MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ELABORÓ	REVISÓ	APROBÓ
CESAR CIFUENTES ALZATE DIRECTOR DE INFORMÁTICA	OSCAR JAVIER ZABALETA URREGO GERENTE	CONSEJO DE ADMINISTRACIÓN MEDIANTE ACTA No. 1127 DEL 31 DE MAYO DE 2025

TABLA DE CONTENIDO

ELABORÓ	REVISÓ	APROBÓ
CESAR CIFUENTES ALZATE DIRECTOR DE INFORMÁTICA	OSCAR JAVIER ZABALETA URREGO GERENTE	CONSEJO DE ADMINISTRACIÓN MEDIANTE ACTA No. 1127 DEL 31 DE MAYO DE 2025

1 OBJETIVO GENERAL

Definir, presentar y adoptar las políticas generales de seguridad de la información establecidas por COOPEBIS y definir los lineamientos frente al uso y manejo de los activos de información permitiendo minimizar los riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de la información, y/o sistemas en donde se procese o interactúe la información de la Cooperativa.

2 OBJETIVOS ESPECIFICOS

- Identificación, valoración y gestión de los riesgos relacionados con Seguridad de la Información.
- Evitar pérdidas de Información con la implementación de buenas prácticas para la gestión de la Seguridad de la Información.

3 ALCANCE

Los lineamientos y directrices generales de seguridad de la información serán aplicados a todos los niveles de la Cooperativa, en su sede principal y sucursales a nivel nacional y a todos sus colaboradores, asociados, proveedores, operadores y aquellas personas o terceros que, debido al cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

a. Requisitos legales y/o reglamentarios

NORMA	DESCRIPCIÓN
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 23 de 1982	Sobre derechos de autor

CIRCULAR EXTERNA No. 36, 5 de enero de 2022 – Anexo 2	Por medio de la cual la Superintendencia de la Economía Solidaria de Colombia, establece los requerimientos de medios tecnológicos y de seguridad de la información que deben ser aplicadas por las cooperativas especializadas en ahorro y crédito y multiactivas e integrales con sección de ahorro y crédito vigiladas.
LEY ESTATUTARIA 1581 DE 2012	Ley de la república por la cual se dictan disposiciones generales para la protección de datos personales.

4 VOCABULARIO

a) **Activo:** Es todo aquello que posee valor para la cooperativa, por lo tanto, debe protegerse.

b) **Activos de información:** Conocimiento o datos que tiene valor para la organización o el individuo

c) **Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la Cooperativa. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado. La información debe clasificarse en términos de sensibilidad e importancia para la Cooperativa.

d) **Criptografía:** Refiere a técnicas seguras de información y comunicación derivadas de conceptos matemáticos y un conjunto de cálculos basados en reglas llamados algoritmos, para transformar mensajes de manera que sean difíciles de descifrar.

e) **Confidencialidad:** Considera que la información no se pone a disposición ni se revela a personal o a entidades no autorizadas.

f) **Custodio:** Es una parte designada de la Cooperativa, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

g) **Disponibilidad:** Posibilidad de que la información debe estar accesible en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

h) **Hardware:** Componentes físicos del computador, es decir, todo lo que se puede ver y tocar.

i) **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados.

j) **Información:** Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Cooperativa.

k) **Información confidencial:** Información que es propia de la cooperativa y de uso exclusivo de un grupo de empleados y/o contratistas. Su circulación está restringida y no debe ser compartida con personas externas al grupo de distribución, la divulgación a un tercero debe tener el aval de la Cooperativa.

l) En caso de ser conocida, utilizada o modificada por personal no autorizado puede impactar negativamente las finanzas y la reputación de la Cooperativa.

m) **Integridad:** La información debe ser precisa, coherente y completa desde su creación hasta su destrucción, debe ser inalterada ante accidentes o intentos maliciosos, siempre se debe prevenir modificaciones no autorizadas de la información.

n) **Propietario:** Es el cargo responsable de definir el nivel de clasificación de la información, dar las directrices de uso del activo, autorizar privilegios y definir el ciclo de vida de este.

o) **Redes:** Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información

p) **Seguridad de la Información:** Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la organización

q) **Servicios:** Aquí se consideran tanto los servicios internos, aquellos que una parte de la Cooperativa suministra a otra (por ejemplo, la gestión administrativa), como los externos, aquellos que la Cooperativa suministra a clientes y usuarios (por ejemplo, la comercialización de productos).

r) **Software:** Todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos. (Sistemas operativos, aplicaciones, etc.)

s) **Acción resolutiva:** Acción tomada para evitar la repetición de un incumplimiento mediante la identificación y tratamiento de las causas que la provocaron.

t) **Amenaza:** Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.

u) **Control:** Medida o acción que modifica un riesgo para prevenir su materialización.

v) Gobierno de seguridad de la información: Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas.

w) **Nivel de riesgo:** Evaluación del riesgo identificando su posible materialización frente al impacto y probabilidad de ocurrencia.

x) **Probabilidad:** Posibilidad que el riesgo se pueda materializar frente a un incidente de seguridad de la información.

y) **Políticas de seguridad:** Conjunto de directrices, lineamientos y reglas que permiten velar porque se resguarden los activos de información, aprobados por el consejo de administración.

z) **Riesgo residual:** Es el riesgo que queda después de aplicar los controles al riesgo identificado.

aa) **Servicios de computación en la nube:** Modelo para permitir un acceso de red conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o proveedor de servicios.

bb) **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas.

5 POLITICAS

5.1 Política de Seguridad de la Información

La Cooperativa para el Bienestar Social - COOPEBIS se compromete a proteger, preservar, y gestionar la confidencialidad, integridad y disponibilidad de la información que se utiliza en todos los procesos de la organización, mediante una gestión integral de riesgos y la implementación de controles, dando cumplimiento a los requisitos legales y reglamentarios orientados a la mejora continua y al alto desempeño del sistema de gestión de seguridad de la información, en concordancia con la misión y visión de la Cooperativa.

Objetivos: La política general de seguridad de la información tiene los siguientes objetivos:

- Gestionar los riesgos de seguridad de la información de manera integral.
- Cumplir con los principios de seguridad de la información.
- Establecer las políticas, procedimientos, metodologías e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los colaboradores, asociados y terceros de la Cooperativa.
- Gestionar los incidentes de seguridad de la información de forma eficaz, eficiente y efectiva.
- Dar cumplimiento a los requisitos legales y normativos en materia de seguridad de la información.
- Mantener la confianza de los colaboradores, asociados, terceros y partes interesadas.

Alcance: La presente política aplica para todas las partes interesadas que, por su rol, interactúen o hagan parte de la Cooperativa.

Responsabilidad: A continuación, se describen de forma general las responsabilidades relacionadas con seguridad de la información:

- La Gerencia General de COOPEBIS es responsable de garantizar que la seguridad de la información sea parte de la cultura organizacional.
- La Gerencia General de COOPEBIS velará por el cumplimiento y mantenimiento de las políticas de seguridad de la información.

- El director de Informática de COOPEBIS es responsable por la implementación y mantenimiento de los controles tecnológicos necesarios para mitigar los riesgos de seguridad de la información.
- El Oficial de Seguridad de la Información de COOPEBIS es el encargado de la seguridad de la información y es responsable de promover la seguridad de la información en la Cooperativa.
- Los colaboradores, asociados, terceros y partes interesadas de COOPEBIS tienen la responsabilidad de cumplir las políticas de seguridad de la información de la compañía.

Excepciones: Las posibles excepciones a los lineamientos definidos que se pueden tener en COOPEBIS son las siguientes:

- **Exenciones:** El Líder de un área puede solicitar la exención temporal de una o más obligaciones derivadas de los lineamientos de Seguridad de la información, basándose en una limitación económica derivada de su área.
- **Desviaciones:** El Líder de un área puede solicitar desviaciones en la aplicación de los controles de seguridad establecidos en las políticas de seguridad de la información para un producto o servicio específico y durante un período limitado de tiempo. Las desviaciones no suponen la no aplicación de controles, sino la aplicación de controles distintos a los descritos en el conjunto de documentos del sistema de gestión de seguridad de la información y que requerirán de un análisis de riesgo específico.

SANCIONES: Todos los colaboradores, asociados, terceros y partes interesadas de COOPEBIS que en el ejercicio de sus funciones utilicen la información y/o servicios TI de la Cooperativa, deben cumplir en su totalidad con las políticas de seguridad de la información.
El incumplimiento de las políticas de seguridad de la información, así como la violación de los procedimientos, manuales, guías o instructivos establecidos en temas de seguridad y las contempladas en las Leyes, Decretos y demás normas que en temas de seguridad soporten este sistema, conllevará consecuencias disciplinarias y/o legales de acuerdo con la normativa vigente.
A continuación, se detallan las políticas específicas que soportan el cumplimiento de la política general.

5.2 Política para el uso de dispositivos móviles

Objetivo: El objetivo de la política es definir las directrices de seguridad para proteger la información de la Cooperativa gestionada a través de dispositivos móviles y las buenas prácticas a aplicar por parte de los usuarios, con el fin de minimizar los riegos frente a

ataques interno y externos, que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, hagan uso de algún dispositivo móvil en la Cooperativa.

Lineamientos:

Se entienden por dispositivos móviles a aquellas computadoras con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para una función, entre los más comunes se encuentran:

- Teléfonos inteligentes y Tabletas.
- Relojes inteligentes
- Agendas digitales
- Calculadoras inteligentes
- Videoconsolas portátiles
- Reproductores digitales
- Cámaras fotográficas digitales / Cámaras de video digitales
- Robots
- Tarjetas inteligentes
- Portátiles

Para aquellos dispositivos móviles suministrados por la Cooperativa, el área de sistemas debe asegurar, como mínimo, los siguientes requisitos de seguridad:

- Contar con un antivirus
- Contar con un cifrado para asegurar la integridad de la información
- Configurar los controles de acceso (Usuario y contraseña)
- Contar con software licenciado.
- Los equipos no deben utilizar software que permita realizar ataques informáticos.
- Los dispositivos deben estar actualizados con las últimas versiones de software.

Los dispositivos móviles de propiedad de la Cooperativa son para uso estrictamente laboral.

El área de gerencia debe asignar a un único usuario la custodia de los dispositivos móviles y llevar un control de estos.

