ACUERDO No.022
(24 de junio del 2024)

Por medio del cual se modifica el **MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN** de la **COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CRÉDITO COONFIE**

EL CONSEJO DE ADMINISTRACIÓN DE LA COOPERATIVA NACIONAL EDUCATIVADE AHORRO Y CRÉDITO "COONFIE", EN USO DE LAS FACULTADES LEGALES Y ESTATUTARIAS

CONSIDERANDO:

1. Que el artículo 120 del Estatuto vigente, establece que el Consejo de Administración debe determinar políticas particulares de la Cooperativa.

2. Ley 1273 de 5 de enero 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".

3. Anexo 2 - INSTRUCCIONES SOBRE SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS de la Circular externa 036 de la superintendencia de economía solidaria.

4. Que es un compromiso de la dirección aprobar el manual de gestión de seguridad de la información y controlar el cumplimiento estricto de las políticas aquí establecidas.

5. Que es responsabilidad del Consejo de Administración garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

ACUERDA:

ARTÍCULO 1: Poner en vigencia el presente MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN para el desarrollo de la operación completa operativa, rigiéndose por las siguientes políticas.

TABLA DE CONTENIDO

1 INTRODUCCIÓN

En la Cooperativa Nacional Educativa de Ahorro y Crédito COONFIE la seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de la confidencialidad, la integridad y disponibilidad de los activos, donde sólo pueden ser accedidos y custodiados por funcionarios autorizados; garantizando el contenido y los métodos de proceso.

En este documento se describen los controles implantados, tales como políticas, prácticas, procedimientos y funciones del software; definidos por la Cooperativa. Apoyando la realización del manual a través de la Norma ISO/IEC 27001:2022 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad – Sistemas de gestión de la seguridad de la información, la Ley Estatuaria 1266 de 2008 por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente deterceros países y se dictan otras disposiciones; y la Ley 1581 de 2012 donde se dictan disposiciones para la protección de datos personales.

2 OBJETIVO

Establecer las políticas de seguridad de la información con el fin de definir lineamientos claros para el personal de Coonfie que permitan controlar y mitigar los riesgos asociados alacceso y uso de la información incluidos los datos personales.

3 ALCANCE

El presente Manual tiene como propósito definir los lineamientos y las políticas concernientes al aseguramiento de la información que recolecta, almacena y trata COONFIE dentro del desarrollo de su actividad económica, estableciendo los parámetros mínimos de actuación a nivel técnico, administrativo y humano que permitan alcanzar niveles óptimos de confidencialidad, integridad y disponibilidad de la información.

4 APLICABILIDAD

Las políticas del SGSI aplican y son de obligatorio cumplimiento para el Consejo de Administración, la Gerencia general, Subgerentes, directores de Oficina, funcionarios, contratistas, y en general a todos los usuarios que tengan acceso a la información tratada por la cooperativa.

5 TÉRMINOS Y DEFINICIONES

- **Acción Correctiva:** Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.

- **Acción Preventiva:** Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

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

- **Aceptación del riesgo:** Decisión de asumir un riesgo.

- **Activo de información:** Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que tiene algún valor para la Cooperativa y, en consecuencia, debe ser protegido.

- **Acuerdo de Confidencialidad**: Documento en el que el personal de la Cooperativa COONFIE o los provistos por terceras partes acuerdan mantener bajo confidencialidad la información que se trate en virtud del vínculo contractual, comprometiéndose a no divulgar, usar o explotar la información para fines distintosa los acordados.

- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede generar el daño a un sistema o la organización.

- **Análisis de riesgos:** uso sistemático de la información para identificar las fuentes y estimar el riesgo.

- **Antivirus:** Programa que protege sistemas informáticos finales de software malicioso contenidos en cualquier tipo de almacenamiento, tráfico de red entrante ysaliente de dicho sistema.

- **Áreas propietarias:** área encargada de adquirir y desarrollar los sistemas de información dentro de la Cooperativa.

- **Autenticación:** procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un sistema de información.

- **Backup:** Es una copia de seguridad de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida de la fuente original.

- **Base de datos:** Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

- **Capacity Planning:** Proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita COONFIE para satisfacer las necesidades de procesamiento de dichos recursos.

- **Centros de cableado**: Es un sistema colectivo compuesto de cables, canalizaciones, etiquetas, espacios, conectores y otros dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio.

- **Centro de cómputo:** Instalación dentro de una edificación que alberga los componentes físicos que soportan los sistemas de información, telecomunicacionesy almacenamiento que componen la mayoría de la infraestructura del procesamiento de datos de una empresa.

- **Cifrado:** Es un procedimiento que transforma los datos a fin de hacerlos ininteligibles usando un algoritmo matemático, pero sin alterar los datos originales,se requiere una clave o palabra secreta para su lectura y/o uso.

- **Confidencialidad:** Propiedad que determina que la información no esté disponibleni sea revelada a individuos, entidades o procesos no autorizados.

- **Control:** Toda actividad o proceso encaminado a mitigar o evitar un riesgo.

- **Criptografía:** Disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación y su uso no autorizado.

- **Disponibilidad:** Pilar de la seguridad de la información que provee la característica a la información de 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.

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

- **Equipo de cómputo:** Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

- **Evaluación del Riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar el impacto del riesgo.

- **Evento de seguridad de la información:** Presencia identificada de una condiciónde un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

- **Hacking ético**: Conjunto de actividades para ingresar a las redes de datos y voz dela Cooperativa, con el objeto de lograr un alto grado de penetración, de forma controlada, teniendo como propósito mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

- **Hardware:** Se refiere a las características técnicas y físicas de los equipos.

- **Incidente de Seguridad:** Un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad:** Protección de la exactitud y estado completo de los activos.

- **IP:** Etiqueta numérica que identifica de manera lógica y jerárquica a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente un computador) dentro de una red que utilice el protocolo IP.

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

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

- **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.

- **Perfiles de usuario:** Conjunto de características que identifican los permisos de un usuario sobre un aplicativo, sobre una red o archivos físicos organizados y clasificados. En ambientes corporativos los conjuntos de permisos deben estar basados en las funciones de los diferentes cargos.

- **Recursos tecnológicos:** Son aquellos componentes de hardware y software tales como: servidores, estaciones de trabajo, equipos portátiles, dispositivos de

comunicaciones y de seguridad, servicios de red y bases de datos, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de COONFIE.

- **Registros de Auditoría:** Es un compendio de eventos organizados de forma cronológica de los recursos tecnológicos, que muestran de forma detallada el comportamiento de dichos recursos y pueden ser consultados de forma periódica con el fin de identificar anomalías y/o comportamientos que requieran de revisión.
  Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la Cooperativa.

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

- **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

- **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.

- **Servidores:** Equipo con capacidades destacables (software y hardware) que provee diferentes servicios a una red de computadores. computador que respondepeticiones o comandos de un computador cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidores el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

- **Sistema de información:** Es un conjunto de datos que interactúan entre si con unfin común. Ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos de la cooperativa. Es un conjuntoorganizado de datos, operaciones y transacciones interrelacionadas que permiten el almacenamiento y procesamiento de la información en la Cooperativa.

- **Sistema de control ambiental:** Conjunto de inspecciones, vigilancia y aplicación de las medidas legales y técnicas que se aplican y son necesarias para disminuir oevitar cualquier tipo de afección al medio ambiente.

- **Software:** Soporte lógico de un sistema informático, que comprende el conjunto delos componentes lógicos necesarios que hacen posible la realización de tareas

específicas, mediante la gestión y administración del hardware. programas y documentación de respaldo que permite y facilita el uso del pc. El software controlala operación del hardware.

- **Software malicioso:** Es una variedad de software o programas de códigos hostilese intrusivos que tiene como objeto infiltrase o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

- **Tratamiento del riesgo**: Proceso de selección e implementación de medidas para mitigar el riesgo.

- **Terceros:** Todas las personas, jurídicas o naturales, como proveedores,contratistas o consultores, que provean servicios o productos a la Cooperativa.

- **Usuario:** funcionario que utiliza cualquiera de los recursos tecnológicos de la cooperativa y realiza múltiples tareas con ellos.

- **Usuario externo:** Tercero que utiliza cualquiera de los recursos tecnológicos de la cooperativa y realiza múltiples tareas con ellos.

- **Usuarios registrados:** Son aquellos usuarios que han sido identificados y almacenados en un algún tipo de registro, con el fin de conceder permisos especiales y/o accesos a diferentes sitios o plataformas.

- **Valoración del riesgo:** Proceso global de análisis y evaluación del riesgo.

- **Vulnerabilidades:** Son las debilidades, brechas de seguridad inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Cooperativa (amenazas), las cuales se constituyen en fuentes de riesgo.

6 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 TIC, 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 TIC, 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.

6.1 CONSEJO DE ADMINISTRACIÓN

- Definir y promover la dirección estratégica para la seguridad de la información.
- Proporcionar los recursos para la adecuada implementación de la seguridad de la información.
- Proporcionar, velar y apoyar la implementación y asignación del Sistema de Seguridad de Información.
- Autorizar, facilitar e integrar la puesta en operación del sistema de seguridad de la información, mediante la definición de mecanismos y la supervisión e integración por parte de cada líder de proceso.
- Velar por el cumplimiento de las obligaciones regulatorias en materia de seguridad de la información.
- Velar por la disponibilidad de los recursos y su uso apropiado.
- Designar los responsables de la implementación del sistema de seguridad de la información.

- Pronunciarse y hacer seguimiento a los informes trimestrales que presente el representante legal, dejando constancia en las actas de las reuniones respectivas.

- Revisar los niveles tolerables de los riesgos asociados a la seguridad de la información, procurando que permanezcan dentro de los niveles tolerados por la cooperativa.

- Revisar que la estrategia de seguridad de la información se encuentre alineada con los objetivos de negocio.

- Revisar y aprobar las actualizaciones al Sistema de Gestión de Seguridad de la Información (SGSI), para garantizar su continua conveniencia, idoneidad y efectividad.

- Establecer las prioridades de los proyectos e iniciativas relacionadas con la seguridad de la información.

6.2 GERENCIA GENERAL

- Velar por el desarrollo de los objetivos estratégicos para la seguridad de la información, definidos por el consejo de administración.

- Velar por la implementación de la política de seguridad de la información.

- Facilitar la integración entre los diferentes dueños de procesos de negocio para lograr la implementación del modelo de seguridad de la información.

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

- Velar por la correcta aplicación de los controles de seguridad para reducir el riesgo de seguridad de la información.

- Velar por la designación de los responsables de la implementación de la política de seguridad de la información.

- Presentar un informe periódico, como mínimo trimestral, al Consejo de Administración sobre la evolución y aspectos relevantes de la seguridad de la información incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar, seguimiento y resultados de mediciones y cumplimiento de objetivos de seguridad de la información.

