Las consideraciones de seguridad deben ser cumplidas por los funcionarios, proveedores y/o contratistas y en general toda persona (terceros) que haga uso o interactúe de alguna forma con los recursos tecnológicos de la Cooperativa COONFIE. Todos deben conocer la intención de la Cooperativa en materia de seguridad y protección de la información, se presenta las siguientes políticas.

1. Política General de Seguridad de la Información

COONFIE para el cumplimiento de su misión, visión, objetivos estratégicos y valores corporativos asignara a través del Consejo de Administración y la Gerencia General los recursos humanos, financieros y tecnológicos necesarios para la implementación del Sistema de Gestión de Seguridad de la información, con el objetivo de minimizar los riesgos a los cuales se expone los activos de información, ayudar a la reducción de costos operativos y financieros, establecer una cultura de seguridad y garantizar el cumplimiento de los requerimientos legales y de negocio vigentes, aplicando los elementos necesarios para establecer, implementar, mantener y proveer mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

La subgerencia de sistemas, el comité de seguridad de la información, auditor interno y la dirección de SIAR definirán y aplicarán una metodología de monitoreo y evaluación para dar cumplimiento al presente manual, con el objetivo de identificar correcciones, cambios o nuevos riesgos. La información es un recurso fundamental que como el resto de los activos tiene un valor para la Cooperativa, razón por la cual existe un compromiso de protección de sus propiedades como parte de una estrategia orientada a la continuidad del negocio, la administración y control de riesgos para la prestación de sus servicios.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes de información y recursos de procesamiento, deben adoptar los lineamientos contenidos en el presente manual, con el fin de mantener los niveles adecuados que garanticen la integridad, disponibilidad y confidencialidad de la información.

COONFIE designa como responsable de la seguridad de la información al Subgerente de sistemas, quién debe velar por el cumplimiento de la normatividad vigente al interior de la Cooperativa respecto a estas políticas que involucran a asociados, funcionarios directos y en misión, aprendices, proveedores, contratistas y comunidad en general.

1.1 Cumplimiento con la seguridad de la información

Todos los funcionarios y personal provisto por terceras partes vinculados a la Cooperativa deben cumplir y acatar las *Condiciones generales de la seguridad de la información*, el *Manual del sistema de gestión de seguridad de la información,* así como sus documentos relacionados en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Dirección del SIAR, Subgerencia de Sistemas y Auditoría Interna.

1.2 Obligaciones

Deben salvaguardar la Confidencialidad, Integridad, Disponibilidad de la Información que administre y/o maneje dentro de la Cooperativa Coonfie durante la vigencia del contrato o vínculo laboral, así como realizar la respectiva devolución de la información digital y/o física que le fue entregada al momento de iniciar el contrato o vínculo laboral y durante la vigencia de este hasta su finalización.

Todo usuario debe firmar el formato *Aceptación de Cumplimiento de la Política General de la Seguridad de la Información* antes de otorgarle cualquier tipo de información sin importar el medio en el que se maneje, o su identificación de usuario y contraseña y sus respectivos privilegios para el uso de los recursos tecnológicos de la Cooperativa COONFIE, este formato también cubre a empleados temporales, consultores y toda aquella persona o empresa que de una u otra manera tenga acceso a la información de la Cooperativa.

Cualquier acceso por parte de un tercero a los recursos tecnológicos o a la información de la Cooperativa, debe haber cumplido con las autorizaciones respectivas y además estén debidamente firmados los acuerdos de confidencialidad, formato *Aceptación de Cumplimiento de la Política General de la Seguridad de la Información* y el formato *Autorización Uso de Equipo de Trabajo de Terceros.*

1.3 Seguridad física y ambiental

Todos los funcionarios, contratistas y terceras partes deben tener asignados privilegios de acceso a las áreas seguras de la Cooperativa, es responsabilidad de la Subgerencia de Sistemas, su manejo y control. En caso de finalización de contratos se deben eliminar inmediatamente los privilegios de acceso físico.