El custodio del dispositivo móvil es responsable de dar un tratamiento seguro a la información almacenada en éste aplicando los siguientes lineamientos:

- No descuide el dispositivo móvil dejándolo a disposición de personal no autorizado
- No conecte el dispositivo móvil a redes de internet publicas
- Cambie la contraseña de acceso al menos una vez cada 90 días

- Preferiblemente no almacene información confidencial en el dispositivo móvil, si lo requiere ésta debe estar cifrada.
- No mantenga líquidos o inflamables cerca al dispositivo móvil
- Mantenga una copia de seguridad de la información contenida en los dispositivos móviles en los equipos o carpetas fijas de la Cooperativa (que tienen respaldo), el área de sistemas no se hace responsable de las copias de seguridad de los dispositivos móviles.

Está prohibido acceso y/o almacenamiento de información confidencial desde dispositivos móviles personales. Su uso sólo podrá ser autorizado por el Oficial de Seguridad de la información quien debe validar que dicho dispositivo móvil cuente con los requisitos mínimos de seguridad detallados en el lineamiento anterior.
El área de Informática debe hacer revisiones periódicas para asegurar que los dispositivos móviles cuentan con las versiones de software vigentes, de lo contrario debe aplicar los parches a los que haya lugar.

5.3 Política de Seguridad de la Información para el Trabajo Remoto

Objetivo: El objetivo de la política es definir las condiciones, directrices, acuerdos y restricciones que deben implementarse en las diferentes modalidades de Trabajo Remoto de la Cooperativa y el uso seguro de las herramientas tecnológicas suministradas para este fin, las cuales se encuentran alineadas con la legislación colombiana vigente.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, hagan uso de los sistemas de información y/o accedan a información de forma remota.

Lineamientos:
Se deben implementar medidas de seguridad para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares que se realiza el trabajo remoto.
El Teletrabajo hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual".
Para ello, se deben cumplir los siguientes lineamientos, teniendo en cuenta que el teletrabajo requiere unas condiciones básicas tecnológicas que dan soporte a los teletrabajadores en el desarrollo de sus funciones y que desprenden unas responsabilidades asociadas al manejo de la información en cuanto a su confidencialidad, integridad y disponibilidad.

Responsabilidades de la Dirección de Informática

La Dirección de Informática es responsable de definir las herramientas tecnológicas necesarias y suficientes para garantizar el adecuado ejercicio del teletrabajo, por lo que se deben tomar las medidas técnicas y de seguridad necesarias sobre dichos elementos si son requeridos. Así mismo, es la responsable por gestionar los riesgos de seguridad de la información que se identifiquen y proporcionar los controles que los mitigue, de igual manera, debe proveer el acceso a los diferentes sistemas de información que el Teletrabajador requiera para el desarrollo de sus actividades, es necesario que este acceso sea seguro por medio de VPN y escritorio remoto de ser necesario.

Responsabilidades del Teletrabajador

De acuerdo con los tres pilares de la seguridad de la información, confidencialidad, disponibilidad e integridad de la información, los teletrabajadores de la Cooperativa tienen las siguientes responsabilidades:

- Interiorizar y aplicar las diferentes políticas de seguridad de la información de la compañía.
- Informar si detecta comportamientos extraños en su equipo de trabajo y reportar los incidentes de seguridad que se llegaran a presentar.
- No compartir con otras personas el equipo asignado, así como las contraseñas para el acceso al mismo. Esta información deberá ser tratada como confidencial y no será compartida con nadie.
- Utilizar buenas prácticas de navegación por Internet.
- Se prohíbe el uso de redes WiFi públicas o aledañas al entorno del teletrabajador ya que implica riesgo a la información de la Cooperativa.
- Mantener la confidencialidad, disponibilidad e integridad de la información bajo su responsabilidad.
- Conservar y custodiar con la debida diligencia los equipos, herramientas informáticas y programas provistos por la compañía, éstos deben ser utilizados únicamente para llevar a cabo las actividades laborales encomendadas y evitar la utilización de éstos por personas diferentes a las autorizadas.
- Comunicar de inmediato sobre cualquier pérdida, robo, hurto u otro uso indebido de equipos, programas y/o documentos con información sensible para la compañía.
- Los colaboradores teletrabajadores son responsables de la información que resida en el computador asignado y deben hacer uso del almacenamiento en la nube que disponga la compañía.
- En la actividad del teletrabajo se debe acatar todas las medidas necesarias que protejan los derechos de autor y propiedad intelectual por lo que está prohibido tener software no avalado por la compañía en el equipo asignado.

5.4 Política de Gestión de Activos

Objetivo: El objetivo de la política es definir los lineamientos de seguridad para lograr la clasificación y gestión de los activos de información de COOPEBIS, con el fin de suministrar la protección adecuada de acuerdo con la legislación y estándares vigentes.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, hagan uso de algún activo de información en la Cooperativa.

Lineamientos:

Se deben establecer las responsabilidades respectos del manejo y la gestión de los activos de información de la organización.

Inventario de Activos

El Oficial de Seguridad de la Información debe gestionar para que cada área de la Cooperativa realice un inventario de activos de información, donde se identifiquen con sus respectivos propietarios y su ubicación.

Los responsables de cada área deberán mantener actualizado el inventario de sus activos de información ante cualquier modificación de la información allí registrada y será revisado de forma anual.

Se debe crear una metodología para la gestión de los activos de información la cual debe ser conocida y aplicada por los colaboradores de la compañía.

Propiedad de los Activos

Cada activo de información identificado debe tener su propietario con la responsabilidad delegada sobre la gestión del activo dentro de su ciclo de vida.

El propietario del activo debe asegurarse de que los activos están inventariados, asegurarse de que los activos están clasificados y protegidos apropiadamente, definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables y asegurarse del manejo apropiado del activo cuando es eliminado o destruido.

Uso Aceptable de los Activos

Los activos de información, aplicaciones, herramientas tecnológicas y equipos, asignados a los colaboradores y terceros de COOPEBIS, son para uso exclusivo del cumplimiento de las funciones y obligaciones designadas; razón por la cual, la información almacenada, procesada y generada a través de dichos activos, herramientas y dispositivos, se considera propiedad de la Cooperativa y el uso inadecuado de dichos recursos puede conllevar a sanciones disciplinarias y legales correspondientes.

Los colaboradores y usuarios de partes externas deberán utilizar únicamente los aplicativos y equipos de cómputo autorizados por la el área de Informática.
COOPEBIS podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado en caso de posible desacato a las leyes, decretos o reglamentación interna de la Cooperativa.

COOPEBIS se reserva el derecho de monitorear los accesos a sistemas de información y el uso de los buzones de correo institucionales de todos sus colaboradores y terceros con accesos otorgados, además podrá realizar copias de seguridad en cualquier momento, así como limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la Cooperativa, por solicitud expresa al área de Informática por parte del jefe inmediato, Gerencia General, consejo de administración el área de Talento Humano. Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados al área de Informática, con su correspondiente justificación para su respectiva viabilidad.

En caso de ser necesario se podrá acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de internet o de cualquier otra red o medio, en los equipos informáticos a su cargo.
El área de Informática efectuará la revisión de los programas y software utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerado como una violación a la política de Seguridad de la Información de la Cooperativa.

Los recursos informáticos de COOPEBIS no podrán ser utilizados para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

Los colaboradores de la Cooperativa no podrán efectuar ninguna de las siguientes labores sin previa autorización del Área de Informática:

- Instalar software en cualquier equipo de la Cooperativa.
- Descargar software de internet u otro servicio en línea en cualquier equipo de la Cooperativa.
- Modificar, revisar, transformar o adaptar cualquier software propiedad de la Cooperativa.
- Copiar o distribuir cualquier software propiedad de la Cooperativa.

Devolución de los Activos

En el momento de desvinculación o cambio de labores, los colaboradores y terceras partes deben realizar la entrega de su puesto de trabajo al jefe inmediato o a quien este delegue; así mismo, debe encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

Para el traslado de equipos de cómputo a otros colaboradores o baja de los inventarios por cualquier motivo, se deberá realizar un respaldo de la información que en él se encuentre. En caso de ser necesario, se debe realizar borrado seguro de la información, con el fin de propender que la información de la Cooperativa contenida en estos medios no se pueda recuperar, esta solicitud la debe de realizar el responsable del área correspondiente. La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es el área de Informática.

Mantenimiento de Equipos

El área de Informática debe asegurar que todos los equipos de cómputo activos en la Cooperativa se encuentren actualizados en el inventario de equipos de cómputo y la Hoja de vida del equipo.
Tanto los equipos de escritorio como los portátiles deben estar ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado.
Los mantenimientos a equipos se deben realizar dando cumplimiento a la programación previamente establecida.

5.5 Política de Clasificación de la Información

Objetivo: Establecer los lineamientos para implementar la clasificación de la información y los controles necesarios garantizar los niveles apropiados de protección de la información de acuerdo con la confidencialidad, integridad y disponibilidad.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, interactúen o hagan uso de algún sistema de información de la Cooperativa.

Lineamientos:

Se debe Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la compañía.

Clasificación de la Información

En COOPEBIS se definieron los siguientes niveles de clasificación de la información de acuerdo con su confidencialidad, integridad y disponibilidad:

CONFIDENCIALIDAD	
Clasificación	**Definición**
Pública	Información creada para ser publicada de forma abierta. La divulgación no autorizada al público de información pública no perjudicará la Cooperativa, proveedores o asociados.
Interna	Información a la que pueden acceder **todos los empleados o la gran mayoría de ellos**. No está destinada a ser publicada. La divulgación no autorizada al público de información interna no debe perjudicar la Cooperativa, ni a sus proveedores o asociados.
Restringida	Información para una **audiencia específica.** La divulgación no autorizada al público de información restringida puede causar un perjuicio de imagen o financiero significativo, puede resultar en consecuencias legales o puede dañar la reputación de la Cooperativa, de sus asociados o proveedores.
INTEGRIDAD	
Clasificación	**Definición**
Estándar	Es posible que **no se controle** la integridad del activo. La modificación o destrucción no autorizada de información o activos de información solo puede tener un impacto extremadamente limitado para la Cooperativa, a sus asociados o proveedores.
Controlada	Es posible que el activo no esté completo, siempre que **se identifique la alteración y se pueda restaurar la integridad.** La modificación o destrucción no autorizada de información o activos de información puede tener un impacto significativo en la Cooperativa, o en sus asociados o proveedores.
Intacta	El activo debe **estar intacto** (no modificable). El activo debe contar con los mecanismos adecuados que imposibiliten la alteración de los

	datos. La modificación o destrucción no autorizada de información o activos de información puede tener un impacto muy desfavorable para la Cooperativa o a sus asociados o proveedores.
DISPONIBILIDAD	
Clasificación	**Definición**
Estándar	Falta de disponibilidad o pérdida temporal aceptable. La pérdida de activos o la interrupción del acceso a un activo solo puede tener un impacto limitado en la Cooperativa o en sus asociados y proveedores.
Alta	Falta de disponibilidad o pérdida temporal aceptable. La pérdida de activos o la interrupción del acceso a un activo pueden tener un impacto significativo en la Cooperativa o en sus asociados y proveedores.
Critica	Falta de disponibilidad o pérdida temporal aceptable. La pérdida de activos o la interrupción del acceso a un activo pueden tener un impacto muy desfavorable en la Cooperativa o para sus asociados y proveedores.