6.3 OFICIAL DE SEGURIDAD DE LA INFORMACION

- Definir los objetivos estratégicos para la seguridad de la información.
- Velar por la implementación de la política de seguridad de la información.
- Facilitar la integración entre los diferentes dueños de procesos de negocio para lograr la implementación del modelo de seguridad de la información.
- Velar por la disponibilidad de los recursos y uso apropiado.
- Velar por la correcta aplicación de los controles de seguridad para reducir el riesgo de seguridad de la información.
- Presentar un informe periódico, como mínimo trimestral, al Consejo de Administración y a la Gerencia General sobre la evolución y aspectos relevantes de la seguridad de la información incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar, seguimientos y resultados de mediciones y cumplimiento de objetivos de seguridad de la información.
- Definir y promover la dirección estratégica para la seguridad de la información.
- Proporcionar, velar y apoya la implementación y asignación del Sistema de Seguridad de la Información.
- Supervisar el cumplimiento de las obligaciones regulatorias en materia de seguridad de la información.
- Realizar las evaluaciones de riesgo de seguridad de la información resultantes.
- Revisar que la estrategia de seguridad de la información se encuentre alineada con los objetivos
- Proponer las actualizaciones al Sistema de Gestión de Seguridad de la Información (SGSI), para garantizar su continua conveniencia, idoneidad y efectividad.

Establecer las prioridades de los proyectos e iniciativas relacionadas con la seguridad de la información.

6.4 CONTROL INTERNO

- Tener conocimiento apropiado en materia de seguridad de la información y de esta normativa en particular.

- Evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos clave del sistema de seguridad de la información, con el fin de determinar las deficiencias y sus posibles soluciones.

- Informar los resultados de la evaluación de la seguridad de la información al consejo de administración.

6.5 DIRECCIÓN DEL SIAR

- Tener comprensión de las amenazas, las vulnerabilidades, y el perfil de riesgo de la organización.

- Tener entendimiento de la exposición al riesgo y las posibles consecuencias para el negocio.

- Crear conciencia de las prioridades de la gestión de riesgos con base en las posibles consecuencias de materialización.

- Definir e implementar estrategias organizacionales adecuadas para la mitigación de riesgos para obtener consecuencias aceptables.

- Fijar la atención organizacional con base en un entendimiento de las posibles consecuencias del riesgo residual.

- Conservar información documentada del proceso de gestión de riesgos de seguridad de la información.

7 POLÍTICA DE SEGURIDAD DE LA INFORMACION

7.1 POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

COONFIE establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación, control y monitoreo de la seguridad de la información.

7.1.1 SUBGERENCIA ADMINISTRATIVA

- Definir y establecer los roles y responsabilidades relacionadas con la seguridad de la información en niveles administrativo y operativo.

- Velar por la infraestructura física necesaria para la gestión de la seguridad de la información de la Cooperativa.

7.1.2 COMITÉ DE SEGURIDAD DE LA INFORMACION

- Presentar ante el Consejo de Administración las Políticas de Seguridad de la Información las actualizaciones o modificaciones al sistema de gestión de la seguridad de la información.

- Analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

- Verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

- Definir protocolos de respuesta que involucren a los titulares, las autoridades administrativas y judiciales.

7.1.3 SUBGERENCIA DE TIC

- Asignar las funciones, roles y responsabilidades a sus funcionarios para la operación y administración de la plataforma tecnológica de la Cooperativa; estas deben encontrarse documentadas y apropiadamente segregadas.

- Documentar de manera suficiente, soportada y detallada cada incidente de seguridad que se presente con el fin de identificar si COONFIE actuó con la debida diligencia, así como las medias correctivas que permitan evitar eventos futuros, y demostrar el cumplimiento de los lineamientos legales en materia de protección de datos personales en el evento de una investigaciónpor parte del organismo de control.

- Efectuar la revisión permanente de las medidas de seguridad adoptadas para mitigar los riesgos asociados al tratamiento de la información e implementar revisiones constantes con el fin de adoptar nuevas medidas que permitan prevenir la pérdida de la información, adulteración de la información, o el acceso no autorizado o fraudulento.

- Deberá definir un presupuesto anual que contemple la criticidad de los activos de información involucrados, y los recursos que aseguren la función de seguridad de la información, herramientas tecnológicas que apoyen a la protección de los activos de información y el proceso de mejora continua.

7.1.4 TODOS LOS FUNCIONARIOS

- Cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

8 POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

COONFIE establecerá las condiciones para el manejo de los dispositivos móviles (teléfonos inteligentes, tabletas, entre otros) institucionales y personales que hagan uso de servicios de la Cooperativa. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por COONFIE.

8.1 SUBGERENCIA DE TIC

- Investigar y probar las opciones de protección de los dispositivos móviles institucionales que hagan uso de los servicios provistos por la Cooperativa.

- Establecer las configuraciones aceptables para los dispositivos móviles institucionales que hagan uso de los servicios provistos por COONFIE.

- Establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

- Activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivosy restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

- Contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales de COONFIE, dichas copias deben acogerse a la Política de copias de respaldo de la información.

- Instalar un software de antivirus tanto en los dispositivos móviles institucionales, como en los personales que hagan uso de los servicios provistos por la Cooperativa.

- Activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

8.2 FUNCIONARIOS CON DISPOSITIVOS MÓVILES INSTITUCIONALES

- Solo los cargos autorizados, dotados de teléfonos móviles institucionales y de una línea de celular empresarial pueden acceder a la información y los recursos tecnológicos de la Cooperativa desde estos dispositivos, estos cargos son:

  - Gerente general.
  - Subgerentes
  - Directores de oficina.
  - Administrador base de datos.
  - Asistente de consejo de administración.
  - Asistente de gerencia general.
  - Asistente de Sistemas 4.
  - Analista social media.
  - Analista mercadeo.
  - Mensajero.
  - Auxiliar de archivo.

- Evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

- Evitar modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

- Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

- Cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

- Evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, bluetooth o infrarrojos en los dispositivos móviles

institucionales asignados.

- Evitar conectar los dispositivos móviles institucionales asignados por puertos USB a cualquier computador público de hoteles o cafés internet, entre otros.

- No almacenar en ellos fotografías, videos o información personal. Su uso deber ser exclusivo con fines laborales.

8.3 FUNCIONARIOS CON DISPOSITIVOS MÓVILES PERSONALES

- Está permitido su uso solo cuando se requiera como medida adicional de seguridad para el inicio de la sesión del correo electrónico empresarial. Procurar hacer uso responsable del dispositivo teniendo en cuenta que una vez habilitada esta característica, cualquier vulnerabilidad en este dispositivo podría ocasionar un incidente de seguridad sobre el correo electrónico empresarial.

9 POLÍTICA DE SEGURIDAD PARA LOS RECURSOS HUMANOS

9.1 VINCULACIÓN DE FUNCIONARIOS

COONFIE reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que el acceso a la información de los nuevos funcionarios se realizará siguiendo un proceso orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

9.2 NORMAS RELACIONADAS CON LA VINCULACIÓN DE FUNCIONARIOS

La subgerencia Administrativa debe de realizar la verificación necesaria para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en COONFIE, antes de su vinculación definitiva.

Se debe asegurar que los funcionarios y demás colaboradores de COONFIE asuman sus responsabilidades en relación con las políticas de seguridad de lainformación y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de las normas que reglamenten los

procesos disciplinarios para los funcionarios.

Actualmente los usuarios que tienen cuenta de usuario de COONFIE, pueden realizar el cambio de su fotografía para correo electrónico institucional, de tal forma que al realizar la inclusión y/o cambio de fotografía, al ser considerada un dato sensible, "una foto contiene la imagen de una persona, la cual es un dato biométrico", el titular está dando su aprobación, en cuanto al tratamiento de sus datos personales de acuerdo a la Ley Estatutaria 1581 de 2012 ya que es el funcionario mismo quien ejecuta la acción, lo cual se interpreta como un acto inequívoco.

La Subgerencia Administrativa debe certificar que los funcionarios de la Cooperativa firman un Acuerdo y/o Clausula de Confiabilidad y un documento de Aceptación de Políticas de Seguridad de Información; estos documentos deben de ser anexados a los demás documentos relacionados con la ocupacióndel cargo.

COONFIE implementa acciones para asegurar que los funcionarios y demás colaboradores de COONFIE, entiendan sus responsabilidades como usuarios y responsabilidad de los roles asignados, con el fin de reducir el riesgo de hurto,fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

9.3 DURANTE LA VINCULACIÓN DE FUNCIONARIOS Y PERSONAL

COONFIE en su interés por proteger su información y los recursos de procesamiento de esta demostrará el compromiso de la Alta Gerencia en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información mediante capacitaciones regulares para que el funcionario de una correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticasde seguridad de la información de la cooperativa.

Todos los funcionarios de COONFIE deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de COONFIE.

9.4 DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORESDE LOS FUNCIONARIOS Y PERSONAL.

COONFIE asegura que sus funcionarios serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

Cada director de oficina debe de reportar a la Subgerencia Administrativa el cambio de labores de los funcionarios o del personal previsto, a su vez la Subgerencia Administrativa envía la notificación a la Subgerencia de TIC con copia a la dirección del SIAR para su conocimiento y para que se ejecute los cambios necesarios.

9.5 NORMA PARA LA DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIOS DE LABORES DE LOS FUNCIONARIOS Y PERSONAL.

9.5.1 SUBGERENCIA ADMINISTRATIVA:

La Subgerencia Administrativa debe de realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios de la Cooperativa llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin. Notificar a la Subgerencia de TIC mediante el procedimiento **PR-AD-11** CREAR MODIFICAR O INACTIVAR USUARIOS Y PERMISOS EN EL SISTEMA.

9.5.2 DIRECCIÓN DEL SIAR:

La Dirección del SIAR debe de verificar los reportes de desvinculación o cambios de labores.

10 POLÍTICA DE GESTION DE ACTIVOS DE INFORMACION

COONFIE como propietario de la información física, así como de la información generada, procesada, almacenada y trasmitida con su plataforma tecnológica, otorga responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen adecuadamente la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. Estaciones de trabajo, equipos portátiles, impresoras, redes, internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y entre otros,) propiedad de COONFIE, son activos de la cooperativa y se proporciona a los funcionarios y terceros autorizados, para cumplir con los propósitos de COONFIE.

Toda la información de COONFIE, así como de sus activos donde se almacena y se procesa, deben ser asignados a un responsable, inventariada y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Dirección del SIAR.

11 POLÍTICA DE USO DE LOS ACTIVOS

La Cooperativa implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios que deban administrarlos de acuerdo con sus roles y funciones.

11.1 INVENTARIO DE ACTIVOS

La identificación del inventario de activos de información permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

Las actividades por realizar para obtener un inventario de activos son Definición, Revisión, Actualización y Publicación, las cuales se reflejan documentalmente en la Matriz de Inventario y Clasificación de Activos de Información.

Figura 1. Procedimiento Para Inventario de Activos de Información.

11.2 DEFINICIÓN

La definición consiste en determinar qué activos de información van a hacer parte del inventario, para esta tarea debe existir un equipo que realice la gestiónde activos de información al interior de COONFIE y por medio del líder de cada áea ayude en realización de la actividad. En segunda instancia los líderes de procesos deben, solicitar la revisión de la definición de los activos por parte del propietario del activo de información designado, custodio y usuario de este, paraque validen si son las partes interesadas o la parte de COONFIE adecuadas para tener este rol.