1.4 Gestión de comunicaciones y operaciones

Toda conexión a los servicios de la Cooperativa proveniente del exterior sea Internet, redes externas o redes internas (subredes) debe pasar primero por un sistema de protección perimetral (Firewall), con el fin de limitar y controlar el tráfico de red a los activos de información de la Cooperativa.

El sistema de protección de perímetro (firewall) debe ser el único dispositivo conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por dicho componente tecnológico.

1.5 Control de acceso

- Los derechos de acceso a los usuarios serán revisados al menos una vez al año con el fin de mantener un control eficaz de acceso a los datos y a los servicios de información, labor que será realizada por el propietario o responsable del Sistema de Información en acompañamiento de la Coordinación de SGSI e Infraestructura.
- Todos los usuarios de recursos tecnológicos e información deben poseer un identificador único.
- Los identificadores de usuarios genéricos en cualquier sistema operacional, base de datos, o aplicación, deben estar debidamente documentados en caso de ser utilizados.
- Todos los sistemas y computadores deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores. Se brindarán permisos de administrador a los usuarios que lo requieran, siempre y cuando exista una previa validación por parte de la Subgerencia de Sistemas, en donde se valide que se requieren este tipo de permisos especiales para la ejecución de un software o alguna herramienta que no permite la misma bajo el tipo de usuario estándar.
- Los privilegios asignados a los usuarios deben estar asociados a los Sistemas de Información que corresponda de acuerdo con el rol del funcionario en la Cooperativa. Es responsabilidad del líder de área encargado del o los Sistemas de Información definir los privilegios y notificar a los administradores respectivos para su adecuada asignación.
- Las contraseñas iniciales otorgadas deben servir únicamente para el primer ingreso del usuario al sistema, en ese momento el sistema debe obligar al usuario a cambiar su contraseña.
- El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. Después de cinco (5) intentos fallidos el identificador del usuario debe ser bloqueado hasta nueva reactivación por parte del administrador, después que se compruebe la identidad del usuario.
- Todos los sistemas de información de la organización deben validar que las contraseñas deben tener como longitud mínima de 8 caracteres, de igual manera deben validar que no se involucren contraseñas en blanco.
- Los sistemas de información, o componentes tecnológicos que involucren un proceso de autenticación de usuarios debe mantener historia de al menos las últimas 15 contraseñas utilizadas por parte de los usuarios, de tal manera que no puedan ser reutilizadas.
- Todos los sistemas de información de la Cooperativa o cualquier recurso tecnológico que involucre un sistema de control de acceso basado en credenciales (login, contraseña), deben validar como vigencia

de la contraseña un periodo de 30 días hábiles, pasado este tiempo la contraseña debe expirar y bloquear la cuenta del usuario.

- Todos los sistemas y computadores de la organización, debe tener involucrado un sistema de control de acceso, así como un conjunto de credenciales que lo habiliten para utilizar los recursos de la organización.
- Los accesos a los sistemas de archivos de red de la organización deben bloquear por defecto el acceso de usuarios no autorizados. Se excluyen las carpetas que hayan sido definidas de propósito PÚBLICO a la cual pueden tener acceso todos los usuarios para intercambio de archivos.