La Clasificación de los activos de información es un ejercicio que debe ser realizado por cada líder de proceso apoyado en sus colaboradores o a quien este delegue.
Los propietarios y custodios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación. La información física y digital de la compañía deberá tener un periodo de almacenamiento que puede ser dado por requerimientos legales, misionales o contractuales.

Etiquetado de la Información

El etiquetado de la información se mantendrá en el inventario y clasificación de la información, cada activo tendrá su respectiva valoración en confidencialidad, integridad y disponibilidad y se evaluará el impacto que tiene para la compañía.

5.6 Política de Gestión de medios removibles

Objetivo: Establecer los lineamientos para implementar los controles necesarios sobre el uso de medios removibles en la Cooperativa, para mitigar riesgos, como pérdida, daño, fuga o modificación de información.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, interactúen o hagan uso de algún sistema de información de la Cooperativa.

Lineamientos:

Gestión de Medios Removibles

El uso de medios removibles con información de la Cooperativa conlleva a riesgos, como pérdida, daño, fuga o modificación, que compromete no solamente la información sino también la infraestructura tecnológica, por lo tanto, el colaborador que los use será quien asuma la responsabilidad por la seguridad de la información.

En caso de que se usen medios removibles para el manejo de la información se deben seguir los siguientes lineamientos:

Todo medio removible deberá ser escaneado mediante antivirus cada vez que se conecte a un equipo de la Cooperativa.

Es responsabilidad de cada colaborador tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío de este.

En la medida de lo posible, se deberán poner claves a los archivos y/o usar algún método de cifrado de la información.

Se prohíbe el uso de medios removibles con información de la Cooperativa en lugares de acceso al público.

Disposición de los Medios Removibles

Los medios que se regresen para asignarse a otro colaborador, se les deberá realizar un borrado de información. Es requisito realizar el respaldo o copia de la información contenida en el medio, previa ejecución del borrado de información.

En caso de que los medios sean donados, dados de baja o sean devueltos al proveedor, en la medida de lo posible se deberán emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes, con el fin de controlar que la información la compañía contenida en estos medios no se pueda recuperar.

Transferencia de Medios Físicos

Cuando se requiera transferir un medio físico que contenga información de COOPEBIS, se deben usar transportes o servicios de mensajería confiables.

El dueño o propietario de la información a transferir debe autorizar dicho traslado.

Para la transferencia de medios de almacenamiento físicos, es necesario que este medio se proteja contra acceso no autorizado como claves y si es necesario el cifrado de la información.

5.7 Política para el control de acceso lógico

Objetivo: El Objetivo de la política es establecer el control de acceso lógico y las directrices de seguridad que deben implementarse en la gestión de accesos de los usuarios a los diferentes servicios tecnológicos y el control de acceso a las redes, además de definir las responsabilidades de seguridad que los usuarios deben aplicar para minimizar riegos de accesos no autorizados.

Alcance: La presente política aplica para todas las partes interesadas o que, por su rol, brinden o requieran acceso lógico a la información y/o a las instalaciones de procesamiento de información de la Cooperativa.

Lineamientos:

Requisitos para el control de acceso

El acceso a la información y los sistemas asociados, deben estar debidamente controlados, asegurando que sólo el personal autorizado pueda tener acceso a la información, ya sean colaboradores, contratistas, clientes o terceros con previa autorización por parte del propietario de la información, teniendo en cuenta la clasificación que se le haya otorgado a dicha información.

Para ello, es necesario cumplir con los siguientes controles:

- Creación de usuarios
- Modificación / actualización de usuarios
- Eliminación y baja de usuarios
- Gestión de usuarios para terceros y contratistas.

Identificación y Autenticación

Todas las partes interesadas que, con ocasión a sus tareas u obligaciones con la Cooperativa, tengan acceso a los sistemas de información, deben utilizar un nombre de usuario de dominio c*oopebis.local*, asignándole para ello una contraseña que cumpla con las políticas de seguridad adoptadas por la Cooperativa, la cual deberá ser personal e intransferible.

El acceso a los sistemas de información y servicios tecnológicos de la Cooperativa, a través del uso de usuario de dominio *coopebis.coop*, debe estar restringido y delimitado a las tareas, funciones, responsabilidades u obligaciones que ejecuten los empleados, contratistas, proveedores o terceras partes en la Cooperativa.

Sistema de Gestión de Contraseñas

Los empleados, contratistas, proveedores y terceras partes deben crear contraseñas seguras, es decir, que cumplan los siguientes parámetros:

- La longitud debe ser al menos de 8 caracteres.
- Contener caracteres tanto en mayúsculas como en minúsculas.
- Puede tener dígitos y caracteres especiales como _, -, /, *, $, ¡=, +, etc.
- Cambiarla cada 90 días.
- No debe ser basada en información personal, nombres de familia, etc.
- Algunos ejemplos de contraseñas NO seguras como, por ejemplo: Nombres de familiares, mascotas, amigos, compañeros de trabajo, personajes, etc.
- Tipo de numeración como: Cumpleaños, aniversarios, información personal, teléfonos, códigos postales, etc.
- Patrones como: 123456?, qwerty, 1q2w3e4r2017*, etc.
- Composiciones simples como: minombre1, minombre2, etc.
- Tener en cuenta NO utilizar 12 veces las contraseñas usadas.
- Después de 3 intentos no exitosos de ingreso de la contraseña traerá consigo el bloqueo del usuario de manera inmediata para lo cual se debe solicitar el desbloqueo a quien ejecute el rol de Administrador de control de acceso lógico.

En cuanto a la custodia:

Las contraseñas no deben ser almacenadas en formato legible, papeles, agendas de trabajo, computadores sin sistemas de control de acceso o cualquier otro lugar donde las personas no autorizadas puedan encontrarlas.

Si algún empleado, proveedor o terceras partes, sospechan de la pérdida de confidencialidad de alguna de sus claves, deben notificar de manera escrita el evento o incidente de seguridad de la información (según sea el caso) a la mesa de ayuda, a fin de tomar las medidas pertinentes de cuidado de la información y supervisar la generación de nuevas credenciales.

Registro y Cancelación del Registro de Usuarios

Con el objetivo de impedir el acceso no autorizado a la información, en COOPEBIS, se debe implementar un procedimiento el control de la asignación de derechos de acceso a los sistemas, datos y servicios de información de los que se disponen en la Cooperativa, siguiendo estos lineamientos:

Utilizar códigos de usuario únicos, de manera que se puedan identificar por sus acciones, evitando la existencia de múltiples perfiles de acceso para una misma persona, a no ser que el cliente en su proyecto lo defina de forma contraria, para lo cual debe estar soportado y aprobado. Para colaboradores de COOPEBIS, la solicitud para la creación de un nuevo usuario, la realiza el área de Talento Humano, con la creación de una solicitud a través de la mesa de ayuda, donde se le asignará al nuevo colaborador los

privilegios y permisos establecidos por el jefe inmediato, de igual forma se le restringen los accesos a la información que no le compete.

Para terceros y clientes, la solicitud de usuarios la puede realizar el jefe de cada área a través la mesa de ayuda y se manejará de acuerdo con lo estipulado anteriormente. Se debe verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario. Cuando se presenten retiros de personal, el área de Informática verificará los permisos y accesos de este colaborador con el fin de proceder a su cancelación. De igual forma si el colaborador es trasladado de área, se debe realizar la modificación / retiro de los accesos a la información de éste; de acuerdo con lo establecido por el nuevo jefe de que tenga el colaborador.

Suministro de Acceso de Usuarios

Es necesario que cuando se permita el acceso a los usuarios a los sistemas, datos y servicios provistos por COOPEBIS, se cumplan con los siguientes lineamientos:
El acceso a la información de COOPEBIS es otorgado sólo a usuarios autorizados, teniendo en cuenta lo requerido para la realización de sus labores relacionadas con su responsabilidad o tipo de servicio con los privilegios asignados. Se deben definir los controles de seguridad a los tipos de usuarios dependiendo el acceso a la información que este requiera:

Usuario Proveedor o Tercero: son aquellos usuarios externos a COOPEBIS que prestan un servicio bajo un contrato y requieren acceso a la plataforma tecnológica de la Cooperativa.

Usuario Administrador: son los usuarios colaboradores, contratistas o terceros que por sus funciones u obligaciones requieren permisos de administración para el desarrollo de sus actividades en la plataforma de la Cooperativa.

Usuario Estándar: son los usuarios contratistas, pasantes y colaboradores de la Cooperativa que no se encuentran catalogados en ninguno de los anteriores grupos.

No se deberá configurar el acceso a usuarios que no hayan formalizado el proceso de ingreso a la Cooperativa. Todo usuario que quiera acceder a servicios o información de la plataforma tecnológica de la Cooperativa deberá autenticarse. Todos los colaboradores y terceras partes deberán cumplir las condiciones de acceso y mantener de forma confidencial las contraseñas con la finalidad de preservar el no repudio.

Se debe verificar que el nivel de acceso otorgado es apropiado a las políticas de acceso descritas anteriormente. Se debe revisar periódicamente los derechos de usuario otorgados para detectar posibles cambios o retiros del personal.

Gestión de Derechos de Acceso Privilegiado

El área de Informática generará los controles para restringir y controlar la asignación y uso de derechos de acceso privilegiado teniendo en cuenta lo siguiente:

- Se deberá otorgar los privilegios para la administración de los servicios de red y sistemas de información, únicamente a aquellos colaboradores que cumplan dichas funciones.
- Se debe validar que solo cuenten con los permisos de acceso los usuarios autorizados.
- Se debe validar las competencias del personal que usará los usuarios con acceso privilegiado.
- En caso de ser necesario usar identificaciones de usuario de administración genérica, se debe mantener la confidencialidad de la información secreta para la autenticación cuando se comparta, por ejemplo, cambiar las contraseñas con frecuencia, y tan pronto como sea posible cuando un usuario privilegiado ha dejado el trabajo o cambia de rol de trabajo, comunicarlas entre los usuarios privilegiados con los mecanismos apropiados.