Es recomendable que la definición del inventario se lleve a cabo por lo menos una vez al año.

11.3 REVISIÓN

La actividad de revisión se refiere a la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario,o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

- Las razones por las cuales debería realizarse una revisión o validación son:
- Actualizaciones al proceso al que pertenece el activo.
- Adición de actividades al proceso.
- Inclusión de nuevos registros de calidad, nuevos registros de referencia y procesos y procedimientos.
- Inclusión de un nuevo activo.
- Desaparición de un área, proceso o cargo en COONFIE que tenía asignado el rol de propietario o custodio (Cambios Organizacionales).
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
- Cambios físicos de la ubicación de activos de información.

11.4 ACTUALIZACIÓN

Una vez se ha definido qué cambios se realizarían en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información.

11.5 PUBLICACIÓN

El inventario de activos de información debe ser un documento clasificado como“Confidencial”, y no debe tener características que lo permitan modificar por losusuarios no autorizados. Sólo debe tener acceso de modificación a este documento el líder del proceso con previa autorización del oficial de seguridadde la información o quien hagas sus veces.

12 POLÍTICA DE USO DE ESTACIONES CLIENTES

En COONFIE se establecen reglas orientadas a que la seguridad sea parte integral de los activos de información mediante la correcta utilización de equipos por los funcionarios.

- Los funcionarios que hagan uso de equipos institucionales en préstamo NO deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso.

- Los equipos de cómputo u otro recurso tecnológico que no se esté usando o que no esté desempeñando una función específica, sino que por el contrario se encuentren guardados o inactivos, deben ser devueltos a la subgerencia TIC para su debido almacenamiento y control. Si el recurso se requiere, pero su uso no es frecuente, en el caso de computadores de escritorio y portátiles estos deben ser prendidos y conectados a la red por lo menos cada 3 días.

- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter corporativo.

- En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario, la persona que haga uso de los equipos deberá abstenerse de realizar modificaciones a estos archivos.

- Para préstamo de equipos de cómputo y portátiles, el líder de área debe solicitarlo a través del mecanismo diseñado para tal fin y debe hacerse por lo menos con 3 días de antelación, tiempo en el cual se acondicionará el equipo para su correcto funcionamiento. El préstamo del equipo solo quedará registrado/asignado a nombre del funcionario que sea de planta; de lo contrario será registrador/asignado a nombre de su líder de área en los diferentes sistemas de información y se entregará mediante acta.

- No está permitido retirar de las instalaciones los recursos tecnológicos de la cooperativa, solo los cargos de nivel directivo se tienen permitido el traslado de estos según se requiera para el desarrollo de las funciones propias del cargo.

- Para los casos especiales donde se requiera que algún funcionario retire algún recurso tecnológico de la cooperativa de las instalaciones la solicitud deberá ser analizada y estudiada por la coordinación de SGSI e infraestructura y aprobada por la subgerencia TIC y la subgerencia administrativa; se debe llevar un registro de todas las solicitudes junto con las aprobaciones.

- En ningún caso se permitirá a los cargos temporales (contratos a término fijo y de aprendizaje) el retiro de cualquiera de los recursos tecnológicos de las instalaciones de la cooperativa.

- Los equipos que ingresan temporalmente a COONFIE que son de propiedad de terceros deben seguir el procedimiento diseñado para otorgar el permiso necesario. Sin embargo, se especifica que la Cooperativa no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o corporativos de terceros que hayan sido ingresado a sus instalaciones.

- La subgerencia de TIC no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de la Cooperativa.

12.1 SUBGERENCIA TIC

- Proveer los mecanismos tecnológicos necesarios para el cumplimiento de los diferentes lineamientos descritos en esta política.
- Analizar, estudiar y aprobar las solicitudes de retiro de recursos tecnológicos de las instalaciones de la cooperativa.

12.2 SUBGERENCIA ADMINISTRATIVA

- Aprobar las solicitudes de retiro de recursos tecnológicos de la cooperativa previa socialización del análisis y el estudio realizado por la subgerencia TIC.

12.3 FUNCIONARIOS

- Reportar oportunamente las novedades con los recursos tecnológicos de su manejo de manera oportuna haciendo uso de los procedimientos y registros diseñados para tal fin.
- Cumplir a cabalidad con los lineamientos descritos en la presente política.

13 POLÍTICA DE USO DE INTERNET

COONFIE permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado por parte de los funcionarios, evitando errores, perdidas, modificaciones no autorizadas o uso inadecuado de la información no autorizada o uso inadecuado de la información en las aplicaciones WEB.

La Subgerencia de TIC implementará herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento en el internetpara prevenir la fuga de información.

No se permite la navegación a sitios con contenidos contrarios a la ley o que representen peligro para COONFIE como: pornografía, terrorismo, hacktivismo, segregación racial u

otras fuentes definidas.

La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio.

14 POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACION

COONFIE definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los funcionarios que hacen uso de ella la cataloguen y determinen los controles requeridos para su protección; consultar el instructivo **IN-TI-11 Etiquetado de Documentos Digitales y Correo Electrónico.**

Una vez clasificada la información, COONFIE proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de esta, con el fin de promover el uso adecuado por parte de los funcionarios y personal provisto por terceras partes que se encuentre autorizado y requierade ella para la ejecución de sus actividades.

Los usuarios responsables de la información de COONFIE, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como “Valiosa” para laCooperativa; Independiente del tipo de activo.

15 POLÍTICA DE MANEJO DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS

COONFIE establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), navegadores y equipos de cómputo son

propiedad de COONFIE y deben ser usados únicamente para el cumplimiento de la misión deCOONFIE.

Se debe realizar la aplicación del procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez se vayan a almacenar en bodega en espera de ser donados o vayan a ser asignados a otro funcionario.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la dirección del SIAR y será objeto de auditorías de seguridad.

16 POLÍTICA DE CONTROL DE ACCESO

COONFIE define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática de COONFIE, considerándolas como importantes para el SGSI.

El acceso a las instalaciones que hagan uso de dispositivos de control de acceso biométrico tendrá como responsables de estos, a los líderes de área o funcionarios a cargo del lugar donde se encuentre instalado. La coordinación de protección de datos velará por el debido tratamiento de datos personales, conforme a lo dispuesto en la Ley 1581 del 2012, la cual trata del uso de datos sensibles según su clasificación.

El acceso a conexiones o puntos de red de acceso público, incluyendo accesos inalámbricos, dispositivo de telecomunicaciones, hardware de redes o comunicaciones y líneas de telecomunicaciones, serán protegidos por controles físicos, establecidos por la Subgerencia de TIC junto con la Subgerencia Administrativa.

La conexión remota a la red de área local de la cooperativa debe realizarse a través de una conexión VPN segura suministrada por COONFIE, la cual debe ser aprobada en sesión del Comité de seguridad de la Información, registrada y controlada por la Subgerencia de TIC.

17 POLÍTICA PARA USO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO

Coonfie establecerá normas y lineamientos para el uso de dispositivos de almacenamiento masivo USB (Dispositivos USB) en la cooperativa. El objetivo de esta política es proteger la información confidencial, prevenir la pérdida de datos y garantizar el buen funcionamiento de los sistemas informáticos.

- Solo se permite el uso de Dispositivos USB autorizados por la cooperativa (registrados en el formato designado).

- Los Dispositivos USB deben estar formateados según los estándares establecidos por la organización.

- No se permite la instalación de software en Dispositivos USB sin la autorización previa de la subgerencia TIC.

- Los Dispositivos USB deben estar protegidos con contraseña.

- No se permite el uso de Dispositivos USB para almacenar información personal o ajena a la cooperativa y/o que no esté relacionada con las responsabilidades/funciones del funcionario.

- Los Dispositivos USB deben escanearse con la herramienta antimalware de la cooperativa antes de hacer uso de ellos.

- Los Dispositivos USB perdidos o robados deben reportarse inmediatamente a la Subgerencia TIC informando su contenido.

17.1 FUNCIONARIOS CON DISPOSITIVOS DE ALMACENAMIENTO MASIVO

Solo los cargos autorizados, dotados de al menos un dispositivo de almacenamiento masivo (USB) empresarial, lo pueden usar como recurso tecnológico seguro de la Cooperativa, estos cargos son:

- Subgerente Financiero.
- Contador general.
- Director SIAR.
- Coordinador SGSI e Infraestructura.
- Asistente de consejo de administración.
- Asistente de Sistemas 4.
- Asistente de Nomina y Convenios
- Asesor de infraestructura.

Para situaciones no descritas en la política, deberán ser analizadas y evaluadas por la coordinación SGSI e infraestructura previa solicitud radicada por la mesa de ayuda.

- Evitar usar/conectar los dispositivos de almacenamiento masivo (USB) corporativos en equipos que no ofrezcan las medidas mínimas de seguridad para evitar infecciones por malware o perdidas de información.

17.2 SUBGERENCIA TIC

- Proveer los mecanismos tecnológicos necesarios para el cumplimiento de los diferentes lineamientos descritos en esta política.

- Documentar, administrar, controlar y mantener actualizado el inventario de dispositivos de almacenamiento masivo (USB) corporativos.

- Revisar y analizar detalladamente las solicitudes sobre la incorporación de nuevos dispositivos y/o cargos permitidos para el uso de este tipo de recursos. Brindar mecanismos alternativos más seguros.

17.3 DIRECCIÓN DEL SIAR

- Revisar de manera conjunta con la coordinación de SGSI e Infraestructura las solicitudes previamente analizadas y viabilizadas para emitir la recomendación y observaciones con respecto a los riesgos asociados al uso de estos dispositivos en los cargos solicitantes.

17.4 COORDINACIÓN PROTECCION DE DATOS

- Reportar ante los entes de control las pérdidas de información relacionadas con el extravío y/o robo de cualquiera de los dispositivos de almacenamiento masivo (USB) corporativos.

17.5 FUNCIONARIOS

- Reportar la pérdida o robo de un dispositivo de almacenamiento masivo a la subgerencia TIC.

- Hacer uso adecuado de este tipo de recursos tecnológicos que, aunque facilitan ciertas funciones, estos representan un riesgo importante para la información de la cooperativa que en ellas se contenga.

- Cumplir a cabalidad con los lineamientos descritos en la presente política.

18. POLÍTICA PARA EL USO DE SOFTWARE DE ACCESO REMOTO

Coonfie establece las normas y lineamientos para el uso de software de acceso remoto (SAR) en la cooperativa. El objetivo de esta política es proteger la información confidencial, prevenir la pérdida de datos y garantizar el buen funcionamiento de los recursos tecnológicos que permiten este tipo de conexiones.

- Cuando se requiera otorgar por parte de la Cooperativa un acceso remoto a algún tercero o proveedor por cuenta de alguna asesoría o soporte se permitirá el uso de SAR que ese tercero o proveedor utilice si y solo si cumple con los lineamientos aquí descritos, de lo contrario solo estará permitido el adquirido por la Cooperativa.

- Registrar la solicitud a través del formato dispuesto para este fin.

