a Tecnología “aceptando el cumplimiento la política de dispositivos móviles, así como las configuraciones de seguridad establecidas”

12.5. PÉRDIDA DEL DISPOSITIVO.

En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de COOPTENJO, se debe reportar la pérdida a el Departamento de Tecnología Informática y al área administrativa lo más pronto posible.

12.6. AUDITORÍA Y REVISIÓN DE LA POLÍTICA.

En cualquier momento el grupo de Seguridad de la Información de COOPTENJO podrá hacer revisión del cumplimiento de la política directamente en los dispositivos móviles.

Las Auditorías internas o de tercera parte pueden realizar la verificación de las configuraciones de los equipos móviles y su cumplimiento con los lineamientos de esta política.

12.7. INCUMPLIMIENTO

El incumplimiento de las disposiciones establecidas en la presente Política por cualquiera de los actores definidos en su alcance será considerado una falta grave a las obligaciones de seguridad, confidencialidad, protección de datos, gestión de riesgos y cumplimiento de la Entidad.

Dependiendo de la naturaleza del vínculo con la cooperativa, el incumplimiento dará lugar a la aplicación de las medidas, procedimientos y sanciones previstos en el Reglamento Interno de Trabajo, Estatutos, los reglamentos de los órganos de administración y control, los

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 38 de 42

contratos laborales, contratos de prestación de servicios, acuerdos de confidencialidad, cláusulas de seguridad de la información y demás instrumentos normativos o contractuales aplicables

12.8. RESPONSABILIDADES

El grupo de Seguridad de la Información: Velar por el cumplimiento de la presente política, garantizando los niveles de seguridad adecuados para el uso de los dispositivos móviles institucionales.

El coordinador de Tecnología Informática: Designar el personal idóneo para que establezca y configure los dispositivos móviles, acogiendo los lineamientos de seguridad definidos en la presente política.

Personal: Hacer uso responsable de los dispositivos móviles acogiendo los lineamientos establecidos por COOPTENJO.

13. POLÍTICA DE VPN.

13.1. GENERALIDADES

Los usuarios que utilizan el servicio declaran conocer y aceptar las siguientes políticas de uso del servicio VPN.

Es importante mencionar que el uso inapropiado de los recursos dispuestos para los usuarios autorizados expone a COOPTENJO a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, como también problemas judiciales.

13.2. ALCANCE

Las normas mencionadas en el presente documento cubren el uso apropiado del sistema de Red Privada Virtual, para VPN SSL de la Cooperativa y aplica a todos los funcionarios, proveedores, contratistas y en general cualquier usuario

13.3. POLÍTICAS DE USO

- a. Sólo los usuarios previamente autorizados podrán utilizar los servicios de VPN, los que, además serán los responsables del correcto uso del servicio de acceso remoto.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 39 de 42
	Dirección de Tecnología Informática	

- b. Es de responsabilidad del usuario con privilegios VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.
- c. El uso de la VPN debe ser controlado utilizando una contraseña de autenticación fuerte, manteniéndola siempre en secreto.
- d. Las puertas de enlace VPN serán configuradas y administradas por el Departamento de Tecnología Informática.
- e. Mediante el uso de la tecnología VPN, los usuarios declaran conocer que sus computadores, ya sea de la Cooperativa o personales son una extensión de las redes de la Cooperativa y como tales, están sujetos a las mismas normas y reglamentos que se aplican a los equipos dentro de las áreas de la Cooperativa.

14. CONTROL DE CAMBIOS

Los cambios en los sistemas de aplicaciones del negocio pueden tener efectos óptimos o negativos para los servicios que se prestan y para el desempeño del sistema, así como en otras aplicaciones o servicios de la entidad.

La administración de los cambios consta de un conjunto de procedimientos y controles que son necesarios para asegurar que todas las modificaciones realizadas en el hardware, software, equipos y servicios deban ser solicitados formalmente, aprobados y probados adecuadamente para minimizar el riesgo de errores e irregularidades en el ambiente de producción. Por lo tanto, los cambios en cualquier componente deben ser aplicados y controlados de una manera consistente para de esta forma asegurarse que los servicios que se prestan no presenten impactos negativos.

Los estándares y procedimientos de control de cambios son vitales para todos los sistemas y ambientes en los que se compartan recursos, tales como los sistemas de infraestructura, las aplicaciones, los servidores y la red.

En ningún caso será posible instalar, alterar, configurar, ningún sistema que se encuentre en producción, sin antes haber cumplido con las etapas de control de cambios establecidas.