Gestión de Información de Autenticación Secreta de Usuarios

La contraseña para la autenticación se deberá suministrar a los usuarios de manera segura, y el sistema deberá solicitar el cambio inmediato de la misma al ingresar.

Se deberá verificar la identidad de un usuario antes de reemplazar la información secreta para la autenticación o proporcionar una nueva o temporal.

La información secreta para la autenticación por defecto del fabricante, se deberá modificar después de la instalación de los dispositivos o del software.

Revisión de los Derechos de Acceso de Usuarios

El área de Informática realizará revisiones de los derechos de acceso de los usuarios en cada uno de los sistemas de información y plataformas de la Cooperativa para determinar su pertinencia.

Se debe verificar los accesos sobre cualquier cambio, promoción, cambio a un cargo o terminación del empleo de un usuario.

También se deben revisar los derechos de acceso de los usuarios administradores de las plataformas y sistemas de información de la Cooperativa.

Retiro o Ajuste de los Derechos de Acceso

El retiro de los privilegios de un usuario se deberá hacer inmediatamente una vez se realice la solicitud de desactivación.

Es responsabilidad del área de Talento Humano y de los responsables de cada área, dar a conocer al área de Informática el retiro, suspensión o cualquier novedad administrativa que se presente con los usuarios de la Cooperativa.

Uso de Información de Autenticación Secreta

Cada usuario es responsable del uso de las contraseñas de acceso que se le asignen para la utilización de los equipos, servicios o acceso a la plataforma de la Cooperativa y deben mantener su confidencialidad. El cambio de contraseña solo podrá ser solicitada por el titular de la cuenta o jefe inmediato. Los usuarios deben evitar llevar un registro de las contraseñas asignadas.

Restricción de Acceso a la Información

El área de Informática deberá implementar controles de acceso en las aplicaciones dependiendo el rol desempeñado por el usuario.

Se deben proveer controles de acceso físico a las áreas seguras.

El propietario de la aplicación y de la información, debe identificar y documentar explícitamente la sensibilidad o confidencialidad de la información contenida en los sistemas y aplicaciones de la Cooperativa.

Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la clasificación de la información.

No está permitido para ningún empleado, contratista, proveedor o terceras partes, acceder a la información y a las aplicaciones de un sistema de información para el cual no haya sido autorizado.

Las sesiones inactivas deberán cerrarse después de un período de inactividad definido.

Procedimiento de Ingreso Seguro

El área de Informática implementará controles para el ingreso seguro a las aplicaciones minimizando la oportunidad de acceso no autorizado, teniendo en cuenta los siguientes lineamientos:

- No se deben visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente.
- No deben existir mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado y si el ingreso es erróneo, no se debe indicar qué parte de los datos es correcta o incorrecta.
- No se deben transmitir contraseñas en texto claro.
- Se deben terminar sesiones inactivas después de un período de inactividad definido.

Uso de Programas Utilitarios Privilegiados

El uso de programas utilitarios privilegiados está prohibido en la Cooperativa, salvo que él tenga una aprobación por parte del director de Informática y se deben contar con los siguientes lineamientos:
Se deberán establecer los controles para que los usuarios finales no tengan instalados en sus equipos de cómputo utilitarios que permitan escalar privilegios o evadir controles de seguridad informáticos.

Acceso a redes y a servicios en red

Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para aquellos colaboradores, contratistas, clientes o terceros que hayan sido autorizados. Se debe controlar el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de estos.

El área de Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo con el pedido formal del jefe o persona encargada del área correspondiente que lo solicite para el personal de su incumbencia y para el cumplimiento de labores asignadas. El área de Informática suministrará a los usuarios las credenciales respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, de esta forma las credenciales de acceso son de uso personal e intransferible.

Es responsabilidad de los colaboradores o terceras partes de COOPEBIS el manejo que se les dé a las credenciales de acceso asignadas. La conexión remota a la red interna de COOPEBIS deberá establecerse a través de una conexión VPN suministrada por el área de Informática, la cual deberá ser aprobada por el jefe o persona encargada del área correspondiente que lo solicite.

El área de Informática deberá realizar revisiones e inactivaciones de las conexiones VPN periódicamente para verificar que solo estén los usuarios que se encuentren activos en la compañía. El área de Informática deberá realizar monitoreo sobre las redes con el fin de verificar disponibilidad de los servicios y los controles de acceso para los usuarios de COOPEBIS y los provistos a terceras partes, con el fin de revisar que dichos usuarios tengan los permisos únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

Control de acceso a códigos fuente de programas

El director de Informática debe asignar el rol del Administrador de programas fuentes, quien tendrá la responsabilidad de custodiar dichos programas y por virtud de su función no deberá pertenecer al equipo de desarrollo. Quien ejecute el rol de Administrador de programas fuentes debe llevar un registro actualizado de todos los programas fuentes en uso, indicando entre otros, el nombre del programa, programador, analista responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).

Quien ejecute el rol de Administrador de programas fuentes debe restringir el acceso a los códigos fuente de los programas, asegurándose de que solamente los ingenieros desarrolladores tengan acceso. Quien ejecute el rol de Administrador de programas fuentes debe mantener los códigos fuente de los programas en el servidor o repositorio de fuentes. Quien ejecute el rol de Administrador de programas fuentes, debe asegurarse de que el código y las bibliotecas fuentes del programa sean manejadas con los procedimientos establecidos.

La actualización de las bibliotecas de fuentes del programa, así como la emisión de las fuentes para los programadores sólo se deben realizar después de haber recibido la autorización del Equipo de Desarrollo. Quien ejecute el rol de administrador de programas fuentes debe mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa. El mantenimiento y copiado de las bibliotecas fuentes del programa está sujeto a procedimientos estrictos de control de cambios.

Quien ejecute el rol de Administrador de programas fuentes debe asegurarse de que los programas fuentes cuenten con una copia de respaldo actualizada. Quien ejecute el rol de Administrador del control de acceso lógico debe asegurar que los sistemas de información críticos de la Cooperativa cuenten con certificado digital para que el cifrado de información secreta de autenticación pueda ser transportada por medio de la red de forma segura. El acceso al código fuente del programa es limitado, solamente los ingenieros desarrolladores y de soporte serán autorizados por el área de Informática y de acuerdo con sus funciones.

Los repositorios fuentes de los sistemas de información no deberán estar contenidos en el ambiente de producción, sino en la herramienta para el control de versiones definida por el área de Informática. La gestión de los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con lo definido por el área de Desarrollo.

La actualización de las librerías de fuentes de programas y elementos asociados sólo se debe hacer una vez que se haya recibido autorización apropiada de acuerdo a la política de control de cambios.

5.8 Política de protección contra código malicioso

Objetivo: Establecer los lineamientos para implementar en todos los activos de información de la Cooperativa, controles para la detección y remediación de códigos maliciosos.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, interactúen o hagan uso de algún sistema de información de la Cooperativa.

Lineamientos:

Verificar la presencia de códigos maliciosos en archivos de medios de almacenamiento masivo extraíbles o en archivos recibidos a través de la red. Realizar tareas de escaneo en busca de códigos maliciosos en todas las unidades de almacenamiento de la estación de trabajo. Ningún colaborador podrá ejercer actividades de administración sobre su equipo. Los únicos autorizados para desarrollar esta función son los colaboradores autorizados por el área de Informática.

Se prohíbe estrictamente el uso de software no autorizado, todo software instalado debe contar con licencia. El área de Informática realizará sensibilización a los colaboradores sobre la protección contra software malicioso y buenas prácticas de seguridad informática, está prohibido la descarga de software no licenciado en cualquier dispositivo de la Cooperativa, adicionalmente se prohíbe la instalación de software propiedad de la Cooperativa en equipos que no pertenezcan a la organización.

Los colaboradores que sospechen o detecten alguna infección por software malicioso debe notificar al área de Informática, para que, a través de ella, se tome las medidas de control correspondientes. El área de Informática debe incluir en la infraestructura tecnológica que permita identificar y proteger a la organización de ataques externos y que afecten las plataformas tecnológicas de la Cooperativa. El área de Informática debe monitorear los intentos de ataque tanto internos como externos para tomar acciones que mitiguen este riesgo.

El área de Informática debe asegurar la instalación y configuración de un antivirus que identifique y proteja los equipos tecnológicos de la Cooperativa. Así mismo, debe actualizar periódicamente sus firmas para garantizar que la protección sea dinámica y

encaminada a los nuevos vectores de ataque. Cuando se identifique un programa maligno en los equipos de la Cooperativa, se debe seguir el reportar y tratar como un incidente de seguridad de la información.

El área de Informática debe ejecutar, al menos una vez al año, una prueba que identifique vulnerabilidades en las plataformas tecnológicas (Análisis de Vulnerabilidades, Ethical Hacking, entre otros), con el fin de mejorar los niveles de seguridad y proteger los activos de ataques externos e internos, con la interventoría de un proveedor externo. Está prohibida la descarga de cualquier archivo que provenga de correos sospechosos o de destinatarios desconocidos, su descarga sólo podrá ejecutarse con la validación y autorización del líder de seguridad de la información. Cualquier equipo que se conecte a la red y que no sea propiedad de la Cooperativa debe contar con los requisitos mínimos de seguridad establecidos en la Política de uso de dispositivos móviles previamente expuesta.

5.9 Política sobre el uso de controles criptográficos

Objetivo: Asegurar la implementación y el uso apropiado de controles para cifrado de la información en donde el nivel de criticidad de ésta lo requiera. Esta política define los lineamientos de seguridad para el uso de controles de cifrado de información con el fin de proteger su confidencialidad, integridad y disponibilidad.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, hagan uso de controles criptográficos.

Lineamientos:
En COOPEBIS se utilizarán sistemas y técnicas criptográficas para la protección de la información y datos almacenados que así lo requieran (solicitudes del propietario de la información o solicitudes regulatorias), además de implementar protocolos de comunicación seguros como SSL en las últimas versiones para las comunicaciones con los asociados y terceros. Se deben identificar los sistemas y aplicaciones en los que se considere necesario hacer uso de controles criptográficos para proteger la información. El uso de controles criptográficos quedará determinado por el análisis de riesgos del sistema, así como el nivel o fortaleza de los mecanismos de cifrado a utilizar (algoritmos, longitudes de clave mínimas, etc.)