- El SAR debe tener licencia de pago, no se permiten licencias no-comerciales, hogar y/o gratuitas.

- El SAR debe estar configurado con las medidas de seguridad adecuadas, como autenticación de dos factores y cifrado de datos.

- No se permite el uso de SAR para acceder a sistemas informáticos que no estén autorizados.

- Las sesiones de acceso remoto deben estar registradas y auditadas (Logs y grabación de la sesión.)

- Los usuarios deben desconectarse del SAR cuando no lo estén utilizando.

- No se permite el uso de SAR para instalar software en los equipos remotos accedidos sin la autorización previa de la coordinación de SGSI e Infraestructura.

- Los usuarios deben reportar inmediatamente cualquier incidente de seguridad relacionado con el SAR a la coordinación de SGSI e Infraestructura siguiendo el procedimiento destinado para este fin.

18.1 SUBGERENCIA TIC

- Proveer los mecanismos tecnológicos necesarios para el cumplimiento de los diferentes lineamientos descritos en esta política.

18.2 DIRECCIÓN DEL SIAR

- Revisar de manera conjunta con la coordinación de SGSI e Infraestructura las solicitudes previamente analizadas y viabilizadas para emitir la recomendación y observaciones con respecto a los riesgos asociados al uso de este tipo de software según los cargos solicitantes.

18.3 FUNCIONARIOS

Realizar la solicitud mediante el formato definido para este fin con el objetivo de identificar la necesidad y pertinencia y reportar cualquier incidente de seguridad relacionado con el SAR a la subgerencia TIC siguiendo los procedimientos diseñados para tal fin.

19. POLÍTICA DE ESTABLECIMIENTO, USO Y PROTECCIÓN DE CLAVES DE ACCESO.

COONFIE establecerá privilegios para el control de acceso lógico de cada funcionario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Cooperativa. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté reguladapor normas y procedimientos establecidos para tal fin.

19.1 ADMINISTRACIÓN DE ACCESO DE USUARIOS

19.1.1 SUBGERENCIA DE TIC

- En COONFIE el procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la Cooperativa, que contemple la creación, modificación o eliminación de las cuentas de usuario es el **PR-AD-11** CREAR MODIFICAR O INACTIVAR USUARIOS Y PERMISOS EN EL SISTEMA.

- La Subgerencia de TIC, previa solicitud de los jefes inmediatos de los solicitantes de las cuentas de usuario y aprobación tanto de los propietarios de los sistemas de

información como la Dirección del SIAR, debe crear, modificar o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde al procedimiento **PR-AD-11** CREAR MODIFICAR O INACTIVAR USUARIOSY PERMISOS EN EL SISTEMA.

- La Subgerencia de TIC, en conjunto con la subgerencia de SIAR, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de COONFIE; dichas contraseñas son personalizadas y están definidas en el presente acuerdo.

- Cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo, se asegura la modificación o eliminación de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, llevando a cabo el procedimiento **PR-AD-11** CREAR MODIFICAR O INACTIVAR USUARIOS Y PERMISOS EN EL SISTEMA.

19.1.2 SUBGERENCIA ADMINISTRATIVA Y DIRECCIÓN DEL SIAR

- Es responsable de definir los perfiles de usuario y autorizar, las solicitudes de acceso a dichos recursos.

- Verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

19.1.3 SUBGERENTES Y DIRECTORES DE OFICINA

- Solicitar la creación, modificación y eliminación de cuentas de usuario, para los funcionarios que laboran en sus áreas, acogiéndose al procedimiento **PR-AD-11** CREAR MODIFICAR O INACTIVAR USUARIOS Y PERMISOS EN EL SISTEMA establecido para tal fin.

19.2 RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información de COONFIE realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

19.2.1 TODOS LOS FUNCIONARIOS

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de COONFIE, deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

- Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.

- Los funcionarios y personal provisto por terceras partes que posean accesoa la plataforma tecnológica, los servicios de red y los sistemas de información de la Cooperativa deben acogerse a lineamientos para la configuración de contraseñas implantados por la Cooperativa.

19.3 USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACIÓN

19.3.1 SUBGERENCIA DE TIC

- La Subgerencia de TIC debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.

- La Subgerencia de TIC debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.

- La Subgerencia de TIC debe asegurarse que los usuarios o perfiles deusuario que traen por defecto los sistemas operativos, firmwares y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto sean modificadas.

- La Subgerencia de TIC debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

- Los administradores de los recursos tecnológicos y servicios de red, funcionarios de la Subgerencia de TIC, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmwares o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica de COONFIE.

- Los administradores de los recursos tecnológicos deben deshabilitar las funcionalidades, servicios o utilitarios no utilizados de los sistemas operativos, firmwares y las bases de datos. Se deben configurar el conjuntomínimo requerido.

- La Subgerencia de TIC cuenta con el listado de cuentas administrativas de los

recursos de la plataforma tecnológica, almacenados en una base de datos con todos los funcionarios activos e inactivos de la Cooperativa.

19.3.2 AUDITORIA INTERNA

- Validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a los usuarios administradores; así mismo, debe verificar que el cambio de contraseña acoja el procedimiento definido para tal fin. Las políticas se encuentran enunciadas dentro del presente acuerdo.

- Realizar seguimiento a la actividad de los usuarios con altos privilegios en los registros de la plataforma tecnológica y los sistemas de información. A nivel del Core de negocio, existe un módulo administrativo de seguridad de usuarios que permite evidenciar los datos modificados, actualizados, insertados, que realice cualquier operador en la base de datos; para COONFIE existe un log de seguimiento al cuál se le realiza un mantenimiento dinámico periódico.

19.4 CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

Las subgerencias y agencias como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

La Subgerencia de TIC, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados.

19.4.1 SUBGERENCIA DE TIC

- En COONFIE para la asignación de accesos a los sistemas y aplicativos se realiza a través de un usuario donde estos estarán definidos por las inicialesde sus nombres y apellidos; asociado con un perfil, dependiendo del horario laboral o lugar de trabajo del funcionario.

- Establecer ambientes separados a nivel físico y lógico para desarrollo,pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la

información de producción.

- Para el control de usuarios al acceso de los ambientes de producción se debe conectar por escritorio remoto con la cuenta de dominio definida para tal fin.

- Proporcionar repositorios de archivos fuente de los sistemas de información;estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

19.4.2 DESARROLLADORES (INTERNOS Y EXTERNOS)

- Asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

- En COONFIE para certificar la confiabilidad de los controles de autenticación,a nivel de COONFIE para el ingreso al aplicativo cuenta con dos (2) tipos de controles internamente:

    1. Control bajo dominio.
    2. Control para acceso de aplicación.

  Para la parte externa de COONFIE, aplica la seguridad perimetral con rangos de IP. Existen los Log de rastreo y los funcionarios tienen restricciones para el acceso (descargar música, ingreso a páginas no encaminadas a la labor que desempeña).

- Certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

- Establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso y en su lugar, generando mensajes generales de falla.

- Asegurar que no se desplieguen en la pantalla las contraseñas ingresadas. Los usuarios no deben guardar las contraseñas de acceso en ningún caso, siempre deben ser memorizadas y digitadas.

- Certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

19.4.3 CREACIÓN DE CONTRASEÑAS SEGURAS

Es responsabilidad de los funcionarios cuidar las diferentes cuentas de acceso que tienen habilitadas en la cooperativa, por medio de la creación de contraseñas seguras. Para ello es importante tener en cuenta las siguientes recomendaciones:

❖ *LO QUE **NO** DEBE HACER:*

- No utilizar solamente palabras o números — Nunca debería utilizar únicamente letras o sólo números en una contraseña.

- No utilizar palabras reconocibles — Palabras tales como nombres propios, palabras del diccionario o hasta términos de programas de televisión o novelas deberían ser evitados, aún si estos son terminados con números.

- No utilizar palabras en idiomas extranjeros — Los programas de descifrado de contraseñas a menudo verifican contra listas de palabras que abarcan diccionarios de muchos idiomas. No es seguro confiarse en un idiomaextranjero para asegurar una contraseña.

- No utilizar información personal — Mantenerse alejado de la información personal. Si un atacante conoce quién es usted, la tarea de deducir su contraseña será aún más fácil. La lista siguiente muestra los tipos deinformación que debería evitar cuando esté creando una contraseña:
- **No invertir palabras reconocibles** — Los buenos verificadores decontraseñas siempre invierten las palabras comunes, por tanto, invertir una mala contraseña no la hace para nada más segura.

- **No escribir su contraseña** — Nunca guarde su contraseña en un papel. Es mucho más seguro memorizarla.

- **No utilizar la misma contraseña para todos los servicios** — Es importante tener contraseñas separadas para cada servicio. De esta forma, si uno es comprometido, no todos estarán en peligro de ser vulnerados.

❖ *LO QUE **SI** SE DEBE HACER:*

- Crear contraseñas de al menos ocho caracteres — Mientras más larga sea la contraseña, mejor, todo depende de las longitudes permitidas en los diferentes servicios.

- Mezclar letras mayúsculas y minúsculas — Todos los sistemas y servicios son sensitivos a las mayúsculas y minúsculas, por la tanto mezcle las letraspara reforzar

la contraseña.

- Mezclar letras y números — Agregando números a las contraseñas, especialmente cuando se añaden en el medio (no solamente al comienzo o al final), puede mejorar la fortaleza de su contraseña.

- Incluir caracteres no alfanuméricos — Los caracteres especiales tales como &, $, y > pueden mejorar considerablemente su contraseña.

- Seleccionar una contraseña que pueda recordar — La mejor contraseña en el mundo será de poca utilidad si usted no puede recordarla. Por lo tanto, utilice acrónimos u otros métodos que lo ayuden a memorizar las contraseñas.

19.5 REQUERIMIENTOS MÍNIMOS DE COMPLEJIDAD PARA LAS CONTRASEÑAS DE DOMINIO (PRIMERA CLAVE)

- No contener el nombre de usuario (“JAPG - JperezG”) o partes del nombre completo del nombre de usuario (“JUAN ANDRES PEREZ GOMEZ”) que excedan dos caracteres consecutivos.

- Debe tener una longitud mínima de 14 caracteres.

- Letras en mayúsculas (A – Z)

- Letras en minúsculas (a – z)

- Números (0 - 9)

- Caracteres no alfanuméricos (por ejemplo ¡, #, $, %)

19.5.1 PARÁMETROS DE CONTRASEÑA DE DOMINIO (PRIMERA CLAVE)

- Se guardan las últimas 24 contraseñas; estas no pueden ser usadas de nuevo hasta que salgan del historial.

- El tiempo de vida de la contraseña es de treinta (60) días; el sistema bloqueará la cuenta si no se ha realizado el cambio antes de que esta expire.

- El tiempo mínimo de vida de la contraseña es de dos (2) días; pasados los dos días, el usuario cuenta con los veintiocho (28) días restantes para cambiar la contraseña.

- Se dispone de cinco (5) intentos fallidos de inicio de sesión, antes de que sebloque la cuenta. Si este número es superado debe esperar por treinta (30) minutos para volver a intentar un nuevo inicio de sesión o puede hacer la solicitud mediante una mesa de ayuda.