1.6 Cumplimiento

- Los recursos informáticos de la Cooperativa deben ser usados para fines laborales. Cualquier otro uso debe ser realizado está restringido de manera que no interfiera con la productividad de la persona o con las actividades propias de la Cooperativa.
- Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien fue otorgada dicha identificación. Los usuarios no deben permitir que otros usuarios realicen labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la Cooperativa COONFIE.
- La Cooperativa COONFIE usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos COONFIE se reserva el derecho y la autoridad de: 1. Restringir o revocar los privilegios de cualquier usuario; 2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y, 3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de la Cooperativa. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, con conocimiento del jefe inmediato, siempre con el concurso del Subgerente de Sistemas o de quién él delegue esta función.
- Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario.
- Los usuarios no deben buscar, probar y /o explotar las deficiencias de seguridad de los sistemas de información, En el caso de evidenciarlas en la ejecucion de sus funcionesn, estas deben ser reportadas de inmediato a la Subgerencia de Sistemas o al Coordinador de SGSI e infraestructura.
- Los usuarios no deben dejar el computador desatendido sin haber bloqueado la primero la sesión iniciada.
- Todos los colaboradores deben revisar, e investigar los derechos de propiedad intelectual para todo material, software y/o sitio Web encontrado en Internet antes de ser usado para cualquier propósito que esté relacionado con la Cooperativa.
- La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por los funcionarios autorizados de la Subgerencia de Sistemas.
- En ninguna circunstancia es posible almacenar o usar cualquier juego en los recursos computacionales suministrados por la Cooperativa COONFIE.
- Cuando su uso está permitido, es responsabilidad de los usuarios revisar cualquier medio extraíble (memorias USB, CDs, DVDs, teléfonos móviles USBs, cámaras con memoria con conexión a USB y en general cualquier dispositivo que almacene archivos y sea conectable al computador a través de puerto USB), que sea insertado al computador de tal manera que se eviten posibles contagios de software malicioso.
- La contraseña que a cada usuario se le asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible, cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.
- Ninguna contraseña debe ser guardada de forma legible en archivos “Bach”, scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Se recomienda no tener su contraseña en cualquier medio impreso.

- Toda contraseña deberá ser cambiada por el usuario de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.
- En ninguna circunstancia está permitido revelar la contraseña a funcionarios o a personal provisto por terceros. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Cooperativa. Ningún usuario deberá intentar obtener contraseñas de otros usuarios.
- Todas las estaciones de trabajo de los usuarios deben tener activado el protector de pantalla protegida por contraseña, adicional a que no se debe instalar un papel tapiz diferente a los especificados.
- La Información de la Cooperativa COONFIE debe ser usada única y exclusivamente para los propósitos de la función que desempeña el colaborador dentro de su entorno laboral. De igual manera el uso y acceso de la información de la organización debe ser consistente con las políticas que existan.
- La Cooperativa COONFIE tiene la propiedad legal del contenido de todos los archivos almacenados en cualquier sistema informático suministrado, así como cualquier mensaje de datos transmitido vía estos sistemas. La Cooperativa se reserva el derecho de utilizar la información para el desarrollo de sus actividades.
- El uso de Internet se asigna para propósitos laborales y está dado según el cargo y funciones de este. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas.
- El correo electrónico debe ser usado únicamente para los propósitos del trabajo y de ninguna manera para fines personales. Se recomienda usar términos y expresiones adecuadas como en otros medios de comunicación formal de la Cooperativa, para que no sean interpretados al relacionarse con asociados o terceros como la postura oficial de la Cooperativa.
- Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto, podrá ser supervisada por el superior inmediato del empleado.
- La cuenta de correo asignada es de carácter individual y está ligada directamente al cargo, su información solo debe ser accedida por el funcionario que se encuentre asignado a este, y de ninguna manera deberá ser accedida por otro funcionario. Dado el caso de que el cargo sea ocupado por un nuevo funcionario, así mismo será la responsabilidad sobre la cuenta de correo y su buzón asociado.
- La Cooperativa puede utilizar componentes tecnológicos que permitan el bloqueo a sitios de Internet que se consideren cuestionables o cuyo propósito no sea el estrictamente el cumplimiento de sus funciones.
- Los usuarios de la Cooperativa deben abstenerse de descargar a través de Internet videos, audio e imágenes a menos que estas descargas estén debidamente justificadas para propósitos laborales, de la misma manera el acceso, observación o cualquier forma de utilización de sitios Web que en su contenido contemple pornografía, juegos, racismo o que de alguna forma atenten contra los derechos fundamentales, normatividades de ley, reglamento interno de trabajo, la presente normatividad o demás reglas que rigen a la Cooperativa.
- Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones que se utilizan en los sistemas de información de la organización.
- La Cooperativa monitoreará de manera continua y constante el tráfico que circula hacia o de Internet.
- La Cooperativa se reserva el derecho de monitorear y/o revisar los mensajes de correo electrónico corporativo sin notificar al usuario de la acción a realizar.
- Los usuarios deben abstenerse de abrir archivos adjuntos de correos electrónicos de los cuales desconozcan el remitente.
- Los funcionarios de la Cooperativa deben abstenerse de participar en redes sociales, foros, blogs y demás medios electrónicos de intercambio de información, con información relevante de la organización, a menos que está esté debidamente autorizado.
- Cada funcionario es responsable del respaldo de la información y los datos almacenados en los computadores o portátiles según los lineamientos establecidos por la Cooperativa y debe hacerse con regularidad evitando así perdidas de información por cuenta de alguna falla con el dispositivo.
- La subgerencia de Sistemas es la única área autorizada para revisar la configuración, programación, mantenimiento, actualización, administración y monitoreo los sistemas de información de la Cooperativa.