Los aspectos importantes que se deben tener en cuenta para la definición de los criterios criptográficos son:

- Las herramientas y mecanismos de cifrado estandarizados en la Cooperativa.

- La sensibilidad de la información y su nivel de clasificación, así como los sistemas y líneas de comunicaciones por los que se almacena, procesa o transmite la información.
- Requisitos legales
- Uso de firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información sensible o crítica almacenada o transmitida.
- no-repudio: uso de técnicas criptográficas para suministrar evidencia de que un evento o acción ocurre o no ocurre.
- autenticación: uso de técnicas criptográficas para autenticar usuarios y otras entidades del sistema que solicitan acceso a usuarios, entidades o recursos del sistema, o tener transacciones con ellos.

Gestión de Llaves

El área de Informática debe realizar la gestión de llaves criptográficas durante todo su ciclo de vida, incluida la generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción de las llaves.
Los algoritmos criptográficos, la longitud de las llaves y las prácticas de uso se deberán seleccionar de acuerdo con las mejores prácticas.

5.10 Política para Gestión de Cambios

Objetivo: Asegurar la implementación y el uso apropiado de controles que garanticen la aplicación de cambios en los sistemas de información que eviten la interrupción de los servicios y la afectación de la información respecto de la confidencialidad, integridad y disponibilidad.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, hagan uso de controles criptográficos.

Lineamientos:

El área de Informática debe establecer un procedimiento para la gestión de cambios de tecnologías de la información, para asegurar una adecuada gestión de cambios estándar y de emergencia con respecto a infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficacia, seguridad, calidad y permitan determinar los responsables y actividades en la gestión de cambios. Se controlará el ciclo de vida de todos los cambios y se analizará la viabilidad de los cambios beneficiosos con un mínimo de interrupciones en la prestación de servicios de TI.

La gestión de cambios deberá minimizar el impacto de las incidencias relacionadas por los cambios sobre la calidad del servicio y, por consiguiente, mejorar el funcionamiento diario de la compañía y la relación con sus clientes. Los cambios de tecnologías de la información deben ser comunicados previamente al Administrador de Seguridad de la Información para evaluar su impacto. Se debe comunicar a todas las partes interesadas sobre el cambio a realizar y el resultado de éste después de ejecutado.

5.11 Política para la Gestión de Capacidad

Objetivo: Asegurar la implementación y el uso apropiado de controles que garanticen la aplicación de la gestión de capacidad sobre los elementos que componen los sistemas de información, para evitar la interrupción de los servicios y la afectación de la información respecto de la confidencialidad, integridad y disponibilidad.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, hagan uso de controles criptográficos.

Lineamientos:
El área de Informática debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido de la plataforma tecnológica de la Cooperativa. Deben de identificarse los requisitos de capacidad sobre los nuevos desarrollos y/o soluciones con el fin de evaluar y aplicar los ajustes necesarios en la plataforma tecnológica para mejorar la disponibilidad y eficiencia de los sistemas.

El área de Informática debe hacer monitoreo que permita detectar problemas oportunamente frente a la capacidad de la plataforma tecnológica y tomar medidas necesarias para la continuidad de la prestación de los servicios.

5.12 Política de escritorio y pantalla limpia

Objetivo: Establecer los lineamientos para prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la Cooperativa.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, tengan acceso a la información de la Cooperativa, en medio digital o físico.

Lineamientos:

Escritorio Limpio

No se deben dejar documentos clasificados como CONFIDENCIAL al alcance de personal no autorizado, en caso de tener información CONFIDENCIAL en físico ésta debe ser guardada bajo llave en los archivadores respectivos.

Ningún dispositivo móvil o medio en tránsito que almacene información CONFIDENCIAL debe dejarse al alcance de personal no autorizado.
No se debe consumir líquidos cerca de dispositivos que procesen o almacenen información.

Al momento de utilizar un computador portátil o dejarlo desatendido, éste se debe asegurar con una guaya de seguridad y retirar la llave o salvaguardar la clave de esta.

Pantalla Limpia

El escritorio del equipo de cómputo debe permanecer libre de documentos clasificados como CONFIDENCIALES.

En el momento de dejar desatendido su estación de trabajo, el usuario debe bloquear su equipo de cómputo.

El área de Informática debe asegurar el bloqueo automático después de (5) minutos de inactividad. Adicionalmente, el usuario se hace responsable por mantener debidamente bloqueado el acceso a su computador, cuando su estación este desatendida.

5.13 Política de respaldo de la información

Objetivo: Establecer los lineamientos para generar las copias de respaldo de los activos de información con el fin de preservar su disponibilidad.

Alcance: La presente política aplica para todos los administradores de los sistemas de información, servidores, bases de datos y los usuarios de copias de respaldo.

Lineamientos:
El área de Informática debe asegurar que se realicen las copias de respaldo de la información de la Cooperativa almacenada en los sistemas de Información, servidores y bases de datos. Es responsabilidad de quien el jefe asigne realizar las copias de seguridad de información, realizando seguimientos regulares a su ejecución.

Quien el jefe asigne debe validar el resultado de la ejecución de las copias de seguridad y registrar las novedades en la bitácora establecida para ello. Cuando se requiera un soporte o mantenimiento correctivo por parte del fabricante, que pueda afectar los procesos o los sistemas de procesamiento de la información, quien ejecute el rol de operador debe solicitar la aprobación del jefe de área.

Es responsabilidad del coordinador o a quien el jefe asigne realizar por lo menos pruebas de restauración una vez al año. El área de Informática debe asegurar la custodia de las copias de seguridad en un sitio externo a las instalaciones de la Cooperativa.

5.14 Política de Registro de eventos

Objetivo: Establecer los lineamientos y controles necesarios para garantizar la definición y la gestión sobre los registros de trazabilidad de los sistemas de información de COOPEBIS con el fin de preservar la confidencialidad, integridad y disponibilidad.

Alcance: La presente política aplica para todos los administradores de los sistemas de información, servidores, bases de datos etc.

Lineamientos:

El área de Informática deberá generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren, en lo posible, los registros de eventos deberían guardar la siguiente información como mínimo: identificación de usuarios, actividades del sistema, fechas y horas. El área de Informática deberá salvaguardar los registros de auditoría que se generen de cada sistema teniendo en cuenta las relaciones contractuales.

Protección de la Información de Registro

El área de Informática deberá generar controles contra acceso no autorizado para la protección de la información generada del registro de eventos.

Registros del Administrador y del Operador

El área de Informática deberá asegurar que los usuarios con cuentas privilegiadas no puedan modificar los registros de eventos que se generen.

5.15 Política de sincronización de Relojes

Objetivo: Establecer los lineamientos para contar con controles que protejan la interceptación, copiado, modificación de la información a través de la manipulación de los relojes de los dispositivos de TI.

Alcance: La presente política aplica para todos los administradores de los sistemas de información, servidores, bases de datos etc.

Lineamientos:
El área de Informática deberá definir un único procedimiento técnico que permita la sincronización de relojes de los servidores con una única fuente de referencia de tiempo, por ejemplo (http://horalegal.inm.gov.co/), con el fin de garantizar la exactitud de los registros de auditoría y evitar posibles fraudes relacionados con la manipulación de los relojes.

5.16 Política Instalación de software en sistemas operativos

Objetivo: Establecer los lineamientos para implementar controles que protejan la Cooperativa de la instalación de software, ilegal o no autorizado que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, tengan acceso a la información de la Cooperativa, en medio digital o físico.
Lineamientos:
La actualización del software operacional, aplicaciones y librerías de programas solo la debe llevar a cabo el personal que designe El área de Informática.

Las aplicaciones y el software del sistema operativo solo se deben implementar después de pruebas exitosas y siguiendo el procedimiento de control de cambios. Se debe de conservar las versiones anteriores del software de aplicación como una medida de contingencia.

Restricciones Sobre la Instalación de Software

Sólo está permitido el uso de software licenciado por la Cooperativa y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por el área de Informática. El área de Informática es la única área autorizada para la administración del software, el cual no deberá ser copiado, suministrado a terceros o utilizado para fines personales por parte de los colaboradores.

El área de Informática designará y autorizará al personal para instalar, configurar y dar soporte a los equipos de cómputo de la Cooperativa. El área de Informática podrá en cualquier momento realizar una inspección del software instalado en los equipos de cómputo de los colaboradores.

5.17 Política de Gestión de vulnerabilidades técnicas

Objetivo: Establecer los lineamientos para la implementación de los controles que aseguren la ejecución de las pruebas de vulnerabilidad, tanto para las aplicaciones como para la infraestructura de TI y se establezca el plan con las acciones de remediación requeridas.

Alcance: La presente política aplica para todos los administradores de los sistemas de información, servidores, bases de datos etc.

Lineamientos:

El área de Informática debe establecer un procedimiento para que periódicamente se realicen las pruebas de vulnerabilidad a los sistemas, con el fin de verificar y analizar los riesgos de seguridad, encontrando vulnerabilidades y realizando gestión sobre cada una para definir el plan de acción especifico necesario para la remediación.

Todo análisis de vulnerabilidad o prueba de penetración debe contar con la autorización del director del área de Informática y estas deberán ser previamente informadas a las partes interesadas con el fin de evaluar el riesgo de la ejecución de ellas, su alcance y el cumplimiento de la normatividad vigente.

5.18 Política para la Gestión de la seguridad de las redes

Objetivo: El Objetivo de la política es establecer el control de acceso lógico y las directrices de seguridad que deben implementarse en la gestión de las redes y los servicios de red y que se deben aplicar para minimizar riegos relacionado.

Alcance: La presente política aplica para todos los administradores de los sistemas de información, servidores, bases de datos etc.

Lineamientos:

Controles de Redes

El área de Informática deberá proporcionar una plataforma Tecnológica que soporte los sistemas de información, esta deberá estar separada en segmentos de red para la conexión de usuarios y visitantes. Garantizar que los puertos físicos y lógicos de diagnósticos y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

Realizar revisiones y monitoreo regularmente en la gestión de los servicios de manera segura y que se encuentran en los acuerdos de servicios de red establecidos con los

proveedores. El acceso físico a los dispositivos de red debe estar restringido al personal autorizado a su gestión.