- El contador de intentos fallidos se reiniciará cada 30 minutos.

Nota: *todos los usuarios deben cambiar su contraseña antes de que expire; con este fin elsistema les informa cinco días antes, el día anterior y el mismo día de la caducidad de la contraseña.*

19.6 REQUERIMIENTOS MÍNIMOS DE COMPLEJIDAD PARA LAS CONTRASEÑASDEL INTEGRADOR (SEGUNDA CLAVE)

- Debe tener una longitud mínima de 8 caracteres.

- Debe contener letras.

- Debe contener números.

- Debe contener caracteres especiales.

19.6.1 PARÁMETROS DE CONTRASEÑA DE INTEGRADOR (SEGUNDA CLAVE)

- El tiempo de vida de la contraseña es de 15 días, después el sistema solicitará cambio.

Nota: *Se dispone de cinco (5) intentos fallidos de inicio de sesión, antes de que se bloquela cuenta. Si este número es superado debe hacer la solicitud de desbloqueo, mediante unamesa de ayuda.*

20 POLÍTICA DE USO DE DISCOS DE RED O CARPETAS VIRTUALES

La Subgerencia de TIC asegura la operación correcta y segura de los discos de red o carpetas virtuales.

la persona responsable o el jefe inmediato del usuario de la carpeta virtual para el caso de la herramienta OneDrive podrá otorgar acceso y permiso a la información allí contenida correspondientes al rol y funciones a desempeñar y le notificará al usuario vía correo electrónico los accesos concedidos.

Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de la solicitud, a las funciones y el rol asignado.

La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.

Está prohibido almacenar archivos que incumplan leyes de derechos de autor, información no relacionada con las funciones asignadas al usuario, información personal calificada como sensible de acuerdo con la ley 1581 de 2012, información de naturaleza privada del usuario.
Archivos que puedan ocasionar o constituir riesgos informáticos, como Software descargado de sitios extraños o sitios de dudosa procedencia estos pueden estar infectados con códigos maliciosos.

Se prohíbe el uso, extracción, divulgación o publicación de la información de cualquier medio que la aloje como discos de red, estaciones de trabajo, carpetas compartidas y sistemas de información sin autorización de su jefe inmediato y la Dirección del SIAR.

21 POLÍTICA DE USO DE REDES DE DATOS (RED DE AREA LOCAL- LAN Y RED DE AREA LOCAL SIN CABLES – WLAN).

Los usuarios deberán emplear los puntos de red y/o las redes inalámbricas, para la conexión de equipos informáticos Institucionales de la cooperativa. La instalación, activación y gestión de los puntos de red junto con las redes inalámbricas son responsabilidad de Subgerencia de TIC.

21.1 SUBGERENCIA DE TIC

- En COONFIE, para proteger el acceso a las redes de datos y los recursos de red se realizan controles a través de la IP (identifica la máquina del usuario) dependiendo del cargo que desempeña el funcionario en la Cooperativa. Para redes inalámbricas el acceso es restringido, se realiza mediante la contraseña previa firma del formato destinado para tal fin.

- La Subgerencia de TIC en conjunto con la dirección del SIAR, deben establecer controles para la identificación y autenticación de los usuarios enlas redes o recursos de red de COONFIE, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

- La Subgerencia de TIC deberá implementar redes lógicas y accesos independientes tanto para el acceso corporativo como para el acceso de invitados o visitantes.

- Todos los puntos de acceso externos que estén expuestos al público deben permanecer desconectados del panel de conexiones del rack de comunicaciones del que dependa su funcionamiento y solo cuando se vaya a poner en funcionamiento se deberá habilitar esta conexión.

21.2 DIRECCIÓN DEL SIAR

- Verificar periódicamente los controles de acceso para los usuarios, con el fin de revisar que tengan permitido únicamente aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

21.3 TODOS LOS FUNCIONARIOS

- Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de COONFIE, deben contar con el formato de autorización de uso de las redes corporativas debidamente diligenciado y autorizado junto con el Acuerdo de Confidencialidad.

  Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la Cooperativa, deben cumplir con todos los requisitos y controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

21.4 ACCESOS REMOTOS

Los funcionarios deben de contar con una autorización y con los mecanismos permitidos por la Subgerencia de TIC y aprobación del comité de seguridad de la información para realizar una conexión remota a equipos conectados a la red interna desde fuera de la misma.

21.5 CONTROLES:

- **FO-TI-13** Solicitud de ingreso o uso de equipos de cómputo de terceros en Coonfie.
- **FO-TI-14** Solicitud de conexión a red privada virtual (VPN).
- **FO-TI-18** Conocimiento y aceptación de políticas de seguridad de la información.
- **AC-TI-03** Entrega de usuarios de conexión a red privada virtual (VPN).

22 POLÍTICA DE USO DE IMPRESORAS Y DEL SERVICIO DE IMPRESIÓN

La subgerencia de TIC es la encargada de asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Los documentos que se impriman en las impresoras de COONFIE deben ser de carácter institucional.

Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la mesa de ayuda de la Subgerencia de TIC.

Los funcionarios en el momento de realizar impresiones de documentos con clasificación pública reservada o información pública clasificada (privada o semiprivada), debe mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.

23 POLÍTICA PARA EL USO DE PIN PAD Y DATAFONOS

COONFIE garantizará que el uso de los dispositivos PIN PAD Y DATAFONO se enmarque bajo los estándares de seguridad y privacidad internacionales, permitiendo así que este sea seguro para el asociado; en este sentido la lectura de las tarjetas solo se deberá hacer a través de los datafonos y los PIN PAD instalados, autorizados y administrados en las oficinas de la Cooperativa.

23.1 DIRECTORES DE OFICINA

- Delegar a uno de los cajeros la responsabilidad del uso y verificación del servicio del PIN PAD y/o Datafono.

23.2 FUNCIONARIOS

- El funcionario responsable, debe reportar la falla del servicio cuando así lo identifique por medio de la mesa de ayuda. De igual forma, estará a cargo de la entrega de los dispositivos e identificación del tercero en caso de mantenimiento previa autorización de la Subgerencia de TIC.

- El funcionario responsable debe velar porque la información confidencial de los asociados y/o usuarios no sea almacenada o retenida en el lugar en donde los equipos estén siendo utilizados reduciendo la posibilidad que terceros puedan ver

la clave digitada por el asociado o usuario.

24 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

COONFIE velará porque la información de la cooperativa sea clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

24.1 SUBGERENCIA DE TIC

Debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

Debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.

Debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado de las estaciones de trabajo de toda la cooperativa.

La Subgerencia de TIC, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

24.2 PROGRAMADORES-DESARROLLADORES (INTERNOS O EXTERNOS)

Los desarrolladores y programadores deben cifrar la información reservada o restringiday certificar la confiabilidad de los sistemas de almacenamiento de dicha información.

Los desarrolladores deben asegurarse de que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Subgerencia de TIC.

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

25 POLÍTICA DE ÁREAS SEGURAS

COONFIE proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus oficias. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

Las áreas seguras de la Cooperativa son:

- Centro de datos - Dirección General.
- Cuartos técnicos – Todas las oficinas.
- Oficina de asistentes de sistemas y coordinación de SGSI e infraestructura – Dirección General.
- Área Call center – Dirección de Cartera.

25.1 SUBGERENCIA DE TIC

- Las solicitudes de acceso al centro de cómputo, cuartos técnicos y oficina asistentes de sistemas – coordinación de SGSI e infraestructura deben ser aprobadas por el Subgerente de TIC o Coordinador SGSI e Infraestructura; los visitantes siempre deberán estar acompañados de un funcionario de la Subgerencia durante su visita al área.

- El ingreso de los visitantes al centro de datos, cuartos técnicos y oficina asistentes de sistemas – coordinación de SGSI e infraestructura, será registrado en una bitácora ubicada en la entrada de estos lugares de forma visible, se archivará en el área de Sistemas.

- Descontinuar o modificar de manera inmediata los privilegios de acceso al centro de datos, cuartos técnicos y oficina asistentes de sistemas – coordinación de SGSI e infraestructura, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

- Proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de datos; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

- Velar porque los recursos de la plataforma tecnológica de COONFIE, ubicados en el centro de datos se encuentren protegidos contra fallas o interrupcioneseléctricas.

- Certificar que el centro de datos, cuartos técnicos y oficina asistentes de sistemas – coordinación de SGSI e infraestructura se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

- Asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos, a través de un formato de registro junto con el cronograma de mantenimiento.

25.2 DIRECTORES DE OFICINAS

- Los directores deben velar, mediante monitoreo, por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en su área, autorizando cualquier ingreso temporal, evaluando la pertinencia del ingreso, delegando personal del área para que realice el registro y supervisión de la visita.

- Deberán garantizar que el área y los equipos sean dedicados exclusivamente para la operación del servicio de Call Center, deberá contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, y dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.

- El ingreso a cuartos técnicos por personal ajeno será registrado en una bitácora ubicada en la entrada de estos lugares de forma visible y se archivará en cada una de las áreas.

- Velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios de la Cooperativa.

25.3 SUBGERENCIA ADMINISTRATIVA

- Proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de COONFIE.

- Identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la Cooperativa.

- Almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de COONFIE.

- Certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.

- La subgerencia administrativa, con el acompañamiento de la subgerencia de sistemas, debe garantizar que las condiciones medioambientales del lugar de trabajo se encuentren controladas con los recursos mínimos necesarios, con el fin de disminuir las interrupciones o daños a la infraestructura tecnológica.

25.4 TERCEROS

- El personal provisto por terceras partes no debe intentar ingresar a áreas a las cuales no tenga autorización.

26 POLÍTICA DE DESTRUCCIÓN DE DOCUMENTOS CONFIDENCIALES

Se debe seguir el PR-GI-12 Eliminación Documental el cual define el proceso a seguir con la finalidad controla la disposición final de los documentos, conforme a lo establecido a las Tablas de Retención Documental-TRD y en Programa de Gestión Documental PGD.

Toda eliminación documental debe ser aprobada por el Comité de Archivo garantizando que los documentos a eliminar no poseen valores primarios o secundarios y cumplen con los tiempos de retención dispuestos en las Tablas de Retención Documental TRD. Las eliminaciones documentales deberán contar con la Acta de eliminación, Inventario a eliminar, si la eliminación documental se lleva a cabo por tercero se deberá enviar certificado he informe fotográfico de la respectiva eliminación.

Si, el comité de archivo decide en el acta de eliminación en la técnica de destrucción a utilizar sea picar, el funcionario debe asegurar que el proceso sea lo óptimo posible, optando por destruir los documentos con responsabilidad. No basta con romper el papel en cuatro trozos, puesto que esto facilita el proceso de recuperación de información, lo que acarrea efectos negativos, especialmente al titular de la información, por ello se debe asegurar que no será posible recuperar ningún soporte, archivo o documento que contenga información confidencial, de tal modo que en ningún momento del proceso de

destrucción esté en riesgo la confidencialidad de los datos a eliminar.