- A menos que exista una autorización de la Subgerencia de Sistemas escrita, ningún sistema de control de la infraestructura de seguridad debe ser desactivado, inhabilitado, desconectado, apagado, o sobrepasado.

1.7 Prohibiciones

- Actuaciones que conllevan a la violación de la seguridad de la información establecidas por Coonfie.
- No firmar los acuerdos de confidencialidad, aceptación de políticas de seguridad y sus consideraciones de seguridad.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, “documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada)”.
- Copiar cualquiera de los aplicativos que se aloja en los computadores de la Cooperativa.
- Obtener acceso a sistemas de información a los que no se tiene permitido el acceso e igualmente se prohíbe cualquier modificación o consulta de la información contenida en el sistema. Esto implica la prohibición de capturar contraseñas, llaves de cifrado y otros mecanismos de control de acceso que le puedan permitir obtener acceso a sistemas no autorizados.
- No grabar la información digital producto del procesamiento de la información perteneciente al Cooperativa.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Dejar las cajoneras abiertas o con las llaves puestas en los escritorios.
- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas a la Cooperativa deambulen sin acompañamiento, al interior de las instalaciones y en áreas no destinadas al público.
- Almacenar información corporativa en cualquier medio de almacenamiento que no sean propiedad de la Cooperativa, como computadores, dispositivos móviles personales, dispositivos de almacenamiento masivo como memorias flash de conexión USB, tarjetas SD y CD-DVD.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la Cooperativa, para obtener, mantener o difundir en los equipos de sistemas, material fraudulento, difamatorio, de vandalismo, pornográfico (penalizado por la ley) u ofensivo.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos de seguridad establecidos para la divulgación.
- Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, publicitarios, en cadena o masivos no autorizados, y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.
- Utilizar equipos electrónicos o tecnológicos desatendidos o que, a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.

- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por la Subgerencia de Sistemas.
- Permitir el acceso de funcionarios a la red corporativa, sin la debida autorización.
- Utilización de servicios disponibles a través de internet, no permitidos o uso de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Cooperativa.
- No cumplir con las actividades designadas para la protección de los activos de información.
- Destruir o desechar de forma incorrecta la documentación institucional.
- Descuidar documentación con información pública reservada o clasificada sin las medidas apropiadas de seguridad que garanticen su protección.
- Registrar información pública reservada o clasificada, en apuntes, agendas, libretas, etc. Sin el debido cuidado.
- Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos, sin la debida autorización.
- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos para beneficio personal.
- Acceder sin autorización en todo o parte del sistema informático o se mantenga dentro del mismo en contra de las autorizaciones otorgadas.
- Impedir u obstaculizar el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones, sin estar autorizado.
- Destruir, dañar, borrar, deteriorar o suprimir datos informáticos o un sistema de información.
- Distribuir, enviar, introducir software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica.
- Superar las medidas de seguridad informática para suplantar un usuario ante los sistemas de autenticación y autorización establecidos.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de COONFIE o de terceros.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por la seguridad de la Cooperativa.
- Retirar de las instalaciones de la Cooperativa, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- Sustraer documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento, para traslado, reasignación o para disposición final.
- Usar cualquiera de los recursos tecnológicos de la Cooperativa para difamar, abusar, afectar la reputación o presentar una mala imagen de COONFIE o de alguno de sus funcionarios.
- Realizar cambios no autorizados en la plataforma tecnológica de COONFIE.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por la Subgerencia de Sistemas.
- Se prohíbe interceptar datos informáticos en su origen, destino o en el interior de cual sistema informático o las emisiones electromagnéticas provenientes de un sistema informático que los transporte (redes inalámbricas) de la Cooperativa sin tener la autorización o consentimiento del comité de seguridad de la información.