Seguridad de los Servicios de Red

El área de Informática debe identificar mecanismos de seguridad para las redes. El área de Informática debe verificar la capacidad del proveedor de servicios de red para gestionar en forma segura los servicios acordados y acordar los niveles de servicio. Se habilitarán dispositivos de seguridad que permitan el filtrado del tráfico (cortafuegos) entre las redes internas de COOPEBIS y las redes externas, tales como proveedores, clientes o con otras Empresas.

El área de Informática mantendrá la información actualizada de la topología de comunicaciones de COOPEBIS, con el objetivo de asegurar la información actualizada para las revisiones de seguridad sobre los Sistemas de Información.

Separación de las Redes

Se deben separar las redes de colaboradores y usuarios internos con las de invitados. Los dispositivos de interconexión de redes deberán disponer de una configuración adecuada para mantener el nivel de seguridad de la organización incluyendo, entre otros, el acceso restringido a los administradores, la comunicación de administración con protocolos seguros o la inhabilitación de claves por defecto. Se debe establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

5.19 Política para la transferencia de información

Objetivo: Establecer los lineamientos para contar con controles que protejan la información transferida con respecto a la interceptación, copiado, modificación, y enrutado, así como mantener la seguridad de la información transferida al interior de la Cooperativa y/o con cualquier organización externa.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, transfieran información al interior de la Cooperativa y/o con cualquier organización externa.

Lineamientos:

Acuerdos de confidencialidad o de no divulgación

Confidencialidad: Todos los empleados y terceras partes con quienes se firme un acuerdo de confidencialidad están obligados a dar cumplimiento a la Política de Confidencialidad establecida por la Cooperativa. El intercambio de información al interior de la Cooperativa debe hacerse por medio de los canales de comunicación formalmente establecidos para ello. Está prohibido el envío de información corporativa a canales personales como correo electrónico, drive, WhatsApp web, entre otros.

Acuerdos sobre transferencia de información

Cuando se trate de un intercambio o transferencia de información confidencial con un tercero, el propietario del activo de información debe realizar acuerdos para el intercambio seguro de la información mediante acuerdos y/o actas en donde ambas partes deben estipular los medios por los cuales se realizará la transferencia de la información.

El propietario del activo de información debe establecer un acuerdo de confidencialidad con la parte externa solicitante o interesada, esto con el fin de, prevenir que se vulnere la confidencialidad de la información y que pueda ser usada para fines fuera del acuerdo con las partes firmantes. Los acuerdos de confidencialidad sólo aplican cuando la información a intercambiar sea clasificada como Confidencial.

5.20 Política de seguridad para las relaciones con proveedores

Objetivo: Establecer los lineamientos para asegurar la protección de los activos de información de la Cooperativa que sean accesibles a los proveedores y contratistas.

Alcance: La presente política aplica para todos los proveedores o terceras partes que requieran acceso a los activos de información de la Cooperativa y para los empleados o contratistas que establezcan dichos contratos.

Lineamientos:

Cadena de suministro de tecnología de información y comunicación

Antes de la selección del proveedor, el área solicitante de la contratación debe identificar el nivel de clasificación de la información y/o instalaciones o componentes de procesamiento de información a los que tendrá acceso el proveedor. (Ej.: Información confidencial, bases de datos, servidores, etc.)

El área solicitante debe identificar los riesgos de seguridad de la información a los que se expone la Cooperativa con la contratación del servicio requerido, los cuales deben estar incluidos en la estimación y cobertura de los riesgos del proceso de contratación, teniendo en cuenta los siguientes aspectos: clasificación, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.

El director de Informática debe identificar sí el objeto de la propuesta u oferta evaluada, requiere del acceso de los proveedores a la información confidencial de la Cooperativa, sistemas de información y/o áreas seguras de la Cooperativa.

Tratamiento de la seguridad dentro de los acuerdos con proveedores

El Oficial de seguridad de la información a fin de determinar los requisitos mínimos de seguridad y los controles necesarios por parte del proveedor para ejecutar dicho contrato. En cualquiera de los casos, se debe dar a conocer a los proveedores interesados o terceras partes, las políticas de seguridad de la información. En el contenido del contrato que se celebre entre la Cooperativa y aquellos proveedores o terceras partes que tendrán acceso a la información confidencial, se deben incluir las siguientes cláusulas contractuales: confidencialidad, protección de datos.

Seguimiento y revisión a los servicios proveedores

Durante la etapa contractual y post contractual, es función del interventor y/o interventoría asignada, monitorear, hacer seguimiento y asegurarse de que los controles pactados para garantizar la seguridad de la información a que se ha tenido acceso por parte de los proveedores o terceras partes cumplan con los tres pilares de la información, esto es: confidencialidad, integridad y disponibilidad frente a los riesgos previamente identificados.

Antes de iniciar la ejecución del contrato, el interventor debe socializar a los proveedores y terceras partes, según sea el caso, el canal para el reporte de los incidentes de seguridad de la información. Como parte de la supervisión a la ejecución del contrato, se debe contemplar los procesos de auditoría a proveedores o terceras partes, cuyo objetivo sea validar el cumplimiento de los requisitos de seguridad de la información estipulados desde la etapa precontractual, dichos resultados deben quedar consignados también en los informes presentados por el interventor del contrato.

Para los servicios de tecnología y de comunicaciones contratados, se debe exigir que los proveedores apliquen y cumplan los requisitos y prácticas de seguridad de la información, adoptados por la Cooperativa, a lo largo de la cadena de suministro. Para

toda gestión del proveedor que represente una modificación, mantenimiento, revisión al servicio de tecnología de la información, comunicaciones o equipos de suministros, se debe autorizar por el jefe del área.

Para la contratación de servicios o componentes de la infraestructura de TI y/o áreas seguras, se debe exigir a los proveedores la presentación de los planes de contingencia que aseguren la disponibilidad de la información suministrada y procesada entre las partes.

Gestión de cambios en los servicios de los proveedores

Se deben gestionar todos los cambios aplicados a los servicios prestados por los proveedores, incluidos cambios en la documentación como políticas y procedimientos, así como los cambios relacionados con procesos de negocio y sistemas, dependiendo de los cambios se debe evaluar si es necesaria la actualización del mapa de riesgos desde la nueva perspectiva.

5.21 Política de Gestión de incidentes de Seguridad

Objetivo: Tiene como objetivo definir los lineamientos para el cumplimiento de los requisitos y buenas prácticas para la gestión de incidentes de seguridad de la información en COOPEBIS.
Igualmente define la organización de la gestión de incidentes de seguridad, proporciona las reglas para manejar incidentes de seguridad, así como los pasos de la gestión de incidentes de seguridad, desde la detección y reporte hasta la resolución y diagnóstico.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol o sus funciones, tengan algún vínculo con la Cooperativa.

Lineamientos:
Un incidente de seguridad es un evento con impacto en las operaciones habituales de un recurso del Sistema de Información (o de un servicio proporcionado por la función de SI) y que probablemente afecte la confidencialidad, integridad y disponibilidad de la información.

Los incidentes de seguridad pueden tener las siguientes causas:

- Malicia (probada o sospechada, interna o externa):
- Accidentes.
- Errores.
- Fallos/Colapsos Técnicos.

- Intentos de fuentes no autorizadas para acceder a sistemas o datos.
- Interrupción no planificada de un servicio o denegación de un servicio.
- Tratamiento o almacenamiento no autorizado de datos.
- Cambios no autorizados en el hardware, firmware o software del sistema.

Organización de la gestión de incidentes de seguridad

La gestión de incidentes de seguridad debe incluir lo siguiente:

- Definición de los tipos de incidentes de seguridad (fallas, defectos y errores);
- Registro de incidentes de seguridad mediante un mecanismo propio que permita tanto el registro, como el seguimiento, y se deben considerar todas las posibles entradas que podrían desencadenar incidentes de seguridad.

Funciones y responsabilidades de la gestión de incidentes de seguridad

Los roles y responsabilidades de todos los actores involucrados en la gestión de incidentes de seguridad deben identificarse, formalizarse y comunicarse a las personas y departamentos relevantes.

Informes de incidentes de seguridad por parte de proveedores

De acuerdo con la "Política de relaciones con los proveedores", los proveedores deben notificar acerca de cualquier incidente de seguridad en su perímetro que pueda afectar a la Cooperativa y/o causar un incidente de seguridad en el sistema de información (por ejemplo, falta de disponibilidad de un servicio, filtración de datos, virus). El personal de los Proveedores en el sitio debe respetar las mismas reglas y deberes que los empleados con respecto a los incidentes de seguridad (notificación de incidentes, no explotación y validación del cierre).

Aprendizaje obtenido de los incidentes de seguridad de la información

Se debe elaborar una base de conocimiento de incidentes de seguridad y actualizarla periódicamente después de la resolución de cualquier incidente de seguridad para capitalizar el conocimiento y las experiencias y mejorar la eficiencia del proceso de gestión de incidentes de seguridad. Al menos, la base de conocimientos debe contener:

- Descripción de incidentes de seguridad;
- Métodos operativos de resolución.
- La base de conocimientos debe ser accesible para todas las personas involucradas en la resolución de incidentes de seguridad (por ejemplo, equipo de soporte, equipos técnicos, equipos de seguridad), al menos en modo lectura.

Recolección de evidencia y registros

De acuerdo con la "Política de gestión de eventos", se deben recopilar pruebas y registros a lo largo del proceso de gestión de incidentes de seguridad. Podrían ser necesarios en caso de acciones legales o forenses. Deben tener un alto nivel de integridad, de acuerdo con la "Política de Clasificación de la información". Además, todas las decisiones e implementaciones realizadas en el marco de la resolución de incidentes de seguridad deben estar documentadas y aprobadas.

Procedimientos de seguimiento y reporte

Las soluciones y procesos de monitoreo y reporte deben implementarse y comunicarse a todos los actores relevantes y todos los puntos de contacto identificados (por ejemplo, equipo de soporte) a cargo de manejar los incidentes de seguridad. Estos procesos deben definir cómo detectar y reportar incidentes de seguridad, formas de reportarlos y medidas a tomar cuando se reportan incidentes de seguridad (por ejemplo, respuestas a los usuarios, progresividad).

Reporte de incidentes de seguridad

Los canales para la notificación de incidentes de seguridad deben estar disponibles para todas las personas que interactúan con el sistema de información.

- Llamada telefónica al equipo de soporte;
- Informes en una herramienta interna dedicada;
- Envío al equipo de soporte.
- Autoridades (Entidad gubernamental, policía, unidad de delitos informáticos);
- Terceros especializados.