27 POLÍTICA DE SEGURIDAD DE LOS EQUIPOS

COONFIE para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la Cooperativa que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

27.1 SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

27.1.1 SUBGERENCIA DE TIC

- Proveer los mecanismos y estrategias necesarios para proteger laconfidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de COONFIE.

- Realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la Cooperativa.

- La subgerencia de TIC, en conjunto con la subgerencia administrativa debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.

- Establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la Cooperativa y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

- En COONFIE para aislar los equipos de áreas sensibles, como la de los servidores protegiendo su acceso de usuarios no autorizados de la red de datos, a este proceso se le llama segmentación y se realiza con la creación de redes de área local virtuales (VLANs), con ellas se garantiza la seguridady administración de los equipos.

- En COONFIE, los lineamientos del manejo de equipos tecnológicos (activos), en cuanto a su traslado, movimiento de agencia y/o dependencia y cambio de responsable se realiza por medio de un acta, dirigida al área de TIC. Referente a la información contenida en el equipo se debe realizar un borrado después de hacer una copia de seguridad (en caso de requerirse), para luego hacer entrega a otro funcionario, puesto que dichos datos solo corresponden al personal que desempeña el cargo.

27.1.2 AUDITORIA INTERNA

- Incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de COONFIE.

27.1.3 DIRECCIÓN DEL SIAR

- Analizar las recomendaciones emitidas por los órganos de control interno de las diferentes áreas de la Cooperativa, en particular de las áreas sensibles.

27.1.4 SUBGERENCIA ADMINISTRATIVA

- Autorizar o restringir los accesos físicos a las áreas donde están los equiposde cómputo en horas no hábiles mediante el formato **FO-AD-13 Permiso de Trabajo Horario No Hábil**.

- Velar por la salida de equipos de cómputo institucionales de las instalaciones de COONFIE cuenten con la autorización documentada y aprobada previamente por su área, de acuerdo con el formato **FO-AD-11 Movimiento de Activos Fijos**.

- Velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la Cooperativa posean pólizas de seguro.

27.1.5 TODOS LOS FUNCIONARIOS

- La subgerencia de TIC es la única área autorizada para realizar movimientos o asignaciones de recursos tecnológicos, por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la Cooperativa.

- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione la subgerencia de TIC.

- La instalación, reparación o retiro de cualquier componente de hardware de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la Cooperativa, solo puede ser realizado por los funcionarios de la subgerencia de TIC, o personal de terceras partes autorizados por dicha área.

- Los funcionarios y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no

laborales.

- Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados, priorizando las medidas de seguridad apropiadas que garanticen su integridad física.

- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

- En caso de pérdida o robo de un equipo de cómputo de COONFIE, se debeinformar de forma inmediata al líder del proceso para que se inicie el trámite interno, interponer la denuncia ante la autoridad competente.

- Los funcionarios y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones mientras el equipo este desatendido y una vez finalice las labores diarias, estos deben ser almacenados bajo las protecciones de seguridad necesarias.

28 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los funcionarios.

Los funcionarios, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con la Cooperativa deben conservar su escritorio libre de información, así como la carpeta “Descargas”, propiedad de COONFIE, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de los sistemas de información y comunicaciones de COONFIE deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los usuarios de los sistemas de información y comunicaciones de COONFIE deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.

No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

29 POLÍTICA DE SEGURIDAD DE LAS OPERACIONES DE TIC.

29.1 ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

La subgerencia de sistemas, encargada de la operación y administración de los recursostecnológicos que apoyan los procesos de COONFIE, asignará funciones específicas a sus funcionarios, quienes deben efectuar la operación y administración de recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos serán adecuadamente controlados y debidamente autorizados.

Además, proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la Cooperativa, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

29.1.1 SUBGERENCIA DE TIC

- Efectuar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la Cooperativa

- Proporcionar a sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de COONFIE.

- Proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

- La subgerencia de TIC, a través de sus funcionarios, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (Capacity Planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

29.1.2 DIRECCIÓN DEL SIAR

- Emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica de la Cooperativa.

30 POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

COONFIE en cabeza de la subgerencia de sistemas proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica, en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataquesde software malicioso.

30.1 PROTECCIÓN FRENTE A SOFTWARE MALICIOSO.

30.1.1 SUBGERENCIA DE TIC

- Proveer herramientas tales como antivirus, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de COONFIE y los servicios que se ejecutan en la misma.

- COONFIE se protege de virus, spam y spyware interna y externamente, debido a que el ataque de software maliciosos no sólo se presenta a través del uso de internet, sino de manera interna en los servidores; se generan parches de seguridad mensualmente para que el atacante no pueda explotar la vulnerabilidad de la información.

- Certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

- La subgerencia de TIC, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus.

30.1.2 TODOS LOS FUNCIONARIOS

- No deberán cambiar o eliminar la configuración del software de antivirus, definida por la subgerencia de sistemas; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

- Ejecutar el software de antivirus sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

- Asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provengan de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar por medio de la plataforma a la mesa de ayuda, para que, a través de ella, la Subgerencia de TIC tome las medidas de control correspondientes.

- Abstenerse de descargar programas o aplicaciones en ningún equipo.

31 POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

COONFIE certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la subgerencia de TIC, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, la cooperativa velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad físicos y medio ambientales apropiados.

31.1 SUBGERENCIA DE TIC

- Generar y adoptar los procedimientos, protocolo de nombramientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

- COONFIE cuenta con una base de datos que es la encargada de almacenar la información del CORE de negocio (OPA), a la cual se le hacen copias de seguridad automáticas que se almacenan en unidades de cinta (TAPES).

- Disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos, para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

- Definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

- La subgerencia de TIC, a través de sus funcionarios, restaura la base de datos y cuenta con una modalidad de recuperación en caso de desastre. Las estrategias de generación, retención y rotación de las copias de respaldo de los activos de información de la Cooperativa están definidas dentro de los planes de mantenimiento SQL.

- Definir e implementar un procedimiento para probar, de forma regular, las copias generadas y así garantizar su integridad y funcionalidad al momento de una restauración

32 POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACION

COONFIE realizará monitoreo permanente del uso que dan los funcionarios y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información de la cooperativa. Además, velará por la custodia de los registros de cumpliendo con los periodos de retención establecidos para dichos registros.

La subgerencia de TIC y la Dirección del SIAR definirán la realización de monitoreo de los registros sobre los aplicativos donde operan los procesos misionales de la Cooperativa. El comité de seguridad regularmente se reunirá a analizar los resultados del monitoreo efectuado a los logs.

32.1 REGISTROS DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN.

32.1.1 SUBGERENCIA DE TIC Y DIRECCIÓN DEL SIAR

- En COONFIE para los eventos que generan registros de auditoría en los recursos tecnológicos y los sistemas de información a nivel de la base de datos existen los Logs de seguimiento, donde se observa la integridad de los Backups, al performance de los servidores, a los Logs de procesos generados por políticas de la empresa, a

los cierres de mes y en general a los cierres diarios.

- Determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de COONFIE.

- Definir de manera mensual cuáles monitoreos se realizarán de los registros sobre los aplicativos donde se opera los procesos misionales de la Cooperativa. Así mismo, se deben reunir para analizar los resultados de cada monitoreo efectuado.

- La subgerencia de TIC, a través de sus funcionarios, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos establecidos a auditar.

- La subgerencia de TIC debe certificar la integridad y disponibilidad de los registros generados en la plataforma tecnológica y los sistemas de información de COONFIE. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

- La subgerencia de TIC debe garantizar que todos los sistemas de información, equipos y/o dispositivos que permitan la sincronización de la hora por red, cumplan con su correcta sincronización teniendo como referencia la hora legal colombiana dada por el instituto nacional de metrología.

32.1.2 DESARROLLADORES (INTERNOS Y EXTERNOS)

- Generar registros (log) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados.

- Registrar en los logs de auditoria eventos como: fallas de validación, intentos de autenticación fallidos o exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la subgerencia de sistemas y la Dirección del SIAR.

- Evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoría que brinden información adicional a la estrictamente requerida.

33 POLÍTICA DE CONTROL DE SOFTWARE OPERACIONAL DE COONFIE

COONFIE a través de la subgerencia de TIC, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el

software operativo es actualizado.

33.1 CONTROL AL SOFTWARE OPERATIVO

33.1.1 SUBGERENCIA DE TIC

- COONFIE, a través de la subgerencia de TIC y sus funcionarios, designará responsables y establecerá restricciones para el control de la instalación del software operativo, donde solo personal autorizado podrá realizar dicha actividad.

- Asegurarse que el software operativo instalado en la plataforma tecnológica de COONFIE cuenta con soporte de los proveedores.

- Establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Cooperativa.

- Conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones. Las actualizaciones de OPA las realiza un funcionario de la Cooperativa con previa asistencia y asesoría de los proveedores.

- Validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado. En COONFIE, cuando existe cambio o procesos de migración, se debe crear un comité técnico, con un líder de cada área cuya función es validar y controlar que los datos migrados de un sistema a otro sean exactos; dando a ellos el visto bueno y dando por cumplido el proceso de migración. El proceso de validación de la migración se realiza a través de nivel de balances y de productos.

34 POLÍTICA DE GESTION DE VULNERABILIDADES

COONFIE, a través de la subgerencia de TIC y el comité de Seguridad de la Información, se revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

34.1 GESTIÓN DE VULNERABILIDADES

34.1.1 COMITÉ DE SEGURIDAD DE LA INFORMACION

- Establecer en conjunto el cronograma para la aplicación de las pruebas de vulnerabilidades y hacking ético.

- Revisar, valorar y gestionar las vulnerabilidades técnicas encontradas según las pruebas o escaneos de penetración y hacking ético.

34.1.2 SUBGERENCIA DE TIC

- Revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.

- La subgerencia de TIC, a través de sus funcionarios, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades detectadas en la plataforma tecnológica según los informes de las pruebas realizadas.

- Identificar y remediar las vulnerabilidades de la infraestructura tecnológica de forma periódica, generar los informes de los hallazgos con sus respectivos planes de remediación, así mismo generar un análisis diferencial entre los resultados del informe actual con respecto al inmediatamente anterior. Las herramientas usadas para este fin deberán estar homologadas por el CVE (Common Vulnerabilitis and Exposures).

- Adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético por un ente independiente con el fin de garantizar la objetividad. En COONFIE las pruebas de vulnerabilidades y hacking ético se llevarán a cabo cada 3 años.

- Presentar al comité de seguridad de la información el análisis de los informes entregados por el ente independiente y los efectuados por la Cooperativa.

34.1.3 SUBGERENCIA DE TIC Y DIRECCIÓN DE SIAR

- Revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

35 POLÍTICA DE SEGURIDAD DEL SOFTWARE

COONFIE asegurará que el software adquirido y desarrollado tanto al interior de la Cooperativa, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos según las necesidades identificadas en los comités donde se planteen las diferentes necesidades. Las áreas propietarias de sistemas de información, la Subgerencia de TIC y la Dirección del SIAR incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

35.1 ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

35.1.1 PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN, SUBGERENCIA DE TIC Y DIRECCIÓN DEL SIAR

- Todos los sistemas de información o desarrollos de software deben tener un área responsable dentro de la Cooperativa formalmente asignada.