2. Política de Conexión VPN

Los usuarios externos de empresas que tengan relación con la Cooperativa **COONFIE** por motivos de asesoría, consultoría y/o soporte podrán solicitar el servicio de conexión remota por redes privadas virtuales (VPN).

El túnel VPN permite acceder a determinados servicios de red de la Cooperativa **COONFIE** desde la cualquier ubicación en Internet, y operar con los recursos habilitados como si se hiciera desde dentro de la red interna. Para ello se requiere la instalación en el equipo de un software específico (cliente de VPN) que será instalado por la subgerencia de sistemas en una ventana de instalación programada por las partes.

2.1 Obligaciones

Todos los usuarios que tengan habilitado el servicio de VPN se obligan expresamente a:

- Usar los datos facilitados y la conexión de VPN exclusivamente para tareas relacionadas con su puesto de trabajo o la prestación del servicio (en caso de personal externo)
- Tratar los datos de carácter personal con la máxima cautela con el fin de garantizar su confidencialidad e integridad, adoptando las medidas técnicas y organizativas necesarias en lo que respecta a la custodia, almacenamiento y conservación con el fin de evitar su alteración, pérdida, tratamiento o acceso no autorizado.
- Adoptar todas las medidas necesarias para el cumplimiento de las obligaciones derivadas de la Ley 1581 de 2012 de Protección de Datos Personales.
- Finalizadas la relación contractual o la labor por la cual se dio origen a la ***Solicitud de Conexión VPN*** con la Cooperativa **COONFIE**, o alcanzada la fecha de finalización del servicio, se cancelará la conexión automáticamente.

2.2 Incidentes de Seguridad

En caso de que se produjese algún incidente de seguridad originado por la conexión VPN, ambos responsables que figuren en la solicitud colaborarán de forma activa con subgerencia de Sistemas de la Cooperativa **COONFIE** aportando la información que se le pudiera requerir.

2.3 Recomendaciones

- Instale, configure y pruebe con suficiente antelación el cliente VPN necesario para la conexión.
- No facilite a nadie las credenciales de acceso.
- Contar con un software de antivirus actualizado a la fecha.
- Contar con el sistema operativo actualizado y activado legalmente.
- Evitar utilizar el servicio de conexión remota VPN desde computadores públicos o desconocidos como, cafés internet, aeropuertos, hoteles o redes inalámbricas públicas.
- Abstenerse de usar el servicio VPN en caso de estar infectado por virus informático.
- Desconectarse del servicio una vez finalizada la sesión de tareas o consultas a realizar.

3 Política de Uso Aceptable Red Inalámbrica

3.1 Consideraciones Generales

El servicio de WiFi permite conectar a Internet usuarios simultáneamente a través de equipos como computadores, tablets, smartphones, celulares y equipos portátiles mediante el uso de radiofrecuencias, lo que representa un ahorro en infraestructura de medios físicos, cableado, puertos, entre otros, brindando un servicio completamente móvil. Esta solución tecnológica ha sido implementada para brindar el servicio de conectividad a Internet y a los recursos de la Cooperativa al personal provisto por terceras partes y funcionarios dentro de las instalaciones de la COONFIE en las diferentes sedes, permitiendo así el intercambio de información y acceso con un servicio óptimo y confiable.