5.22 Política Continuidad de seguridad de la información

Objetivo: Tiene como objetivo definir los requisitos de seguridad de la información con respecto a la continuidad de las actividades de tecnología en caso de presentarse un desastre.

También ayuda a preservar la continuidad del nivel de seguridad de la información durante una situación adversa; además da las reglas para evaluar el nivel de servicio necesario para la recuperación de actividades esenciales y una calidad mínima de servicio en caso de desastre y describe los pasos para la implementación y el mantenimiento en condiciones operativas del plan de continuidad del negocio.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, tengan algún vínculo con la Cooperativa.

Lineamientos:

Planificación de la continuidad de la seguridad de la información

La continuidad de la Seguridad de la Información, será parte integral del BCP (Business Continuity Plan) del Negocio, la continuidad de la seguridad estará en el marco de los planes de contingencia y las actividades de recuperación para los escenarios definidos y validados dentro del alcance del DRP (Disaster Recovery Plan) de Tecnología.

Se debe designar un responsable del DRP dentro de la entidad, quien estará a cargo de la implementación y mantenimiento en condiciones operativas del DRP bajo su alcance. El responsable es el encargado de definir el contexto, el alcance, los objetivos y las limitaciones del DRP. Los roles y responsabilidades de todos los actores involucrados en el DRP deben ser identificados, formalizados y comunicados a las personas y departamentos relevantes.

Todos los empleados de la Cooperativa incluidos en el marco del DRP deben estar capacitados para el DRP y los procedimientos relacionados cuando se active.
El personal (usuarios, operadores, equipos técnicos ...) involucrados en el DRP debe estar específicamente capacitado para aplicar los procedimientos.

Implementación de la continuidad de la seguridad de la información

Los procedimientos de continuidad de la actividad deben crearse para todos los pasos del DRP, aplicarse y actualizarse después de cada actualización significativa y se deben incluir los siguientes temas:

- Procedimiento de activación, también definiendo los roles a cargo de la decisión de activar el DRP (por ejemplo, Gerencia Ejecutiva, Gerente de DRP);
- Procedimiento de comunicación y roles autorizados para comunicarse en función de la población (por ejemplo, clientes, usuarios, medios de comunicación);
- Regreso al procedimiento de normalidad, incluido el aumento del plan de carga y la comunicación sobre la disponibilidad de recursos;
- Cualquier otro procedimiento necesario para la correcta realización del DRP (por ejemplo, activación del sitio de respaldo).

La documentación del DRP debe crearse, actualizarse periódicamente y archivarse de manera segura y debe ser gestionada únicamente por personal autorizado. Esta documentación debe copiarse en un sitio remoto seguro. Los propietarios de la aplicación están a cargo de definir los requisitos de continuidad (incluido RPO / RTO) de la aplicación.

Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Todo el alcance (técnico y organizativo) del DRP debe probarse al menos una vez al año. Estas pruebas deben medir la efectividad del DRP a través de escenarios de prueba definidos (por ejemplo, Interrupción del centro de datos, indisponibilidad de las instalaciones, procesos de recuperación de copias de seguridad).

Además de los equipos técnicos, los usuarios también deben participar para validar el funcionamiento. Debe elaborarse un plan de prueba. Cada prueba del plan de continuidad permite evaluar el nivel de madurez del DRP y debe conducir a:

- Creación de la lista de anomalías (organizativas y técnicas) detectadas durante la prueba;
- Elaboración del listado de acciones correctivas.

Con base en este retorno de la experiencia, el responsable del DRP debe formalizar y monitorear un plan de acción para la mejora del DRP. El DRP debe ser evaluado y actualizado continuamente para asegurar su idoneidad, conveniencia y efectividad con su alcance. Por ejemplo, un cambio de infraestructura, una evolución legal y regulatoria o el reemplazo de aplicaciones comerciales podrían llevar a una actualización del DRP. Los propietarios de activos (software o hardware) son responsables de las actualizaciones de los elementos de continuidad del negocio de sus activos (documentación, trámites). También deben notificar al responsable de DRP de cualquier cambio.

La evaluación de riesgos y todos los elementos que componen el DRP (por ejemplo, la documentación, los procesos, las capacitaciones) deben evaluarse y revisarse una vez al año y, si es necesario, actualizarse.

5.23 Política de cumplimiento de las normas de Seguridad de la Información

Objetivo: Establecer los lineamientos para asegurar el cumplimiento de las políticas descritas en el presente documento.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, tengan algún vínculo con la Cooperativa.

Lineamientos:

Identificación de la legislación aplicable y de los requisitos contractuales

Se deben definir procesos internos que permitan la identificación de los requisitos tanto estatutarios, reglamentarios y contractuales que apliquen para la Cooperativa, igualmente se deben asignar las responsabilidades con respecto al proceso de documentación y actualización de la respectiva matriz de requisitos legales incluyendo propiedad intelectual, privacidad y datos personales.

Privacidad y protección de información de datos personales

Se debe garantizar el cumplimiento de la reglamentación vigente respecto de la privacidad y la protección de la información de datos personales (Ley 1581 del 2012).

5.24 Política para la Gestión de POS (Point of Sales System) incluye PIN-Pad

Objetivo: Establecer los lineamientos para asegurar y garantizar la aplicación de las buenas prácticas en los servicios POS de la Cooperativa, y evitar la materialización de los riesgos relacionados con la seguridad de la información en los POS.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, tengan algún vínculo con la Cooperativa.

Lineamientos:
Las organizaciones solidarias que manejen este tipo de servicios deben verificar que los POS cumplan, como mínimo, con los siguientes requerimientos:

- La lectura de tarjetas solo se deberá hacer a través de la lectora de los datáfonos y los PIN Pad cumpliendo con los estándares PCI-DSS.
- El área de Informática es responsable de validar automáticamente la autenticación del datáfono que se intenta conectar a ellos, así como garantizar que los canales de comunicación se encuentren con los debidos controles criptográficos descritos en el presente documento.
- Establecer procedimientos que le permitan identificar los responsables de los datáfonos en los establecimientos comerciales y confirmar la identidad de los funcionarios autorizados para retirar o hacerles mantenimiento a los equipos.
- Velar porque la información confidencial de los asociados y usuarios no sea almacenada o retenida en el lugar en donde los POS estén siendo utilizados reduciendo la posibilidad que terceros puedan ver la clave digitada por el asociado o usuario.

5.25 Centro de Atención Telefónica (Call Center, Contact Center)

Objetivo: Establecer los lineamientos para asegurar y garantizar la aplicación de las buenas prácticas en los servicios prestado en los centros de atención telefónica de la COOPEBIS, y evitar la materialización de los riesgos relacionados con la seguridad de la información y la privacidad de datos personales.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, tengan algún vínculo con la Cooperativa.

Lineamientos:
Los Centros de Atención Telefónica deberán cumplir, como mínimo, con los siguientes requerimientos para garantizar el cumplimiento al tratamiento de datos personales, según lo establecido en la Ley 1581 del 2012:

- Se debe destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio, la cual deberá contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada.
- Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.
- Garantizar que los equipos destinados a los centros de atención telefónica solo serán utilizados en la prestación de servicios por ese canal.
- En los equipos usados en los Centros de Atención Telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida.
- Estos registros deberán ser conservados, por lo menos un (1) año o, en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

5.26 Política de seguridad para las transacciones por Internet

Objetivo: Establecer los lineamientos para asegurar y garantizar la aplicación de las buenas prácticas en los servicios prestados a través de Internet de COOPEBIS, y evitar la materialización de los riesgos relacionados con la seguridad de la información.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, tengan algún vínculo con la Cooperativa.

Lineamientos:

Se deben implementar los siguientes controles para los servicios prestados a través de Internet:

- Implementar los controles descritos en los algoritmos y protocolos necesarios para brindar una comunicación segura. (HTTPS -SSL)
- Ejecutar como mínimo dos (2) veces al año, una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional, esto debe ir acompañado de su respectivo documento de control de cambios.
- Promover y poner a disposición de los asociados, mecanismos que reduzcan la posibilidad de que la información de sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.
- Definir y establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.
- Informar al asociado, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.
- Implementar mecanismos que permitan a la organización verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.

5.27 Política de seguridad en la nube

Objetivo

Establecer los lineamientos y controles necesarios para garantizar la confidencialidad, integridad, disponibilidad y legalidad de la información y los servicios tecnológicos que se gestionan en ambientes de computación en la nube, de acuerdo con las buenas prácticas de seguridad, las disposiciones normativas del sector solidario y los objetivos estratégicos de la Coopebis.

Alcance:

Esta política aplica a todos los servicios en la nube utilizados Coopebis, incluyendo modelos de servicio (SaaS, PaaS, IaaS) y modelos de despliegue (público, privado, híbrido). Es de cumplimiento obligatorio para todos los colaboradores, contratistas, proveedores y terceros que gestionen o accedan a recursos en la nube en nombre de la cooperativa.

Lineamientos:

1. Evaluación de proveedores:
   - Se deberá realizar una evaluación previa de seguridad, cumplimiento legal y madurez del proveedor de servicios en la nube antes de su contratación.
   - El proveedor debe demostrar cumplimiento con estándares reconocidos como ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, y normas locales (Circular Básica.).

2. Clasificación de la información:
   - La información almacenada o procesada en la nube debe clasificarse conforme a la política de clasificación de la información de la cooperativa.
   - No se permitirá el almacenamiento en la nube de información confidencial o sensible sin las debidas medidas de cifrado y autorización del Oficial de Seguridad de la Información.

3. Autenticación y control de acceso:
   - El acceso a servicios en la nube debe estar protegido mediante autenticación multifactor (MFA).
   - Debe aplicarse el principio de mínimo privilegio, controlando el acceso por roles y realizando revisiones periódicas.

4. Cifrado de datos:
   - Todos los datos sensibles deben estar cifrados en tránsito y en reposo mediante algoritmos criptográficos robustos.
   - Las claves de cifrado deberán gestionarse de forma segura, preferiblemente bajo control exclusivo de la cooperativa.

5. Respaldo y recuperación:
   - Se deben establecer mecanismos de respaldo periódico de la información alojada en la nube y planes de recuperación ante desastres que aseguren la continuidad del negocio.

6. Monitoreo y auditoría:

   - Se debe mantener un monitoreo continuo del uso de los servicios en la nube, incluyendo registros de acceso, cambios y eventos críticos.
   - Los servicios en la nube deben permitir la auditoría de sus operaciones y ofrecer visibilidad a la cooperativa sobre sus datos.