- La Subgerencia de TIC debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

- Las áreas propietarias de los sistemas de información, en acompañamiento con la Subgerencia de TIC y la Dirección del SIAR deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

- Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

- Liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

35.1.2 DESARROLLADORES (INTERNOS O EXTERNOS).

- Documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiere desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
- Certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
- Asegurar que los requerimientos de seguridad establecidos por la dirección del SIAR sean aplicados en cada desarrollo.
- Establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- Asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.
- Utilizar los protocolos sugeridos por la subgerencia de sistemas y Dirección del SIAR en los aplicativos desarrollados.
- En cuanto a comunicaciones, por seguridad la Cooperativa maneja canales dedicados de alta calidad (fibra óptica) lógicamente controlados por la seguridad perimetral que se encarga de la protección y/o detección de intrusos en áreas especialmente sensibles. A nivel de usuarios con previa información del área administrativa se habilitan o deshabilitan los operadores.

35.2 DESARROLLO SEGURO, REALIZACIÓN DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

COONFIE velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Cooperativa.

35.2.1 SUBGERENCIA DE TIC

- Implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

- Contar con sistemas de control de versiones para administrar los cambios delos sistemas de información de COONFIE.

- Aprobar y gestionar la compra de todo aplicativo informático o software en concordancia con el requerimiento efectuado por el área solicitante, este deberá ser con licenciamiento tipo propietario en su mayoría, todo software con licenciamiento GNU, GPL o libre deberá ser analizado antes de su instalación y/o uso.

- En cuanto a los sistemas de información adquiridos o desarrollados por terceros, dentro de las políticas que define la Cooperativa se tienen claros aspectos tales como: el licenciamiento, calidad y la eficiencia del software para de esta manera salvaguardar la información que por normatividad se vuelve confidencial para COONFIE; razón por la cual debe ser lo más fiable posible.

- Generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación; estas son realizadas por medio de un reglamento o manual.

- La subgerencia de TIC, a través de sus funcionarios, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

- Generar controles de gestión de cambios al software aplicativo y los sistemas de información OPA, Opita y Administrador de Informes.

- En COONFIE los controles de seguridad en la tercerización de servicios para el tratamiento de la información se realiza a través de túneles VPN para empresas como: OPA y VISIONAMOS.

35.2.2 DESARROLLADORES (INTERNOS O EXTERNOS)

- Considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, pasando desde el diseño hasta la puesta en marcha.

- Proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de COONFIE; dicho soporte debe contemplar tiempos de respuesta aceptables.

- Construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

- Suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

- Asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados, permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.

- Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

- Garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

- Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción; e información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

- Prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

- Evitar incluir las cadenas de conexión a las bases de datos desde los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, lo cual se recomienda que estén cifrados.

- Certificar el cierre de la conexión a las bases de datos desde los

aplicativos tan pronto como estas no sean requeridas.

- Desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurarque dichos archivos solo tengan privilegios de lectura.

- Proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

- Asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

35.2.3 DIRECCIÓN DEL SIAR

- Verificar que las pruebas de seguridad sobre los sistemas de información se efectúen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

36 POLÍTICA DE USO DE CORREO ELECTRÓNICO

COONFIE proveerá las condiciones para el acceso y manejo del correo electrónico empresarial. Así mismo, velará porque los funcionarios autorizados hagan uso responsable de los servicios y los accesos asignados.

36.1 USO DEL CORREO ELECTRÓNICO EMPRESARIAL

- Todos los mensajes enviados o recibidos por medio del correo electrónico empresarial pertenecen a COONFIE, el cual se reserva el derecho de acceder y revelar los mensajes enviados por este medio para cualquier propósito; sólo los siguientes funcionarios cuentan con previa autorización para el acceso desde el dispositivo móvil:

    - Gerente General.
    - Subgerentes.
    - Directores de Oficina.
    - Director de cartera.
    - Administrador de la Base de Datos.
    - Asistente de Consejo.

- Asistente de Gerencia General.
- Asistente de Sistemas 4.

- El envío de correos electrónicos a dominios diferentes a los de la cooperativa será limitado y controlado. Sólo tendrán autorización los funcionarios mencionados en el punto anterior y aquellos a quienes su jefe inmediato ha considerado que lo requiere para el desempeño de sus funciones.

  Nota 1: si en el desarrollo de las actividades un funcionario requiere autorización para el envío de correos externos, debe manifestarlo a su jefe inmediato y será éste quién toma ladeterminación de dar continuidad al proceso, comunicándolo así a la Dirección del SIAR.

  Nota 2: No se autorizará, por ningún motivo, a los buzones que manejan los brigadistas, pasantes, aprendices Sena y supernumerarios el envío de correos externos.

- Los funcionarios autorizados a enviar correos externos deben hacerlo bajo un estricto sentido de responsabilidad, velando por el buen nombre de la cooperativa, cerciorándose de la veracidad de la información enviada y asegurando su privacidad.

- Se prohíbe el uso del correo electrónico empresarial para fines personales.

- El funcionario debe evitar que su cuenta de correo electrónico empresarial sea utilizada por terceros.

- Es responsabilidad del funcionario evitar que la información confidencial de la Cooperativa sea transmitida por medio de su cuenta de correo electrónico empresarial, salvo previa autorización expresa; en este caso los archivos deben viajar de forma segura por canales encriptados.

- Evitar conectarse a redes inalámbricas de uso público, deben desactivar las redes inalámbricas como WIFI, bluetooth o infrarrojos en los dispositivos móviles.

- Es responsabilidad de los funcionarios mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar a terceros (internos o externos) la ejecución de operaciones o acciones.

- Para mejorar el nivel de seguridad en el inicio de sesión de los correos electrónicos se configura un método de autenticación adicional, función que solo está habilitada para los líderes de área.

37 POLÍTICA ESPECIFICAS PARA WEBMASTER

Objetivo: Proteger la integridad de la página Web institucional, el software y la informacióncontenida en ellas.

37.1 DIRECTRICES.

Los responsables de áreas que requieran publicar información institucional en la página Web deben prepararla y depurarla para reportar al área encargada de la publicación, esta tramitará la solicitud solo si esta cuenta con las autorizaciones correspondientes.

A continuación, se enuncia los responsables de las publicaciones (administradores de contenido) y las áreas-funcionarios encargados de dichas autorizaciones.

- Webs externas

		Externas			
	Web	**coonfie.com**	**Credivirtual**	**QuieroMiCredito**	**CoonfiAnalytics**
Contenido	**Área Admin**	Comercial	Sistemas	Sistemas	Sistemas
	Usuario Admin	Diseñador G	Desarrollador G	Desarrollador G	Desarrollador G
Publicación	**Área Autoriza**	Comercial	Comercial/Crédito	Comercial	Comercial/Crédito
	Usuario Autoriza	Subgerente	Subgerentes	Subgerente	Subgerentes

- Webs internas

		Internas		
	Web	**Intranet**	**WorkManager**	**Informes**
Contenido	**Área Admin**	Transformación Digital	Transformación Digital	Sistemas
	Usuario Admin	Coordinado PDP	Asesor GD	Asistente 3
Publicación	**Área Autoriza**	Transformación Digital	Transformación Digital	Área solicitante
	Usuario Autoriza	Director	Director	Líder de área

El área responsable de realizar las copias de seguridad, su almacenamiento y su respectivo registro histórico es la subgerencia de sistemas.

Los responsables de los contenidos de las páginas Web (Web masters), deben llevar un registro de cambios y/o actualización del contenido de esta según la autorización dada por parte del funcionario autorizado.

Las claves de acceso de los responsables de los contenidos de las páginas Web (Web masters), son estrictamente confidenciales y solo deben ser usadas bajo la autorización del funcionario autorizado.

38 POLÍTICAS ESPECIFICAS PARA FUNCIONARIOS Y CONTRATISTAS DEL AREA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACION.

Definir las pautas generales para asegurar una adecuada protección de la información de COONFIE por parte de los funcionarios y contratistas de TI.

Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.

Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de Manejo Disposición de Información, Medios y Equipos, es decir llevar a cabo mejores prácticas parala eliminación de la información de acuerdo con el software disponible en COONFIE. Ej.: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
Los funcionarios encargados de realizar la instalación o distribución de software sólo instalarán productos con licencia y software autorizado.

Los funcionarios de la Subgerencia de TIC no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Subgerente de Sistemas y el registro en la mesa de ayuda.

Los funcionarios de la Subgerencia de TIC se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.

Los funcionarios de la Subgerencia de TIC no utilizarán la información para fines comerciales particulares o diferentes al ejercicio de sus funciones.

Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro. Las copias

licenciadas y registradas del software adquirido deben ser únicamente instaladas en los equipos y servidores de COONFIE. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de COONFIE.

La copia de programas o documentación requiere tener la aprobación escrita y del proveedor si éste lo exige.

Aquellos servicios y protocolos que no son esenciales para el normal funcionamiento de los sistemas de información deben ser deshabilitados, pero de requerirse pueden ser habilitados y estos deben ser informados en el comité denotando su razón y uso.

El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado. Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.

Las pruebas de laboratorio o piloto de software con licenciamiento freeware o shareware deben ser realizadas por la subgerencia de TIC y estas a su vez informadas al Comitéde Seguridad de la Información y en lo posible hacerlas sin una conexión a la red LAN de la Cooperativa.

39 POLÍTICA DE TERCERIZACIÓN O PROVEEDORES.

Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la cooperativa, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por COONFIE.

Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de COONFIE, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

La subgerencia de TIC deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información de COONFIE.

40 POLÍTICA DE GESTION DE LOS INCIDENTES DE LA SEGURIDAD DE LA

INFORMACIÓN

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.

COONFIE promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, el Oficial de Protección de Datos debe ser informado de los incidentes de seguridad de la información que involucren datos personales, quien tendrá la responsabilidad de reportar ante la Superintendencia de Industria y Comercio.

La Gerencia General o Consejo de Administración a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades administrativas y/o judiciales; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

40.1 RESPONSABILIDADES Y CUMPLIMIENTOS

Los directores o jefes de área como responsables de los activos de información deben reportar a la Subgerencia de TIC los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

- El Comité de seguridad debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información. El Comité de seguridad deben evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares y escalar aquellos en los que se considere pertinente.

- El Comité de seguridad debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su ocurrencia nuevamente.

- La Subgerencia de TIC debe crear bases de conocimiento de acuerdo con los lineamientos definidos por el Comité de seguridad para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

- Los funcionarios, deben reportar cualquier evento o incidente relacionado con la seguridad de la información y los recursos tecnológicos con la mayor prontitud posible.

- Los funcionarios deben informar, en caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno o confidencial, a la dirección del SIAR, para que se registre y se le dé el trámite necesario.

41 POLÍTICA DE CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

La Cooperativa COONFIE, velará por la identificación, documentación y cumplimiento de lalegislación relacionada con la seguridad de la información, entre ellas la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

La Subgerencia de TIC deberá garantizar que todo el software que se ejecute los activos de información de COONFIE esté protegido por derechos de autor y requiera licencia de uso o, sea software de libre distribución y uso.