Al crear zonas Wifi en las sedes se obtienen los siguientes beneficios:

- Optimizar la prestación del servicio de conexión a los recursos tecnológicos autorizados a los funcionarios y al personal provisto por terceras partes para la realización y cumplimiento de las funciones-labores para las cuales les es necesario el uso de movilidad provista por esta tecnología.
- Administración de las conexiones vía web, optimizando así el ancho de banda para cada usuario.
- Movilidad a los usuarios, garantizando una conexión continua, con acceso controlado a los recursos de la Cooperativa en todas las oficinas.

3.2 Condiciones Generales del Servicio

El presente documento establece los lineamientos para el acceso y uso de las redes inalámbricas de la Cooperativa COONFIE y son aplicables a todos los usuarios del servicio. Todos los usuarios al acceder a las redes inalámbricas aceptan de manera directa las políticas, términos y condiciones de uso descritos a continuación sin ninguna reserva, así como las políticas de seguridad de la Información de la entidad, las de protección de datos personales y cualquier condición adicional que en el futuro se pudiera complementar en estos lineamientos.

3.2.1 Términos y Condiciones de la red Wifi para visitantes

El funcionario y/o personal provisto por terceras partes podrá hacer uso de la red de Wifi de COONFIE después de leer y verificar los términos y condiciones de uso de la red y las Políticas de Seguridad y protección de datos personales.

- Al acceder y utilizar la red de Wifi de COONFIE los usuarios declaran que han leído, entendido y acepta los términos y condiciones para su utilización. Si el visitante no está de acuerdo con esta normatividad no podrá acceder a este servicio.
- El visitante acepta y reconoce que hay riesgos potenciales a través de un servicio Wifi. Deben tener cuidado al trasmitir datos como: número de tarjetas de crédito, contraseñas u otra información personal sensible a través de redes WIFI. COONFIE no puede y no garantiza la privacidad y seguridad de sus datos y de las comunicaciones al utilizar este servicio.
- La Entidad puede establecer límites de uso, suspender el servicio o bloquear ciertos comportamientos, acceso a ciertos servicios o dominios para proteger la rede de la Cooperativo de fraudes o actividades que atenten contra leyes nacionales e internacionales.

3.2.2 No se podrá utilizar las redes de Wifi de Visitantes con los siguientes fines:

El funcionario y/o personal provisto por terceras partes se compromete a usar el servicio de acceso Wifi de forma diligente y correcta y se compromete a no utilizarlo para la realización de actividades contrarias a la ley, a la moral, a las buenas costumbres aceptadas y/o con fines o efectos ilícitos, prohibidos o lesivos de derechos e intereses de terceros, así como a no realizar ningún tipo de uso que de cualquier forma pueda dañar, inutilizar, sobrecargar, deteriorar o impedir la normal utilización del servicio, los documentos, archivos y toda clase de contenidos

almacenados en cualquier equipo informático accesible a través de Internet. La Cooperativa declina cualquier responsabilidad que de todo ello pudiera derivarse con toda la extensión que permita el ordenamiento jurídico.

Con carácter enunciativo, no se permiten intercambiar contenidos que incluyan material que infrinja derechos de autor no debidamente autorizados, o que infrinja cualquier otro derecho de Propiedad Intelectual o Industrial, material ofensivo para la comunidad y la moral pública material que realice apología del terrorismo, racismo, u otras conductas ilegales, material pornográfico, especialmente el que atente contra menores, materiales amenazadores, difamatorios o que inciten a la violencia contenidos ilegales o ilícitos de cualquier naturaleza. Asimismo, igualmente a título enunciativo pero no limitativo, el funcionario y/o personal se compromete a no utilizar, transmitir o difundir: lenguaje difamatorio, amenazante o que sea contrario al derecho al honor, a la intimidad personal o familiar o la propia imagen de las personas físicas y jurídicas, acceder ilegalmente o sin autorización a sistemas, o redes que pertenezcan a otra persona, o a tratar de superar medidas de seguridad del sistema de otra persona (“hacking”), cualquier actividad que pueda ser usada como causante de un ataque a un sistema (escaneo de puertos, etc.). Distribución de virus, gusanos, troyanos a través de Internet, o cualquier otra actividad destructiva; Distribuir información acerca de creación o transmisión de virus por Internet, gusanos, troyanos, saturación, “mailbombing”, o ataques de denegación de servicio; Creación o gestión de bootnets; También actividades que interrumpan o interfieran en el uso efectivo de los recursos de red de otras personas o la realización de “spamming”. Realizar un uso fraudulento de la dirección IP proporcionada en cada acceso, Cualquier otra forma que sea contraria, menosprecie o atente contra los Derechos Fundamentales y las libertades públicas reconocidas en la Constitución, en los Tratados Internacionales.