7. Cumplimiento legal y normativo:
   - El uso de servicios en la nube debe cumplir con la legislación aplicable en materia de protección de datos personales, seguridad de la información y normativa del sector solidario.

8. Gestión de incidentes:
   - Todo incidente relacionado con servicios en la nube debe ser gestionado conforme al procedimiento de gestión de incidentes de seguridad de la cooperativa.
   - El proveedor debe notificar de inmediato cualquier brecha de seguridad que afecte los datos o servicios de la cooperativa.

5.28 Política de transformación digital

Objetivo: Establecer los lineamientos para la adopción, implementación y gestión de la transformación digital en la cooperativa, garantizando la mejora continua de los procesos, la optimización de los servicios financieros y el fortalecimiento de la experiencia de los asociados y colaboradores mediante el uso de tecnologías innovadoras.

Alcance: Esta política aplica a todas las áreas de la cooperativa, incluyendo sus colaboradores, proveedores de tecnología y terceros que participen en la digitalización de procesos o prestación de servicios tecnológicos.

Lineamientos:

1. Gobierno Digital:
   a. La cooperativa tendrá un equipo de transformación digital, compuesto por los designados por la gerencia, quienes serán responsables de la planificación y supervisión de las estrategias digitales.
   b. Se establecerán, métricas e indicador para evaluar el impacto de la digitalización en los procesos y la experiencia del asociado.
   c. Las estrategias de transformación digital se presentarán al comité de sistemas de gestión para su revisión y socialización.
2. Digitalización de los servicios:
   a. Se priorizará la automatización de procesos internos para mejorar la eficiencia y reducir tiempos de respuesta.
   b. Se implementarán plataformas digitales para la gestión de productos financieros, tales como banca en línea, pagos electrónicos y autoservicio en sucursales digitales.

c. Se fomentará el uso de firma electrónica y documentos digitales para reducir el uso de papel y agilizar trámites.

3. Seguridad de la información y protección de datos:
   a. Se garantizará la implementación de controles de ciberseguridad en todos los sistemas digitales.
   b. Se cumplirán las normativas vigentes de protección de datos personales, asegurando la confidencialidad, integridad y disponibilidad de la información.
4. Capacitación y cultura digital:
   a. Se capacitará a los colaboradores en herramientas digitales, metodologías ágiles y seguridad de la información.
   b. Se fomentará la adopción de tecnologías emergentes mediante programas de formación y actualización continua.
5. Ecosistema digital:
   a. Se explorarán nuevas tecnologías como inteligencia artificial, blockchain y big data para mejorar la toma de decisiones y personalización de servicios.

Principios:

- Centrado en el Asociado: Todas las iniciativas digitales deben mejorar la experiencia de los asociados y facilitar el acceso a los servicios de la cooperativa.
- Seguridad y Confianza: La adopción tecnológica debe cumplir con normativas de seguridad de la información, protección de datos y continuidad del negocio.
- Innovación y Mejora Continua: Se fomentará una cultura de innovación que impulse la eficiencia operativa y la creación de nuevos productos y servicios digitales.
- Interoperabilidad y Escalabilidad: Las soluciones tecnológicas deben ser compatibles con los sistemas existentes y permitir futuras mejoras.
- Cumplimiento Normativo: Toda implementación digital debe alinearse con las regulaciones del sector solidario.

5.29 Cumplimiento de las políticas y normas de Seguridad de la Información.

Objetivo: Establecer los lineamientos para asegurar y garantizar la aplicación de todas las políticas y procedimientos que hacen parte del Sistema de Gestión de Seguridad de la Información de COOPEBIS.

Alcance: La presente política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, tengan algún vínculo con la Cooperativa.

Lineamientos:

1. **Cumplimiento de políticas**: Todos los lineamientos detallados en este documento son de total y estricto cumplimiento luego de la aprobación y socialización formal, por parte del consejo de administración, a toda la Cooperativa. Cualquier excepción o exclusión de alguno o todos los lineamientos de alguna de las políticas descritas en este documento debe estar debidamente argumentada y soportada por el solicitante y autorizada por el líder de seguridad de la información y el director del área de Informática.

2. **Revisión de políticas:** Todas las políticas de seguridad de la información se deben revisar y aprobar por el consejo de administración mínimo una vez al año o cuando se presenten cambios que ameriten la revisión y posterior modificación.

3. **Consecuencias del Incumplimiento:** El incumplimiento de alguna política descrita en este documento traerá consigo las consecuencias legales que de ello se deriven de conformidad con la normatividad aplicable al caso y a los procedimientos adoptados por la Cooperativa para tales fines. El incumplimiento puede llegar a sanciones administrativas, disciplinarias y hasta penales como lo establece la Ley 1273 de 2009 de Delitos Informáticos.

4. **Capacitación periódica:** La cooperativa llevará a cabo programas de capacitación periódica en materia de seguridad de la información y prevención de fraude financiero. Estos programas están diseñados para asegurar que todos los colaboradores y asociados estén debidamente informados y capacitados sobre las mejores prácticas y procedimientos para proteger la información y prevenir actividades fraudulentas. La participación en estas capacitaciones es obligatoria.

5. **Divulgación de canales de contacto:** Para proporcionar asistencia en caso de que los colaboradores y asociados sean víctimas de fraude financiero, la cooperativa divulgará periódicamente los canales de contacto establecidos. Estos canales estarán disponibles para recibir reportes de incidentes y brindar el soporte necesario.

6. RECONOCIMIENTO Y CONSENTIMIENTO

La violación e incumplimiento de estas políticas acarrearan las medidas disciplinarias, a las que conlleva una falta administrativa, pudiendo dar lugar esto a suspensión, despido, o cualquier acción en los términos legales vigentes.

Estas Políticas de seguridad informática, tienen vigencia a partir de su fecha de aprobación y hasta cuando una decisión administrativa de nivel Gerencial decida modificarlas y/o reestructurarlas.

Aprobado por el Consejo de Administración a los 31 días del mes de mayo del año 2025 y deroga todas las disposiciones que le sean contrarias.

7. DOCUMENTOS DE REFERENCIA

- Circular 036 de 2022, y su anexo #2 de la Superintendencia de la Economía Solidaria que dicta las instrucciones sobre seguridad y calidad de la información para la prestación de los servicios financieros.
- Norma ISO/IEC 27001.
- Ley 527 de 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
- Decreto 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012
- Decreto 103 de 2015 por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
- Decreto 1008 de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

- ISO/IEC 27001:2013 (Icontec, 2013) Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Especifica los requisitos para establecer, implantar, mantener y seguir mejorando los Sistemas de Gestión de Seguridad de la Información (SGSI) en el contexto de las organizaciones.
- ISO-IEC 27002:2013 (Icontec, 2015) Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información.

8. FORMATOS

- Ninguno

9. CONTROL DE CAMBIOS

VERSIÓN QUE CAMBIA	FECHA DEL CAMBIO	RAZÓN DEL CAMBIO	CARGO / AREA QUE SOLICITA EL CAMBIO
0	30/11/2009	Cambio de Plantilla del documento Inclusión del punto de Reconocimiento y Consentimiento	Dueño de Proceso
1	28 12 2010	Cambio de Plantilla del documento Inclusión del punto de Reconocimiento y Consentimiento	Dueño de Proceso
2	20/12/2012	Cambio de codificación PO-SI-001 a PO-TIC-001	Jefe de Planeación
3	25/09/2013	Revisión, Actualización y publicación de las Políticas de Seguridad de la Cooperativa	Jefe de Informática y Gerencia
4	09/27/2013	Numeral 7: Adicción en tiempos para reasignación de equipos, Uso del formato FO-TIC-005. Numeral 8: Cambio de nombre en el cargo, por reforma organizacional. Modificación en litera d. Adición de l Literal e. Numeral 9. adición de literal r. Numeral 11: Modificación literal a. Numeral 14: Modificación literal b. Eliminación del VoBo. de Auditoría Interna para la asignación de perfiles en el literal J del numeral 5.2.	Jefe de Informática
6	22/03/2023	Ajuste del documento por implementación del SGSI y ajuste a los lineamientos	Profesional de Planeación

ELABORÓ	REVISÓ	APROBÓ
CESAR CIFUENTES ALZATE DIRECTOR DE INFORMÁTICA	OSCAR JAVIER ZABALETA URREGO GERENTE	CONSEJO DE ADMINISTRACIÓN MEDIANTE ACTA No. 1127 DEL 31 DE MAYO DE 2025

		establecidos en la Circular 036 de la Supersolidaria y al sistema de información ISODOC	
7	2024-07-11	Modificación y actualización de numerales 5.2 Política para el uso de dispositivos móviles; 5.3 5.3 Política de Seguridad de la Información para el Trabajo Remoto; 5.4 Política de Gestión de Activos; 5.5 Política de Clasificación de la Información; 5.6 Política de Gestión de medios removibles; 5.10 Política para Gestión de Cambios. Inclusión de los numerales 4 (Capacitación periódica) y 5 (Divulgación canales de contacto) en el numeral 5.27 "Cumplimiento de las políticas y normas de seguridad de la información.	Jefe de Informática
8	31/05/2025	Actualización cargo de jefe de informática a director de informática; Adición de política de seguridad en la nube y política de transformación digital	Director Comercial Área de Planeación

HE LEIDO, ENTIENDO Y ACEPTO LAS CONDICIONES DE USO DEL PRESENTE DOCUMENTO BAJO EL CUAL LA COOPERATIVA PARA EL BIENESTAR SOCIAL COOPEBIS ME PERMITE USAR LOS SISTEMAS INFORMATICOS. ENTIENDO TAMBIÉN QUE EL INCUMPLIMIENTO DE ESTOS TERMINOS Y REQUERIMIENTOS, PUEDEN OCASIONAR ACCIONES DISCIPLINARIAS, INCLUYENDO EL DESPIDO CON JUSTA CAUSA.

Copia: Hoja de Vida del Trabajador

ORIGINAL FIRMADO

Firma: _____

Nombre: _____

Cargo: _____

Fecha: _____

ELABORÓ	REVISÓ	APROBÓ
CESAR CIFUENTES ALZATE DIRECTOR DE INFORMÁTICA	OSCAR JAVIER ZABALETA URREGO GERENTE	CONSEJO DE ADMINISTRACIÓN MEDIANTE ACTA No. 1127 DEL 31 DE MAYO DE 2025