Los usuarios y/o funcionarios de COONFIE deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software, se recuerda que es ilegal duplicar software, duplicar documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la ley.

La Subgerencia de TIC realizará el procedimiento de Copias de respaldo (Backups) de los registros alojados en los sistemas de información.

COONFIE implementará los lineamientos para asegurar la privacidad y protección de datos personales, definiendo claramente los deberes en las actividades de recolección, procesamiento y transmisión de estos; así mismo al momento de suscribir un contrato o acuerdo de prestación de servicio donde se intercambie información se deberá contar con la debida autorización y/o acuerdos de confidencialidad que garantice los tratamientos de información pertinente incluyendo los requisitos y condiciones requeridas para el intercambio de información.

Los lineamientos y directrices especificas se encuentran detalladas en el ***Manual del Sistema de Protección de Datos y Responsabilidad Demostrada***.

COONFIE a través de la Subgerencia de TIC debe implementar métodos y herramientas que permitan proteger la información personal de los funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro tipo dealmacenamiento o

repositorio previniendo su divulgación, alteración o eliminación sin la autorización.

42 POLÍTICA DE EVALUACIÓN Y ACTUALIZACIÓN DE SEGURIDAD DE LA INFORMACION

La Subgerencia de TIC tiene como una de sus funciones proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para salvaguardar la información digital y física, los equipos de cómputo e instalaciones de cómputo, así como de las bases de datos de información automatizada en general.

Así mismo la promulgación, socialización, capacitación y evaluación de los funcionarios de la Cooperativa sobre todo lo relacionado con el Sistema de Gestión de Seguridad de información, políticas y controles.

La Subgerencia de TIC, junto con la Subgerencia Comercial y el apoyo de la Dirección de SIAR deben definir e implementar un procedimiento para la divulgación de información a los asociados, sobre los riesgos derivados del uso de los diferentes medios y canales que la Cooperativa pone a su disposición para el acceso a su información y recursos.

El Gerente general, Subgerentes, directores, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad.

COONFIE a través del comité de seguridad de la información apoyaran la evaluación y seguimiento del Manual de seguridad de la información liderado por la subgerencia de TIC, como parte del proceso de mejora continua y actualización que se realizara como mínimo una vez al año.

43 POLÍTICAS ESPECIFICAS PARA FUNCIONARIOS DE COONFIE

Definir las pautas generales para asegurar una adecuada protección de la información por parte de los usuarios de COONFIE.

Todo el software usado en la plataforma tecnológica del COONFIE debe tener su respectiva licencia y acorde con los derechos de autor. Los recursos tecnológicos y de software asignados de propiedad de COONFIE son responsabilidad de cada funcionario o usuario.

Los usuarios solo tendrán acceso a los datos y recursos autorizados por COONFIE, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información. Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.

Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por COONFIE. Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente a la mesa de ayuda.

Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizandoarchivos compartidos en los computadores, discos virtuales, CD, DVD, medios removibles; deben usarse los mismos servicios del sistema de información, los cuales están controladosy auditados.

44 POLÍTICA DE USO DE MENSAJERÍA INSTANTÁNEA Y REDES SOCIALES

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de COONFIE, que sea creado a nombre personal en redes sociales como: *Twitter*, *Facebook*, *YouTube*, *Instagram*, *etc.,* se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sea originada por COONFIE debe ser autorizada por la subgerencia comercial para ser socializadas y con un vocabulario institucional.

No se debe utilizar el nombre de COONFIE en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.

El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.

No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.

45 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

En desarrollo de la legislación vigente en Colombia en Protección de Datos Personales, la COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CREDITO "COONFIE" domiciliada en Neiva - Huila, en la calle 10 No 6-68, reglamenta el tratamiento de los datos personales de sus asociados, futuros asociados, funcionarios, aprendices, proveedores y contratistas a los cuales se le da tratamiento, para estos efectos esta política se sustenta en los documentos Manual del Sistema de Protección de Datos y Responsabilidad Demostrada, así como el Política de Protección de DatosPersonales.

46 DOCUMENTOS QUE APOYAN LA POLÍTICA DE SEGURIDAD

Los documentos que apoya los procesos en la Cooperativa y en especial que respaldan el Sistema de Gestión de Seguridad de la información, son los siguientes documentos como Manuales, Políticas, Procedimiento, Formatos, Listados, Bitácoras y Documentos de Apoyo.

Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, en él, se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

También es recomendable el uso de instructivos para detallar aún más las tareas y acciones que se deben desarrollar dentro de un procedimiento, como son los instructivos de trabajo y de operación; los primeros para la ejecución de la tarea por la persona y los segundos para la manipulación o la operación de un equipo.

Los funcionarios de la cooperativa COONFIE pueden consultar las descripciones de cada documento a través de la Intranet, en los documentos de calidad por procesos, en Gestión TIC.

47 PROCEDIMIENTO DE LA INFORMACIÓN DOCUMENTADA

Garantiza que la organización cuente con los documentos estrictamente necesarios a partir de su perfil de actuación en cada momento y maneja la dinámica del mejoramiento, mostrando la realidad que atraviesa COONFIE en cada momento, porque incorpora la eficacia de las diferentes acciones, a través de la revisión documental y del cumplimiento de los requisitos idénticos en los diferentes modelos de gestión, sobre el control de la información documentada. Así mismo, busca garantizar que los documentos internos y externos en uso sean confiables y se

mantengan actualizados, una vez se evidencie la eficacia de las acciones correctivas, preventivas y de mejora que hacen que los procesos se ajusten y evolucionen; de igual manera que los documentos existentes en el momento de la evaluación y comprobación del cambio que se implementó como solución a un problema, riesgo o a una oportunidad se conserven.

PR-GI-03 Elaboración y Control de Documentos y el LI-GI-01 Listado Maestro de Documentos.

48 PROCEDIMIENTO DE CONTROL DE REGISTROS

Está definido para evidenciar las acciones realizadas y los resultados obtenidos en la ejecución de las actividades, con el fin de analizar los datos, y lo que es más importante, para la toma de decisiones, de tal forma que un registro físico que no aporta valor o no lleva a una decisión de mejora o de acción, no se debe tener en el sistema, ya que lo único que haría es desgastar a la organización y generar residuos sólidos como papel mal utilizado.

49 PROCEDIMIENTO DE AUDITORIA INTERNA

La auditoría interna es una herramienta para la alta dirección, en el momento de determinarla eficacia y la eficiencia del sistema de gestión, a través de la identificación de las fortalezas y debilidades.

Esta es la razón por la cual se recomienda siempre realizar auditorías internas antes de llevar a cabo la revisión gerencial, ya que para esta última se requiere información sobre el sistema y los procesos, de tal manera que se pueda evaluar la adecuación, la conveniencia y la eficacia del sistema de gestión.

Se hacen auditorias para evaluar la conformidad con las políticas de la organización, para evaluar el nivel de implementación del sistema de gestión, para evaluar el estado de mantenimiento y la capacidad de mejoramiento del sistema de gestión.

La Cooperativa realizará auditorías de acuerdo al plan de auditoría interna para evaluar la seguridad de la información donde como mínimo se tenga en cuenta la disponibilidad, integridad, confidencialidad y calidad del servicio.

PR-GI-04 Auditorías Internas

50 PROCEDIMIENTO DE ACCIÓN CORRECTIVA, PREVENTIVA Y DE MEJORA

El objetivo de este procedimiento es definir los lineamientos para eliminar una o más

causas que determinaron una no conformidad asociada con los requisitos de la política de seguridad de la información de COONFIE, así como, definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad.

PR-GI-01 ACCIONES CORRECTIVAS, PREVENTIVAS Y OPORTUNIDADES DE MEJORA.

51 PROCESO DISCIPLINARIO

Dentro de la estrategia de seguridad de la información de COONFIE, está establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación al Manual del Sistema de Gestión de Seguridad de la información y su Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y los otros colaboradores de la Cooperativa violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de gestión de la Subgerencia Administrativa y se encuentran enmarcadas dentro del reglamento interno de trabajo de la Cooperativa.

52 GESTION DE LA CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de COONFIE, para proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.

Prevenir interrupciones en las actividades de la plataforma informática de la cooperativa, que van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.

52.1 POLÍTICA DE CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACION

COONFIE proporcionará los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos quese presenten en la cooperativa y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de estos; se restablecerán las operaciones con el menor costo

y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. La cooperativa, mantendrá canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.

52.2 NORMAS DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACIÓN

52.2.1 COMITÉ DEL SIAR, SARLAFT Y DIRECCIÓN DEL SIAR

- El Comité del SIAR y SARLAFT junto con la Dirección del SIAR, deben reconocer las situaciones que serán identificadas como emergencia o desastre para la cooperativa, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

- El Comité SIAR y SARLAFT, junto con la Dirección del SIAR, deben liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres.

- La Dirección del SIAR, debe realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

- La Dirección del SIAR, junto con el Comité de SARLAFT, producto del análisis del impacto de negocio (BIA) deben seleccionar las estrategias de recuperación más convenientes para la cooperativa.

- La Dirección del SIAR, debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

- El Comité SIAR y SARLAFT, junto con la Dirección del SIAR, deben asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

52.2.2 SUBGERENCIA DE TIC Y DIRECCIÓN DEL SIAR

La Dirección del SIAR, en conjunto con la Subgerencia de TIC, deben elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

La Subgerencia de TIC y la Dirección del SIAR, deben participar activamente en las pruebas de recuperación ante desastres y notificar los resultados al Comité SIAR y SARLAFT.

52.2.3 CONSEJO ADMINISTRACIÓN, GERENCIA GENERAL, SUBGERENCIAS Y DIRECCIONES

El Consejo, la Gerencia, las Subgerencias y las direcciones, deben identificar al interior desus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

53 CUMPLIMIENTO

Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios y otros colaboradores de COONFIE. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la cooperativa tomará las acciones disciplinarias y legales correspondientes. El Manual de la Política de Seguridad de la Información debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

54 DOCUMENTACIÓN

El Manual de la Política de Seguridad de la Información de COONFIE esta soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este manual. Los usuarios de los servicios y recursos de tecnología de COONFIE pueden consultar los procedimientos a través de la intranet, en los documentos de SIG por procesos, en Gestión de Tecnología de la Información y Comunicaciones TIC.

55 DECLARACIÓN DE APLICABILIDAD

Para el caso específico de COONFIE, este tipo de análisis se hace evaluando el cumplimiento de la Norma ISO/IEC 27001:2022, para cada uno de los controles establecidos en la gestión de la seguridad de la información que este estándar especifica.

56 VIGENCIA

El presente acuerdo fue aprobado por el Consejo de Administración en reunión del 24 de junio de 2024, según Acta No. 009 y deroga todas las normas que le sean contraria y rige a partir de la fecha de su aprobación

COMUNÍQUESE Y CÚMPLASE

ANABELLA GARCIA TORRES
Presidenta del Consejo de Administración

ALICIA ORTIZ VARGAS
Secretaria del Consejo de Administración