La Cooperativa COONFIE se reserva el derecho a suspender y/o bloquear el servicio de forma inmediata y sin previo aviso en caso de detectar usos del servicio incumpliendo lo dispuesto en esta cláusula.

3.2.3 Configuración del servicio en el dispositivo:

Los usuarios son responsables de configurar sus dispositivos con los procedimientos básicos para el funcionamiento dentro de la red inalámbrica y de acuerdo protocolo creado para el efecto.

3.2.4 Disponibilidad del servicio:

El servicio de conexión a la red inalámbrica estará disponible, excepto en situaciones de fuerza mayor, o por cortes parciales o interrupciones relativas al mantenimiento preventivo o correctivo de los equipos y elementos que componen la infraestructura de red inalámbrica, así como de los relacionados a la prestación del servicio de Internet.

El servicio se ha diseñado y desplegado para minimizar el impacto de redes inalámbricas vecinas, debido a las características propias de esta tecnología y su medio de transmisión, es decir la disponibilidad y calidad del servicio está sujeta a la interferencia de redes inalámbricas de terceros y/o a la cantidad de usuarios conectados a la red.

3.2.5 Restricciones del servicio:

- El acceso a Internet está restringido de acuerdo con las políticas de seguridad de la entidad, por lo tanto, se prohíbe el acceso a páginas relacionadas o de contenido inapropiado como pornográfico, juegos, hacking, entre otros. La Cooperativa COONFIE podrá limitar o negar el acceso a sitios o lugares que considere peligrosos o de dudoso destino sin que esto se considere una disminución o falla del servicio.
- Sobre la red inalámbrica se ha habilitado un ancho de banda máximo de 10Mbps, el cual es compartido por los usuarios conectados a ella. Es responsabilidad de los usuarios hacer uso eficiente y racional de este recurso para el aprovechamiento y beneficio de todos los usuarios.
- Para el acceso a la red inalámbrica, los equipos deberán soportar el estándar de comunicación 802.11 b/g/n y soportar cifrado WPA2.

3.3 Responsabilidad frente al Servicio

La subgerencia de Sistemas es responsable de mantener en operación la infraestructura que proporciona red a los puntos de acceso a las redes inalámbricas. El soporte a incidentes sobre esta plataforma solo se brindará a los funcionarios y/o personal provisto por terceras partes que hagan uso de ella para el desempeño de sus labores. Es responsabilidad del tercero contar con el software y configuración de seguridad en su equipo personal para minimizar el riesgo al que se puede ver expuesto a un ataque informático al encontrarse conectado sobre esta red.

De ninguna forma ni caso específico la Cooperativa COONFIE será responsable por cualquier daño que pueda sufrir el equipo o dispositivo personal usado para establecer conexión a la red inalámbrica. Los usuarios son los responsables de toda actividad que se lleve desde su equipo o dispositivo mientras esté conectado a la red inalámbrica. Es obligación del usuario informar a la subgerencia de Sistemas y la dirección del SIAR, la violación de alguna de las consideraciones descritas en este documento tanto por personas ajenas o funcionarios de la Cooperativa. Es responsabilidad del usuario estar enterado de los cambios de las presentes indicaciones.