14.1. OBJETIVOS DEL CONTROL DE CAMBIOS

Los principales objetivos de la administración de cambios son asegurar que:

 ENTIDAD COOPERATIVA DE AHORRO Y CRÉDITO	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 40 de 42
	Dirección de Tecnología Informática	

- a. Los cambios son aplicados a documentos, programas, esquemas de bases de datos y otros ítems que están bajo el manejo de los administradores de la información.
- b. El cambio a los sistemas de información debe ser aplicado de una manera controlada, la estabilidad y seguridad del sistema no debe verse comprometida.
- c. El cambio, solicitud o tarea sobre los Sistemas de Información sólo se implementa por medio del cumplimiento de los términos establecidos en el procedimiento de catalogación.
- d. Cualquier modificación que se realice debe mantener la compatibilidad de todos los componentes del sistema.
- e. La información es y continuará siendo protegida ante cualquier cambio.
- f. Todas las entidades necesarias en la Cooperativa (Propietarios de la infraestructura, Propietarios de la información) debe ser informados de los cambios y estos deben aprobar la modificación antes de su ejecución.

14.2. CONSECUENCIAS DEL CONTROL DE CAMBIOS

La administración de Cambios asegura que:

- a. Los cambios son documentados de acuerdo a estándares de documentación aprobados.
- b. Se establecen guías para organizar por prioridades las diferentes fases de la implementación (basadas en beneficios, cambios técnicos o funcionales y urgencia).
- c. El riesgo de errores intencionales y no intencionales se minimiza.
- d. Los cambios y modificaciones tienen que haber sido autorizados y se debe haber probado que cumplan con los requerimientos o especificaciones requeridas.
- e. Se supervisa la transferencia de software desde el ambiente de desarrollo o pruebas al ambiente de producción.
- f. Los cambios de emergencia deben almacenarse en un log y deben ser controlados. se necesita obtener una autorización de los propietarios, aunque el cambio ya se haya realizado.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 41 de 42

14.3. APLICACIONES DEL CONTROL DE CAMBIO

La administración de Cambios aplica para:

- a. Aplicaciones nuevas
- b. Arreglos hechos a aplicaciones existentes (incluyendo cambios en los controles de seguridad y auditoria)
- c. Cambios en las configuraciones de software
- d. Nuevas versiones de software o actualizaciones
- e. Cambios en los parámetros del sistema
- f. Cambio en los usuarios en todos los sistemas
- g. Modificaciones al ambiente de hardware (Nuevos equipos, configuraciones)
- h. Modificaciones efectuadas en las comunicaciones.

15. REFORMAS DE LA POLÍTICA

La presente política, junto a sus etapas y funciones puede ser modificada total o parcialmente por el Consejo de Administración.

16. ASPECTOS NO CONTEMPLADOS

Los casos no previstos en la presente política serán resueltos acudiendo a las disposiciones sobre la materia emitidas por la Superintendencia de la Economía Solidaria, en su defecto, corresponderá al Consejo de Administración, quien tiene la facultad para su interpretación, resolver el caso.

17. VIGENCIA DE LA POLÍTICA Y SUS REFORMAS

La presente política y sus reformas posteriores entran en vigencia a partir de su aprobación por parte del Consejo de Administración y derogan las disposiciones anteriores que le sean contrarias.

Copia de la presente política se entregará a los miembros del Consejo de Administración, a los miembros del Comité de Riesgos, al Revisor Fiscal, al Gerente General y a todos los trabajadores de la Cooperativa, por los medios institucionales idóneos.

	POLÍTICA DE SEGURIDAD INFORMÁTICA DE LA INFORMACIÓN Y CIBERSEGURIDAD	Junio 2026
		Página 42 de 42

APROBACIÓN

La presente actualización de la Política Integral de Seguridad de la Información y Ciberseguridad de COOPTENJO, articulada formalmente con el Sistema de Gestión de Seguridad de la Información (SGSI), fue aprobada por el Consejo de Administración en reunión extraordinaria celebrada el veintiséis (26) de agosto de 2026, mediante Acuerdo No. 118, según consta en el Acta No. 794 de la misma fecha.

Dado en Tenjo, Cundinamarca a los veintiséis (26) días del mes de agosto de dos mil veintiséis (2026).

CONSEJO DE ADMINISTRACIÓN



JOHANNA TIBAQUIRÁ BERNAL

Presidente

Consejo de Administración



DIVA VIVIANA SOTELO PENAGOS

Secretario

Consejo de Administración