Es responsabilidad del usuario la seguridad física de su equipo o dispositivo, por lo que la Cooperativa no es en ninguna forma responsable por robo o daños al equipo del usuario.

3.4 Prohibiciones

El usuario se compromete a hacer uso productivo y seguro de la red inalámbrica, según los niveles de acceso a los recursos establecidos por la Cooperativa COONFIE.

Al hacer uso de la red Wifi está estrictamente prohibido:

El uso personal de los recursos tecnológicos para fines distintos a los permitidos.

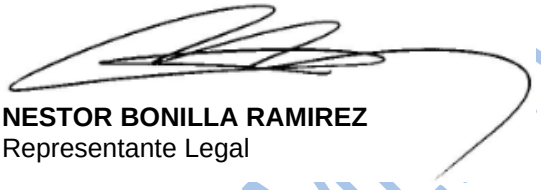
- El uso para generar ganancias monetarias personales o propósitos comerciales.
- Transmitir y/o distribuir cualquier material que viole la ley o regulación de derechos de autor u otros derechos de propiedad intelectual, como software sin licencia, música, videos, películas, entre otros.
- Revelar o ceder las credenciales de autenticación de la red inalámbrica a personal no autorizado.
- Usar programas “peer to peer” (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.
- Extender el alcance de la red por medio de cualquier dispositivo físico o lógico.
- Manipular los equipos de transmisión de la red inalámbrica.
- Instalar o realizar labores de recolección o escucha de información en tránsito por la red.
- El uso del servicio para interferir o molestar a otros usuarios o entorpecer asuntos propios de COONFIE.
- Transgredir cualquier recurso informático, sistema o sitios de telecomunicaciones a los que no le está permitido acceder.
- Instalar equipos y/o software que genere interrupción o interferencia con la emisión normal de la red inalámbrica.
- Realizar el escaneo de vulnerabilidades de la red o de cualquier equipo de esta sin la expresa autorización de la Subgerencia de Sistemas.
- Monitorear los canales de transmisión y comunicación por personas que no pertenezcan a la Cooperativa COONFIE o no estén debidamente autorizadas.
- Cualquier conducta que viole las normas generalmente aceptadas dentro de la comunidad de Internet.
- Realizar alguna acción establecida en la Ley 1273 de 2009 – Ley de delitos informáticos

3.5 Suspensión del Servicio

La Subgerencia de Sistemas podrá definir límites de uso, bloquear, suspender o desactivar temporalmente los servicios o cancelarlos definitivamente a uno o varios usuarios si detecta un uso indebido de la red inalámbrica.

3.5.1 Causas de suspensión:

- Efectuar descargas de manera desmesurada, que afecten el desempeño del servicio de los demás usuarios de la red inalámbrica.
- Transmisión de contenido inapropiado.
- Incumplimiento de las políticas de seguridad de la información.
- Generar o distribuir malware (virus, troyanos) u otro software malicioso.
- Realizar actividades delictivas.
- Envío de mensajes no solicitados (spam).
- Atentar contra la disponibilidad, integridad, confidencialidad del servicio.
- Cualquier conducta que viole las normas aceptadas dentro de la comunidad de Internet, esté o no detallada en estas políticas de uso aceptable.
- Manipular o intentar manipular cualquier componente de la infraestructura de red.



NESTOR BONILLA RAMIREZ
Representante Legal

CONTROL DE CAMBIOS		
La trazabilidad de los cambios generados en el documento podrá ser consultada en el Listado Maestro de Documentos.		
Versión	**Descripción Del Cambio**	**Fecha de Aprobación**
1	Elaboración inicial del documento	08 de julio de 2022

Elaborado Por:	Revisado Por:	Aprobado Por:
SERGIO ALEJANDRO CUELLAR CARDONA **Cargo:** Analista del SIG	**CRISTIAN ANIBAL RODRIGUEZ FALLA** **Cargo:** Subgerente de TIC (e)	**NÉSTOR BONILLA RAMÍREZ** **Cargo:** Gerente General